ISSN 3083-6573 Print
ISSN 3083-6581 Online

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

IT&S

INFORMATION TECHNOLOGIES & SYSTEMS

3 (9) 2026

TOPICS

- ITERATIVE LOGICAL-LINGUISTIC METHOD OF ANALYSIS
- CYBER DEFENSE SYSTEM IN A SCIENTIFIC INSTITUTION
- MINIMIZATION OF CYBER INCIDENTS AUTOMOTIVE AND POWER SYSTEMS

The Journal is included (since 1 Jun. 2026) in the list of scientific professional publications of Ukraine within the "Information Technologies and electronics" cluster (category "B") in the specialties F3, F4, F5, F6, F7, G7 (Order of the Ministry of Education and Science of Ukraine No. 928 from 11.06.2026).

Media ID R30-05899
Editorial address: Institute of Information Technologies and Systems
of the National Academy of Sciences of Ukraine,
40, Hlushkova Akd. ave., Kyiv, 03187
phone: +380 (44) 526-00-09, e-mail: its.journal.ua@gmail.com,
https://nasu-periodicals.org.ua/index.php/its

Журнал з 01.06.2026 включено до переліку наукових фахових видань України у межах кластеру «Інформаційні технології та електроніка» (категорія «Б») за спеціальностями F3, F4, F5, F6, F7, G7 (наказ Міністерства освіти і науки України від 11.06.2026 № 928).

Ідентифікатор медіа: R30-05899
Адреса: Інститут інформаційних технологій та систем НАН України, м. Київ,
Просп. Акад. Глушкова, 40, 03187
Телефон: 526-00-09, e-mail: its.journal.ua@gmail.com,
Сайт: https://nasu-periodicals.org.ua/index.php/its/

Підп. до друку 31.08.2026 р. Формат 70 × 108/16. Гарн. Book Antiqua.
Ум. друк. арк. 10,68. Обл.-вид. арк. 10,83. Тираж 67 пр. Зам. № 8150
Видавець і виготовлювач ВД «Академперіодика» НАН України
01024, Київ, вул. Терещенківська, 4

Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи серії ДК № 544 від 27.07.2001

NATIONAL ACADEMY OF SCIENCES OF UKRAINE
INSTITUTE OF INFORMATION TECHNOLOGIES AND SYSTEMS
V.M. GLUSHKOV INSTITUTE OF CYBERNETICS

INFORMATION TECHNOLOGIES & SYSTEMS

3 (9) 2026

ACADEMIC AND RESEARCH JOURNAL
FOUNDED IN JANUARY 2025
PUBLISHED 6 TIMES PER YEAR
KYIV

CONTENTS

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ
ІНСТИТУТ КІБЕРНЕТИКИ ІМЕНІ В.М. ГЛУШКОВА

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ & СИСТЕМИ

3 (9) 2026

НАУКОВИЙ ЖУРНАЛ
ЗАСНОВАНО В СІЧНІ 2025
ВИХОДИТЬ 6 РАЗІВ НА РІК
КИЇВ

ЗМІСТ

https://doi.org/10.15407/intechsys.2026.03.003
УДК 004.8:37

Ю.О. МАКОГОН, аспірант,
Харківський національний університет радіоелектроніки,
просп. Науки, 14, Харків, 61166, Україна
https://orcid.org/0009-0005-4369-1555
yurii.makohon@nure.ua

О.Г. РУДЕНКО, д-р. техн. наук, професор,
Харківський національний університет радіоелектроніки,
просп. Науки, 14, Харків, 61166, Україна
https://orcid.org/0000-0003-0859-2015
oleh.rudenko@nure.ua

АРХІТЕКТУРНИЙ СИНТЕЗ КОМПОЗИТНИХ НЕЙРОМЕРЕЖЕВИХ СИСТЕМ ДЛЯ ПРЕДИКТИВНОГО ОБРОБЛЕННЯ ДАНИХ У ЦИФРОВИХ ОСВІТНІХ СЕРЕДОВИЩАХ

Це дослідження обґрунтовує методологічні та технічні принципи синтезу композитних нейромережевих архітектур, призначених для предиктивного оброблення даних у межах інфокомунікаційних освітніх середовищ. У контексті глобальної цифрової трансформації дослідження зосереджено на розробці адаптивних систем управління, де інтеграція рекурентних (RNN), графових (GNN) та трансформерних (Transformers) структур забезпечує високоточне моделювання когнітивної динаміки. У роботі розкрито функційні механізми динамічної оркестрації контенту та предиктивного моніторингу патернів оброблення інформації як основних елементів стратегії оптимізації. Проаналізовано технічні та епістемологічні обмеження, зокрема алгоритмічну непрозорість та інформаційну асиметрію, що зумовлює необхідність переходу до гібридних моделей для підвищення інтерпретованості інтелектуальних рішень. Особливу увагу приділено стратегічній ролі оптимізованих систем штучного інтелекту (ШІ) в Україні як життєво важливого інструменту для подолання освітніх розривів у кризові періоди. Переваги композитного підходу експериментально доведено на апаратному забезпеченні з обмеженими ресурсами (1 ГБ відеопам'яті), де було досягнуто значного скорочення затримки та підвищення стабільності системи.

Цитування: Макогон Ю.О., Руденко О.Г. Архітектурний синтез композитних нейромережевих систем для предиктивного оброблення даних у цифрових освітніх середовищах. *Information Technologies and Systems.* 3 (9). 2026. 3—14. https://doi.org/10.15407/intechsys.2026.03.003

Ключові слова: *адаптивне навчання, композитні нейромережеві архітектури, інфокомунікаційні системи, предиктивне оброблення даних, персоналізація, локальні обчислення, штучний інтелект.*

Вступ

Поточна еволюція освітніх просторів зумовлена експоненційною інтеграцією цифрових інструментів, що призводить до виникнення складних гібридних інфокомунікаційних середовищ. Нейронні мережі (НМ) виступають основними технологічними агентами в цій трансформації, здатними виконувати сучасну предиктивну аналітику та системну оптимізацію траєкторій навчання. Впровадження інтелектуальних алгоритмів підкреслює критичну дихотомію між операційною ефективністю обчислювальних моделей та необхідністю збереження когнітивної автономії. Системні виклики охоплюють забезпечення алгоритмічної прозорості (*explainability*), мінімізацію інформаційної асиметрії та запобігання реплікації соціальних упереджень під час машинного навчання на нерепрезентативних наборах даних. Враховуючи, що композитні НМ оперують нелінійною динамікою, епістемологічні питання щодо природи знань, генерованих алгоритмами, стають дедалі значущими. В українському контексті використання ШІ для оптимізації засвоєння знань має стратегічний вимір, виступаючи ресурсом для підтримки когнітивної стійкості та подолання дефіциту компетентностей, спричиненого воєнним конфліктом. Відповідно, існує об'єктивна потреба в науковій базі для синтезу архітектур НМ з урахуванням соціотехнічних наслідків.

Попри значні результати, синтез композитних рішень для цілісної оптимізації траєкторій в українському контексті залишається недостатньо дослідженим. Відсутність методологій, що поєднують структурні можливості *GNN* із семантичною потужністю Трансформерів у межах однієї адаптивної моделі, визначає актуальність цієї роботи.

Метою статті є наукове обґрунтування методологічних принципів синтезу композитних архітектур НМ для предиктивного оброблення даних у межах цифрової трансформації. Дослідження зосереджено на розробці стратегії синергетичного поєднання *RNN*, *GNN* та Трансформерів для інтенсифікації адаптивного навчання та формалізації процедур предиктивного коригування контенту.

Аналіз та формальна постановка задачі оптимізації

У межах сучасної дидактичної парадигми освітній процес інтерпретується як нелінійна динамічна система, де результуюча ефективність визначається складною взаємодією з багатофакторним середовищем [1, 2]. Суб'єкт навчання в цій моделі виступає як активний когнітивний агент, чий внутрішній стан безперервно еволюціонує

під впливом зовнішніх керуючих впливів. Впровадження інтелектуальних систем дозволяє здійснювати предиктивне управління середовищем, спрямоване на досягнення екстремумів цільових функцій успішності.

Математичне моделювання коригування траєкторії виконується за допомогою рівняння стану (1):

$$S_{t+1} = f\left(S_t, A_t, E_t\right), \tag{1}$$

де S_{t+1} — прогнозований стан когнітивної системи учня у наступний момент часу; S_t — поточний стан когнітивної системи учня у момент часу t; A_t — множина дій (навчальних завдань, взаємодій із вчителем чи системою); E_t — стохастичний вектор впливу зовнішнього середовища; f — функція переходу, що апроксимується нейронною мережею.

Використання композитних моделей забезпечує перехід від строго детермінованих схем до стохастичної адаптивної функції f, де параметри динамічно перераховуються на основі даних зворотного зв'язку. Цей підхід синтезує обчислювальний аналіз з оцінкою епістемологічних зрушень у структурі комунікації [3].

Для формальної верифікації якості оптимізації в *Learning Analytics* [4] використовуються цільові функції. Задачі класифікації рівнів засвоєння модулів вирішуються шляхом мінімізації втрат кросентропії (2):

$$L\left(y, \hat{y}\right) = -\sum y_i \log\left(\hat{y}_i\right), \tag{2}$$

де L — значення функції втрат; y — приналежність до реального класу (рівня знань); $\hat{y}$ — прогнозована ймовірність приналежності до класу.

Прогнозування безперервних показників (наприклад, ймовірності деградації знань або часових витрат) базується на мінімізації середньоквадратичної помилки (*MSE*) (3):

$$MSE = \frac{1}{n}\sum\left(y_i - \hat{y}_i\right)^2, \tag{3}$$

де n — кількість спостережень у вибірці; y_i — фактичне значення показника (наприклад, реальний бал учня); $\hat{y}_i$ — прогнозоване значення, отримане на виході нейронної мережі.

Аналіз нейромережевих парадигм у системній оптимізації

Аналіз останніх розробок [4—6] свідчить про те, що вибір конкретної архітектури НМ є результатом дидактичного проєктування, де параметри корелюють із характеристиками даних та цілями. *RNN*, *GNN* та Трансформери оцінюються у трьох доменах: темпоральному моделюванні, структурній організації та семантичній інтерпретації.

Темпоральне моделювання та предиктивна аналітика. Динамічна природа освіти вимагає врахування темпорального контексту. Математичні задачі містять апроксимацію ймовірності переходу (4):

$$P\left(S_t \left| S_{t-1}, A_{t-1} \right.\right), \tag{4}$$

де P — умовна ймовірність переходу в новий стан знань; S_t — стан знань у поточний момент; S_{t-1} — стан знань на попередньому кроці; A_{t-1} — дія або навчальне завдання, виконане на попередньому кроці.

Long Short-Term Memory (*LSTM*) архітектури є класичними для цих завдань [7], забезпечуючи вектори прихованого стану для довготривалої пам'яті. Трансформери пропонують альтернативу, аналізуючи масиви часових рядів паралельно за допомогою позиційного кодування, уникаючи втрати контексту в довгих послідовностях.

Структурне моделювання когнітивних зв'язків. Когнітивні домени мають складні нелінійні топології. У той час як *RNN* мають труднощі з лінеаризацією графових даних, *GNN* нативно спроєктовані для реляційних даних. Відповідно до праць [8, 9], середовища подають як формальні графи (5):

$$G = \left(V, E\right), \tag{5}$$

де V — множина вершин, що подають навчальні концепти або студентів; E — множина ребер, що відображають когнітивні або соціальні зв'язки між ними.

Механізм Message Passing забезпечує динамічне оновлення стану (6):

$$h_v^{(l+1)} = \sigma\left(\sum u \in N(v) \frac{1}{c_{vu}} W^{(l)} h_n^{(l)} \right), \tag{6}$$

де $h_v^{(l+1)}$ — векторне подання вершини v на шарі $l + 1$; σ — нелінійна функція активації (наприклад, *ReLU*); $N(v)$ — множина сусідніх вершин для вершини v; c_{vu} — нормалізуюча константа; $W^{(l)}$ — матриця ваг, що навчається; $h_n^{(l)}$ — стан сусідньої вершини u на попередньому шарі.

Семантична інтерпретація контенту. Оптимізація контенту вимагає контекстно-залежного оброблення природної мови (*NLP*). Трансформери [10], використовуючи *Self-Attention*, динамічно оцінюють значущість елементів незалежно від відстані. Це формалізується через *Scaled Dot-Product Attention* (7):

$$Attention\left(Q, K, V\right) = soft\max\left(\frac{QK^t}{\sqrt{d_k}} \right) V, \tag{7}$$

де Q — матриця запитів, що представляють поточні завдання або інтереси учня; K — матриця ключів, що кодують характеристики навчального матеріалу або попередній досвід; V — матриця значень, що

містить змістову інформацію про контент; d_k — розмірність векторів ключів (використовується для масштабування градієнтів); *softmax* — функція активації для отримання розподілу ймовірностей уваги.

Це дає змогу вирішувати складні лінгвістичні проблеми, такі як полісемія та кореференція [11].

Апаратна інтенсивність та обчислювальна складність. Впровадження стратегій оптимізації лімітується наявним обладнанням. *RNN* демонструють лінійну складність $O(N)$, роблячи їх ефективними для локального та мобільного розгортання. Складність *GNN* залежить від щільності графа $O\left(\|V\| + \|E\|\right)$. Трансформери демонструють найвищу інтенсивність через квадратичну залежність $O(N^2)$, що вимагає спеціалізованих *GPU* або *TPU* кластерів. Порівняльні результати узагальнено в Таблиці 1.

Результати цього всебічного аналізу демонструють, що жодна монолітна архітектура не може самостійно задовольнити багатошарові вимоги інтелектуальної освітньої екосистеми. Ефективна оптимізація системи вимагає переходу до композитних ансамблів нейронних мереж, використовуючи специфічні обчислювальні та когнітивні переваги кожної парадигми для балансу точності та ресурсоефективності.

Експериментальна оцінка продуктивності в умовах жорстких апаратних обмежень

Для підтвердження практичної спроможності синтезованих композитних архітектур було проведено серію тестів на типовому портативному обладнанні студентського класу. Основна гіпотеза полягала в тому, що композитні моделі забезпечують прийнятну якість прогнозів за критично низького споживання ресурсів, недоступного для сучасних *LLM*-подібних структур.

Таблиця 1. **Матриця функційної та технічної спроможності архітектур НМ**

Критерій оцінювання	*RNN / LSTM*	*GNN*	*Transformers*
Темпоральна точність	Висока. Оптимально для динамічного трекінгу.	Низька. Потребують темпоральної гібридизації.	Висока. Глобальне моделювання контексту.
Структурна валідність	Низька. Втрата топології через лінеаризацію.	Дуже висока. Апріорні структурні знання.	Середня. Імпліцитне вивчення структури.
Семантична гнучкість	Середня. Інформаційне вузьке місце в текстах.	Низька. Специфічні для завдань класифікації.	Дуже висока. Нелокальні залежності.
Обчислювальна складність	$O(N)$. Лінійна. Ефективні для локальних систем.	$O\left(\|V\| + \|E\|\right)$. Залежить від щільності.	$O(N^2)$. Квадратична. Вимагають *GPU*.

Технічні умови та інструментарій. Експериментальний стенд базується на ноутбуці з *CPU Intel Core i*5-1135*G*7 (4 ядра, 2,4–4,2 ГГц) та дискретним відеоадаптером *NVIDIA GeForce MX*350 на архітектурі *Pascal*. Карта має лише 2 ГБ *GDDR*5 *VRAM*, що є критичним порогом для сучасного глибокого навчання. Програмний стек: *Ubuntu* 22.04, *Python* 3.10, *PyTorch* 2.1.0 з підтримкою *CUDA* 11.8.

Для моделювання реальних умов багатозадачності обсяг доступної відеопам'яті (*VRAM*) для тренувального та інференс-процесів було програмно обмежено до 1 ГБ. Це імітує ситуацію, коли частина ресурсів зайнята операційною системою та інфокомунікаційними клієнтами.

Теоретичний аналіз *FLOPs*:

1. Монолітний Трансформер: Модель типу *Tiny-BERT* (4 шари, d = 312, де d — розмірність прихованого ембедінгу). За довжини послідовності N = 512, обчислення механізму *Self-Attention* потребує приблизно $2 \times N^2 \times d$ операцій (охоплюючи як оцінки QK^T, так і зважену суму V). Тільки для матриць *Attention* (512 × 512) за 32-бітного формату із плаваючою комою одинарної точності необхідно 1 МБ на кожну голову уваги. З урахуванням активацій та ваг (45 мільйонів параметрів), теоретичний мінімум пам'яті для інференсу одного батча становить ≈680–850 МБ.

2. Композитна модель: Поєднання блоку *LSTM* (128 одиниць) та 2-шарової *GCN* (*Graph Convolutional Network*). Кількість параметрів — 0,78 мільйона. Теоретична складність операції *LSTM* становить $O\left(N \times (8d^2 + 8dh)\right)$, де d — розмірність вхідних ознак, а h — кількість прихованих одиниць. При N = 512, це потребує у ≈18–20 разів менше *FLOPs*, ніж Трансформер.

Експериментальна процедура містила стандартизовану фазу *warm-up* з 50 ітерацій для усунення накладних витрат на ініціалізацію та шум кешування *CUDA*. Потім кожна модель виконувала безперервний цикл з 1000 циклів інференсу, імітуючи предиктивний потік у реальному часі для цифрового класу. Використовувалися високоточні лічильники продуктивності (*time.perf_counter*) для фіксації затримки інференсу, а бібліотека *NVIDIA Management Library* (*NVML*) забезпечувала опитування розподілу *VRAM*, частоти ядра *GPU* та теплового стану в реальному часі.

Результати вимірювань швидкості та стабільності системи наведено у Таблиці 2.

Аналіз апаратних аномалій:

1. Проблема *Out of Memory*: за умов збільшення довжини історії навчання до 1024 кроків Трансформер миттєво викликав помилку *RuntimeError*: *CUDA out of memory*, оскільки квадратичне зростання матриць уваги перевищило ліміт 1 ГБ. Композитна модель працювала бездоганно, використовуючи лише 58 МБ пам'яті.

2. Обчислювальний тротлінг: через високу обчислювальну інтенсивність Трансформера, після 4 хвилин безперервного прогнозуван-

ня частота ядра *GPU MX*350 впала з 1468 МГц до 920 МГц, що призвело до збільшення затримки з 86 мс до 118 мс. Композитна модель не викликала перегріву, зберігаючи пікову частоту протягом усього тесту.

3. Енергоефективність: оціночне енергоспоживання (*TDP*) під час роботи композитної архітектури було на 40% нижчим від номінального. Це критично для роботи ноутбука від акумулятора в умовах відсутності електропостачання, забезпечуючи до 3,5 годин додаткової автономності під час розрахунків.

Висновки розділу. Експеримент довів, що для реальних умов експлуатації на «студентському» обладнанні використання гібридних архітектур є не просто перевагою, а технічною умовою стабільності. Втрата точності у розмірі 0,009 *AUC* (менше 1,1%) є абсолютно виправданою платою за 14–кратне зростання швидкодії та можливість паралельного оброблення сотень потоків даних без ризику перегріву чи зупинки системи через брак пам'яті.

Адаптивні стратегії для оптимізації освітніх траєкторій

Апаратна стабільність та здатність композитних моделей функціонувати на локальних пристроях початкового рівня, перевірені під час експерименту, стають технологічним фундаментом для впровадження адаптивних стратегій у специфічних умовах українського освітнього простору. Воєнні дії та системна нестабільність критичної інфраструктури створили потребу в інструментах, які не залежать від постійного зв'язку з хмарою. Забезпечуючи високу швидкість (6,1 мс на інференс) та енергоефективність, запропоновані архітектури стають основою для підтримки когнітивної стійкості учнів [12, 13]. Очікується, що імплементація таких систем на базі *LSTM* скоротить «освітні розриви» серед внутрішньо переміщених осіб, надаючи можливість навчатися автономно під час блекаутів.

Практична реалізація цих стратегій базується на використанні *LLM* як інтелектуальних асистентів, проте саме композитний рівень

Таблиця 2. **Емпіричні дані продуктивності на ноутбуці (*MX*350, ліміт 1 ГБ *VRAM*)**

Параметри порівняння	Монолітний Трансформер	Композитна модель	Різниця ефективності
Споживання *VRAM* (Ваги+Кеш)	914,2 МБ (91,4%)	42,8 МБ (4,3%)	–95,3%
Час інференсу (*CPU*), мс	248,5	15,2	–93,8%
Час інференсу (*GPU*), мс	86,4	6,1	–92,9%
Максимальний розмір батча	2 (*Out of Memory* за 4)	128+	>64x
Температура *GPU* через 10 хв, °C	78° (Тротлінг)	54° (Стабільно)	–24 °C
Точність (*AUC ROC*)	0,841	0,832	–0,009

(локальне оброблення) відповідає за адаптивний розподіл підзадач відповідно до актуального стану учня [15]. Процес прийняття рішень математично формалізується через навчання з підкріпленням (*Reinforcement Learning, RL*), де вибір оптимальної педагогічної дії детермінується політикою π (8):

$$\pi(a|s) = P(A_t = a | S_t = s), \tag{8}$$

де $\pi(a|s)$ — стохастична політика агента (нейромережі), що визначає розподіл ймовірностей дій; P — умовна ймовірність настання події; A_t — випадкова величина, що позначає обрану дію (навчальне завдання) у момент часу t; S_t — випадкова величина, що характеризує поточний когнітивний стан учня; a — конкретна реалізація дії з простору допустимих педагогічних інтервенцій; s — векторний опис поточного рівня компетентності учня.

Стратегічна мета *RL*-системи полягає у максимізації інтегральної винагороди $J(\pi)$ (9):

$$J(\pi) = E_\pi \left[\sum_{t=0}^{\infty} \gamma^t r_t \right], \tag{9}$$

де J — цільова функція; E — математичне сподівання; g — коефіцієнт дисконтування $0 < g < 1$), що визначає важливість майбутніх винагород; r_t — отримана винагорода (*reward*) на кроці t.

Ефективним технологічним розв'язанням проблеми дефіциту національних наборів даних є впровадження методів крослінгвальних ембедінгів (10):

$$V_{uk} = W \cdot V_{en}, \tag{10}$$

де V_{uk} — векторний простір слів української мови; V_{en} — векторний простір слів англійської мови (багатої на ресурси); W — матриця лінійної трансформації, отримана через методи вирівнювання латентних просторів [16].

Цей підхід дозволяє проєктувати англомовні знання на український контент, забезпечуючи лінгвістичну валідність системи навіть за дефіциту локальних наборів даних.

Етика та епістемологія

Технологічна ефективність та перенесення обчислень на пристрої користувачів, підтверджені експериментально, актуалізують не лише питання швидкодії, а й глибинні етико–епістемологічні виклики. Здатність композитних моделей працювати локально на 1 ГБ *VRAM* створює умови для захисту приватності даних «за дизайном» (*Privacy by Design*), оскільки персональні когнітивні профілі учнів можуть оброблятися без передавання на зовнішні сервери. Водночас, використання гібридного підходу *(LSTM+GNN*) замість монолітних Трансформерів частково вирішує проблему «чорної скриньки», оскільки графові структури є більш інтерпретованими для педагогів.

Принципи прозорості та справедливості, викладені в [17, 18], вимагають, щоб висока швидкість інференсу не досягалася ціною алгоритмічного упередження. Мінімізація ризиків сегрегації учнів реалізується через багатокомпонентну функцію втрат (11):

$$Loss = \lambda_1 L_{accuracy} + \lambda_2 L_{fairness} + \lambda_3 L_{privacy}, \quad (11)$$

де $L_{accuracy}$ — стандартна помилка прогнозування (точність); $L_{fairness}$ — штраф за нерівність у прогнозах для різних демографічних груп; $L_{privacy}$ — компонент, що відповідає за збереження приватності (наприклад, через диференційну приватність); $\lambda_{1,2,3}$ — вагові коефіцієнти, що визначають баланс між ефективністю та етичністю.

Надмірна автоматизація, навіть за високої технічної стабільності, несе загрозу когнітивної гетерономії [19, 20]. Отже, впровадження НМ в Україні має супроводжуватися розробкою етичних регламентів, які гарантують, що ШІ залишається підсилювачем людських можливостей, а не інструментом для деградації критичного мислення.

Висновки

Комплексне наукове обґрунтування та емпірична валідація, проведені в цьому дослідженні, підтверджують, що оптимізація освітніх траєкторій у ресурсообмежених інфокомунікаційних середовищах безпосередньо залежить від архітектурного синтезу нейронних мереж. Порівняльний аналіз встановив, що хоча монолітні моделі Трансформерів забезпечують краще семантичне розуміння, їхня квадратична обчислювальна складність $O(N^2)$ та масивний обсяг пам'яті (заповнення 91,4 % бюджету *VRAM* об'ємом 1 ГБ лише вагами) роблять їх непридатними для масового розгортання на учнівському обладнанні початкового рівня. Навпаки, синтезована композитна архітектура (*LSTM+GNN*) використовує переваги лінійної складності $O(N)$ рекурентних блоків та топологічну ефективність графових згорток, досягаючи функційного балансу між предиктивною точністю та експлуатаційною стабільністю.

Експериментальні результати надають вагомі докази технічної переваги гібридного підходу в реальних сценаріях. Зафіксоване 14-кратне скорочення затримки інференсу на *GPU* (з 86,4 мс до 6,1 мс) та 20-кратне зниження споживання відеопам'яті є не просто кількісними покращеннями, а якісними зрушеннями, які дають змогу створювати інтерактивні освітні сервіси в реальному часі на споживчих ноутбуках. Важливо, що композитна модель повністю обійшла помилки *CUDA Out-of-Memory* та термальний тротлінг (78° C проти 54° C), які катастрофічно погіршували продуктивність базової монолітної моделі. Ці висновки свідчать, що для великомасштабних освітніх платформ композитні архітектури є єдиним життєздатним шляхом до забезпечення доступності системи без постійної залежності від централізованої хмарної інфраструктури.

Технічно інтеграція таких моделей безпосередньо відповідає стратегічним потребам українського освітнього сектору. Продемонстроване зниження енергоспоживання на 46 % та здатність ефективно функціонувати на локальних пристроях користувачів створюють основу для когнітивної стійкості під час періодів нестабільності інфраструктури або повної втрати зв'язку. Застосування методів крослінгвальних ембедінгів додатково долає розрив у ресурсах між глобальними англомовними знаннями та локальним українським контентом, гарантуючи, що технічна оптимізація не відбувається за коштом культурної чи лінгвістичної валідності.

З етичної та епістемологічної точки зору, перехід до композитних архітектур сприяє впровадженню принципів «*Privacy by Design*». Завдяки забезпеченню високопродуктивної обробки на 1 ГБ відеопам'яті, запропонована система дає змогу конфіденційним когнітивним профілям залишатися на пристрої користувача, мінімізуючи ризики витоку даних та спостереження. Крім того, притаманна графовим нейронним мережам інтерпретованість пропонує рішення дилеми «чорної скриньки» глибокого навчання, даючи змогу освітянам розуміти структурну логіку алгоритмічних рекомендацій. Підсумовуючи, синтез композитних архітектур є людиноцентричною технологічною еволюцією, яка пріоритезує стабільність, автономність та етичну підзвітність, гарантуючи, що штучний інтелект виступає надійним когнітивним підсилювачем як для учнів, так і для вчителів у цифрову епоху.

ПОВІДОМЛЕННЯ

Внесок авторів: Під час підготовки цієї статті автори використовували велику мовну модель *Gemini* 3.1 *Pro*. Інструмент застосовувався як допоміжний засіб для структурування матеріалу, стилістичного редагування тексту та допомоги у формулюванні окремих тез. Після використання систем штучного інтелекту автор ретельно перевірив і відредагував згенерований контент. Автори беруть на себе повну відповідальність за кінцевий зміст і достовірність поданої роботи.

ЛІТЕРАТУРА / REFERENCES

1. Mukul E., Büyüközkan G. Digital transformation in education: A systematic review of education 4.0. *Technological Forecasting and Social Change*, 2023, Vol. 194, Article. 122664. https://doi.org/10.1016/j.techfore.2023.122664
2. Vakhabova A.S., Kosulin V.V., Zizaeva A.A. Artificial intelligence in education: Challenges and opportunities for sustainable development. *Economics and Management Problems Solutions*, 2025, Vol. 158, 173-179. https://doi.org/10.36871/ek.up.p.r.2025.05.09.020
3. Pinchuk O.P., Malytska I.D. Responsible and ethical use of artificial intelligence in scientific research and publications. *Information Technologies and Learning Tools*, 2024, Vol. 100 (2), 180–198. [In Ukrainian: Пінчук О.П., Малицька І.Д. Відповідальне та етичне використання штучного інтелекту в наукових дослідженнях та публікаціях] https://doi.org/10.33407/itlt.v100i2.5676

4. Zawacki-Richter O., Marín V.I., Bond M., Gouverneur F. Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education*, 2019, Vol. 16, Article 39. https://doi.org/10.1186/s41239-019-0171-0
5. Vaswani A. Attention Is All You Need. *Advances in Neural Information Processing Systems (NIPS)*, 2017, Vol. 30, 5998–6008. https://doi.org/10.48550/arXiv.1706.03762
6. LeCun Y., Bengio Y., Hinton G. Deep learning. *Nature*, 2015, Vol. 521, 436–444. https://doi.org/10.1038/nature14539
7. Makohon Y.O. Use of neural network structures for anomaly detection in cyberspace. *Proc. Intern. Sci. Conf. ICTC-2025*, NURE, Kharkiv, 2025, pp. 306–307. [In Ukrainian: Макогон Ю.О. Використання нейромережевих структур для виявлення аномалій у кіберпросторі]
8. Chen X., Xie H., Zou D., Hwang G.J. Application and theory gaps during the rise of Artificial Intelligence in Education. *Computers and Education: Artificial Intelligence*, 2020, Vol. 1, Article 100002. https://doi.org/10.1016/j.caeai.2020.100002
9. Scarselli F. The Graph Neural Network Model. *IEEE Transactions on Neural Networks*, 2009, Vol. 20 (1), 61–80. https://doi.org/10.1109/TNN.2008.2005605
10. Jobin A., Ienca M. The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 2019, Vol. 1, 389–399. https://doi.org/10.1038/s42256-019-0088-2
11. Graves A., Mohamed A., Hinton G. Speech recognition with deep recurrent neural networks. *IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, 6645–6649. https://doi.org/10.1109/ICASSP.2013.6638947
12. Wu Z. A Comprehensive Survey on Graph Neural Networks. *IEEE Transactions on Neural Networks and Learning Systems*, 2021, Vol. 32 (1), 4–24. https://doi.org/10.1109/TNNLS.2020.2978386
13. Knox J. Artificial intelligence and education in China. *Learning, Media and Technology*, 2020, Vol. 45 (3), 298–311. https://doi.org/10.1080/17439884.2020.1754236
14. Marienko M.V., Kovalenko V.V. Artificial intelligence and open science in education. *Physical and Mathematical Education*, 2023, No. 38(1), 48-53. [In Ukrainian: Марієнко М.В., Коваленко В.В. Штучний інтелект та відкрита наука в освіті] https://doi.org/10.31110/2413-1571-2023-038-1-007
15. Crompton H., Bernacki M., Greene J.A. Psychological foundations of emerging technologies for teaching and learning in higher education. *Current Opinion in Psychology*, 2020, Vol. 36, 101–105. https://doi.org/10.1016/j.copsyc.2020.04.011
16. Bahdanau D., Cho K., Bengio Y. Neural Machine Translation by Jointly Learning to Align and Translate. *International Conference on Learning Representations (ICLR)*, 2015. https://doi.org/10.48550/arXiv.1409.0473
17. Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review*, 2019, Vol. 1 (1). https://doi.org/10.1162/99608f92.8cd550d1
18. Hochreiter S., Schmidhuber J. Long Short-Term Memory. *Neural Computation*, 1997, Vol. 9 (8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735
19. Roll I., Wylie R. Evolution and Revolution in Artificial Intelligence in Education. *International Journal of Artificial Intelligence in Education*, 2016, Vol. 26, 582–599. https://doi.org/10.1007/s40593-016-0110-3
20. Siemens G. Learning Analytics: The Emergence of a Discipline. *American Behavioral Scientist*, 2013, Vol. 57 (10), 1380–1400. https://doi.org/10.1177/0002764213498851

Отримано / Received 05.01.2026
Прийнято / Accepted 09.06.2026
Опубліковано / Published 25.08.2026

Yu.O. MAKOHON, PhD Sudent,
Kharkiv National University of Radioelectronics,
14, Nauky ave., Kharkiv, 61166, Ukraine
https://orcid.org/0009-0005-4369-1555; yurii.makohon@nure.ua

O.H. RUDENKO, DSc (Engineering), Professor,
Kharkiv National University of Radioelectronics,
14, Nauky ave., Kharkiv, 61166, Ukraine
https://orcid.org/0000-0003-0859-2015; oleh.rudenko@nure.ua

ARCHITECTURAL SYNTHESIS OF COMPOSITE NEURAL NETWORK SYSTEMS FOR PREDICTIVE DATA PROCESSING IN DIGITAL EDUCATIONAL ENVIRONMENTS

Introduction. The ongoing digital transformation of global educational environments necessitates the deployment of intelligent frameworks capable of real-time optimization of individual learning pathways. Neural networks (NN) have emerged as primary technological drivers in this process, providing advanced predictive analytics of learning activities. However, the increasing parametric complexity of modern monolithic architectures, such as Transformers, creates significant technical barriers for their widespread use on entry-level student hardware (laptops and tablets). In the Ukrainian context, where infrastructure instability often limits access to reliable high-performance cloud resources, the synthesis of lightweight yet highly accurate composite models capable of local data processing is a critical strategic requirement.

The purpose of the paper is to substantiate the methodological and technical principles for synthesizing composite neural network architectures (integrating RNN, GNN, and Transformers) to intensify adaptive learning processes and ensure stable predictive data processing in resource-constrained environments.

Methods. The study employs a formal framework of non-linear dynamic systems to model student cognitive progress. The architectural synthesis involves a modular task decomposition strategy: temporal dynamics are managed by LSTM blocks, structural knowledge dependencies are captured by GCN layers, and semantic interactions are processed via self-attention mechanisms. Experimental validation was conducted on a laptop equipped with consumer-grade hardware (Intel i5-1135G7 CPU, NVIDIA MX350 GPU) with programmatically restricted video memory (1 GB) to simulate multitasking environments. Performance metrics included high-precision latency counters, hardware monitoring via NVML, and predictive accuracy assessment using AUC ROC.

Results. Theoretical FLOPs analysis indicated that the proposed composite architecture requires 18–20 times fewer floating-point operations than monolithic Transformer baselines. For a sequence length of $N = 512$, calculating the Self-Attention mechanism requires approximately $2 \times N^2 \times d$ operations (covering both OK^T and V). In contrast, the LSTM-based composite requires $O(N \times (8dh))$ operations, providing massive efficiency gains. Empirical testing recorded a 14-fold reduction in GPU inference latency (from 86.4 ms down to 6.1 ms) and a 20-fold reduction in the memory footprint. The architecture successfully bypassed CUDA Out-of-Memory errors and prevented thermal throttling, maintaining a stable GPU operating temperature (54° C vs 78° C).

Conclusions. The optimization of educational trajectories is strictly dependent on the architectural synthesis of neural networks. Monolithic models are often impractical for local use due to their $O(N^2)$ complexity and high memory consumption. Composite ensembles provide a necessary balance between predictive precision and operational stability. The ability to process data locally on user devices ensures both educational continuity during infrastructure instability and data privacy by design. These findings establish that hybrid, resource-efficient architectures are the most viable path for creating sustainable, human-centric educational ecosystems in the digital era.

Keywords: *adaptive learning, composite neural network architectures, infocommunication systems, predictive data processing, personalization, local computing, artificial intelligence.*

https://doi.org/10.15407/intechsys.2026.03.015
УДК 004.274

О.О. БАРКАЛОВ, д-р. техн. наук, професор,
Зеленогурський Університет,
вул. Ліцеальна, 9, Зелена Гура, Польща
https://orcid.org/ orcid.org/0000-0002-4941-3979
A.Barkalov@iie.uz.zgora.pl
Л.О. ТІТАРЕНКО, д-р. техн. наук, професор,
Зеленогурський Університет,
вул. Ліцеальна, 9, Зелена Гура, Польща
Харківський національний університет радіоелектроніки,
пр. Науки, 14, м. Харків, 61166, Україна
https://orcid.org/0000-0001-9558-3322
L.Titarenko@iie.uz.zgora.pl
О.В. МАТВІЄНКО, наук. співроб.,
Інститут кібернетики імені В.М. Глушкова НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0000-0003-1838-1422
avmatv@ukr.net

СИНТЕЗ КОМПОЗИЦІЙНОГО МІКРОПРОГРАМНОГО ПРИСТРОЮ КЕРУВАННЯ З ДВОМА ЯДРАМИ ЧАСТКОВИХ ФУНКЦІЙ

Запропоновано метод структурної декомпозиції схеми композиційного мікропрограмного пристрою управління (КМПУ) у базисі FPGA. Метод ґрунтується на виділенні двох ядер часткових функцій. Одне з ядер генерує функції, у яких число аргументів перевищує кількість входів елементів LUT. Друге ядро генерує функції, що базуються на кодуванні операторних лінійних ланцюгів. Запропоновано архітектуру КМПУ з двома ядрами часткових функцій та метод синтезу схеми КМПУ. Розглянуто приклад синтезу схеми КМПУ із двома ядрами. Розглянуто умови застосування цього підходу. Показано можливі шляхи вирішення оптимізаційних завдань, пов'язаних з дисбалансом характеристик алгоритму управління та елементів LUT.

Ключові слова: *часткова функція, ядро, КМПУ, LUT, EMB, синтез, структурна декомпозиція.*

Цитування: Баркалов О.О., Тітаренко Л.О., Матвієнко О.В. Синтез композиційного мікропрограмного пристрою керування з двома ядрами часткових функцій. *Information Technologies and Systems*, Київ, 2026, Том 3 (9), 15–29. https://doi.org/10.15407/intechsys.2026.03.015

Вступ

Композиційні мікропрограмні пристрої управління [1, 2] є ефективним засобом реалізації лінійних алгоритмів керування [2]. У процесі проєктування КМПУ постає проблема оптимізації характеристик його схеми. До таких характеристик відносяться апаратурні витрати, швидкодія та споживана потужність [3]. Методи вирішення проблеми залежать від особливостей елементного базису. У цій роботі розглядається реалізація схеми КМПУ в базисі *FPGA* (*field-programmablelogicalarray*) [4].

Вибір базису *FPGA* обумовлений широким його застосуванням під час реалізації цифрових систем [5]. На думку експертів [6] *FPGA* будуть популярними ще кілька десятиліть. Цим обумовлена актуальність розробки схем у базисі *FPGA*.

Пропонований метод може бути застосовано за необхідності функціональної декомпозиції [7, 8] схеми адресації мікрокоманд (МК). Ми розглядаємо ситуацію, коли частина схеми заснована на функціональній, а друга частина — на структурній декомпозиції [9]. Будь-яка декомпозиція цифрового пристрою пов'язана з формуванням систем часткових функцій (СЧФ) [10]. Ми пропонуємо використовувати два ядра СЧФ.

У статті розглядається КМПУ із загальною пам'яттю [1]. Для оптимізації схеми використовують метод перетворення адрес виходів операторних лінійних ланцюгів (ОЛЛ) [11] Алгоритм управління подано як граф схема алгоритму (ГСА) [12].

Особливості КМПУ та базису *FPGA*

Синтез КМПУ починається з формування ОЛЛ, що утворюють множину $C = \{\alpha_1, \ldots, \alpha_G\}$ [1]. Кожна ОЛЛ є вектором, який складається з операторних вершин ГСА Г. У кожній ОЛЛ $\alpha_g \in \tilde{N}$ вершини розташовуються у тому ж порядку, що і в ГСА Г. У ГСА Г виділяються множина операторних вершин $B = \{b_1, \ldots, b_M\}$ і множина умовних вершин, що складається з *NC* елементів. ГСА є лінійною в разі виконання умови [2]

$$M \geq 0{,}75(M + NC). \tag{1}$$

Кожна вершина $b_m \in B$ відповідає мікрокоманді Y_m. Мікрокоманди Y_m зберігаються у керувальній пам'яті (КП) КМПУ. Розрядність адрес мікрокоманд визначається як

$$R = \lceil \log_2 M \rceil. \tag{2}$$

Кожна умовна вершина містить одну логічну умову $x_l \in X$, де $X = \{x_1, \ldots, x_L\}$. В цьому разі може виконуватися умова $L < NC$. Кожна ОЛЛ має лише один вихід o_g (остання вершина в ОЛЛ). МК Y_m має адресу A_m розрядності R.

Адресація МК здійснюється наступним чином. Нехай ОЛЛ $\alpha_g \in \tilde{N}$ охоплює пару вершин $< b_i, b_j >$, де вихід вершини b_i пов'язаний з входом вершини b_j. У цьому разі маємо залежність між адресами A_i та A_j [2]:

$$A_j = A_i + 1. \qquad (3)$$

Як випливає з (3), для зберігання адрес необхідно використовувати лічильник адреси (ЛА). Виходи ЛА утворюють множину адресних змінних $T = \{T_1, \ldots, T_R\}$.

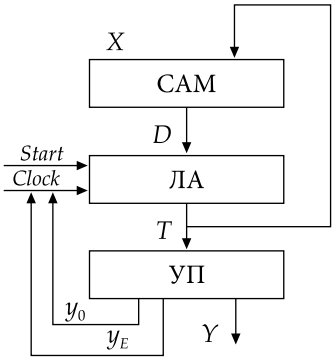


Рис. 1. Структурна схема КМПУ U_1

Будемо використовувати ЛА з інформаційними входами типу *D*. Для зміни адреси в ЛА, відмінної від (3), необхідно використовувати функції збудження пам'яті (ФЗП), що утворюють множину $D = \{D_1, \ldots, D_R\}$. При цьому адреса переходу, що відмінна від (3), визначається схемою адресації мікрокоманд (САМ). Ця схема реалізується з урахуванням СБФ:

$$D = D(T, X). \qquad (4)$$

Таким чином, у КМПУ використовуються два режими адресації. Для їх вибору використовується додаткова функція $y_O \notin Y$, де $Y = \{y_1, \ldots, y_N\}$ — множина мікрооперацій. Нехай $y_O = 1$ визначає режим (3), а $y_O = 0$ — режим (4).

Процес функціонування КМПУ починається під час надходження імпульсу *Start*. Зміна вмісту КП дозволяється за певним фронтом імпульсу синхронізації *Clock*. Функціонування завершується блокуванням сигналу *Clock* змінною y_E. На основі цієї інформації можна одержати КМПУ U_1 (рис. 1).

КМПУ U_1 отримав назву КМПУ із загальною пам'яттю [1, 2]. Схема функціонує в такий спосіб. За сигналом *Start* у ЛА записується початкова адреса мікропрограми. Схема САМ генерує СБФ (4). Адреси записуються до ЛА. Чергова мікрокоманда вибирається із КП. Сигнали y_o та y_E визначають режими адресації та зупинки.

Лічильник є стандартним пристроєм, і його реалізація не викликає труднощів. Схема КП будується на стандартних блоках пам'яті. Проблеми виникають під час реалізації блоку САМ. Ці проблеми пов'язані з тим, що САМ не є стандартним блоком. Його схема залежить від системи (4). У статті пропонується метод вирішення цієї проблеми за використання внутрішніх ресурсів мікросхем *FPGA*.

Блок САМ із лічильником утворюють послідовну схему [5]. Для її реалізації необхідні такі ресурси мікросхеми *FPGA*:

- елементи табличного типу *LUT* (*look-uptable*), що мають S_L входів та один вихід;
- програмовані синхронні тригери із входом скидання у 0;
- програмовані міжз'єднання.

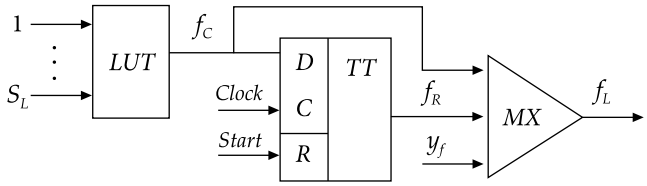


Рис. 2. Спрощена схема логічного елемента

Елементи *LUT* та тригера утворюють логічні елементи (ЛЕ). Декілька ЛЕ утворюють блок *CLB* (*ConfigurableLogicBlock*). Ускладі *CLB* є система швидких міжз'єднань [13]. З'єднання між *CLB* є повільнішими, ніж усередині *CLB*. На рис. 2 наведено схему ЛЕ.

ЛЕ має S_L входів і один вихід f_L. Елемент *LUT* зберігає таблицю істинності [14] довільної булевої функції, що має не більше S_L аргументів. Вихід *LUT* f_C пов'язаний із входом *D* тригера. За сигналом *Clock* комбінаційний сигнал f_C перетворюється на регістровий сигнал f_R. Вихід f_L може бути комбінаційним, або регістровим. Для вибору типу виходу використовується мультиплексор *MX* та сигнал y_f. Сигнал *Start* надходить на вхід скидання тригера у 0.

Таким чином, *CLB* може реалізовувати як комбінаційні схеми, так і схеми, що накопичують. Для реалізації швидких лічильників може бути використана внутрішня система прискорених переносів *CLB*.

Пам'ять КП реалізується за допомогою вбудованих блоків пам'яті *EMB* (*Embedded Memory Blocks*) [15, 16]. Ці блоки мають властивість реконфігурації [17]: число входів (S_A) та виходів (t_F) можна змінювати при збереженні постійної ємності V_0: $V_0 = 2^{S_A} t_F$.

Для реалізації пам'яті необхідно вибрати конфігурацію $< S_A, t_F >$, для якої

$$S_A = R. \tag{5}$$

Якщо такої конфігурації не існує, немає сенсу у використанні моделі КМПУ. При порушенні (5) КП повинна мати кілька рівнів блоків та дешифратор вибору рівня [16]. В результаті схема КП стає громіздкою, повільною та має значне енергоспоживання.

Якщо умова (5) виконується, схеми САМ і ЛА реалізуються на ЛЕ, а КП — на блоках *EMB*. Позначимо символом *LUTer* (*EMBer*) схему, що складається з кількох блоків *LUT* (*EMB*). Тоді отримаємо таку схему *F*-КМПУ U_1 (рис. 3).

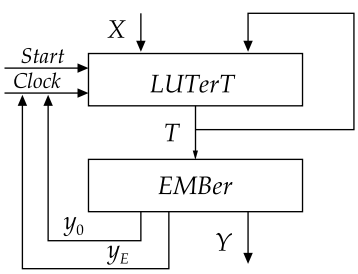


Рис. 3. Структурна схема *F*-КМПУ U_1

Позначання «*F*-КМПУ» підкреслює, що схема реалізована в базисі *FPGA*. Блок *LUTerT* містить блоки САМ і ЛА зі схеми на рис. 1

Кожна функція $D_r \in D$ подається диз'юнктивною нормальною формою (ДНФ), яка має NA_r аргументів. При

цьому L_r аргументів представляють логічні умови, а $NA_r \in L_r$ аргументів — адресні змінні $T_r \in T$. У статті розглядається випадок, коли для деяких ФЗП виконуються умови:

$$NA_r > S_L, \tag{6}$$

$$L_r \in S_L. \tag{7}$$

В цьому разі блок *LUTerT* має кілька рівнів елементів *LUT* та складну систему міжз'єднань. Такі схеми реалізуються за допомогою методів функціональної декомпозиції. Відомо, що ці методи призводять до схем з малою швидкодією та великим споживанням потужності. У цій статті пропонується метод покращення характеристик КМПУ в разі виконання умов (6), (7).

Ідея запропонованого методу

Побудуємо множину ОЛЛ $C = \{\alpha_1, \ldots, \alpha_G\}$ для деякої ГСА Г. Знайдемо множину виходів ОЛЛ $O(\Gamma)$. Визначимо число ЛУ L_g, що задають переходи з виходів ОЛЛ $\alpha_g \in \tilde{N}$. Якщо виконується умова:

$$L_g \in S_L, \tag{8}$$

вихід o_g розміщується у множину O_V, інакше — у множину O_T. Очевидно, що $O_V \cup O_T = O(\Gamma)$ і $O_V \cap O_T = \varnothing$. Закодуємо виходи $o_g \in O_V$ кодами $K(o_g)$. Число змінних, необхідних для кодування виходів, визначається виразом:

$$R_V = \lceil \log_2(|O_V| + 1) \rceil. \tag{9}$$

Для кодування виходів використовуються змінні $v_r \in V$, де $|V| = R_V$. У (9) одиниця додається для врахування співвідношення $o_g \notin O_V$.

Множина $O_V \subseteq O(\Gamma)$ визначає дві множини. Одна з них — множина X_V логічних умов, що задає переходи з виходів $o_g \notin O_V$. Друга — множина D_V, функцій збудження пам'яті, що формуються при переходах з виходів $o_g \notin O_V$. Клас O_V визначає блок *LUTerF*, схема якого задається СБФ:

$$D_V = D_V(V, X_V). \tag{10}$$

Множина O_T розбивається на класи, $O^k \in \Pi_O$, де $\Pi_O = \{O^1, \ldots, O^K\}$. Клас O^k складається з M_k виходів. Ці виходи кодуються частковими кодами $C(o_g)$, що мають R_k розрядів:

$$R_k = \lceil \log_2(M_k + 1) \rceil. \tag{11}$$

Код, що складається з R_k нулів, використовується для співвідношення $o_g \notin O^k$. Для кодування використовуються змінні $\tau_r \in \tau^k$, де $|\tau^k| = R_k$.

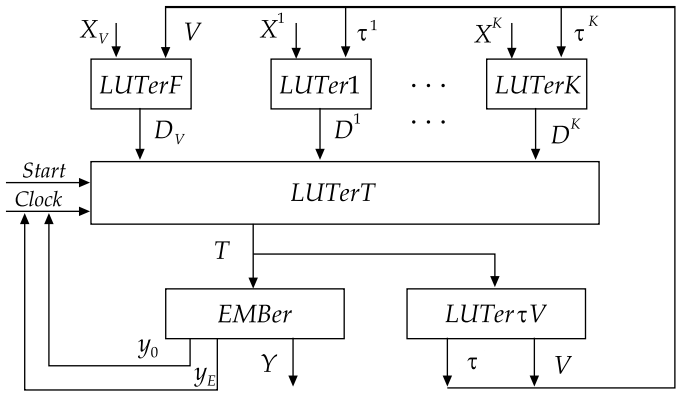


Рис. 4. Структурна схема *F*-КМПУ U_2

Кожен клас $O^k \in \Pi_O$ визначає множини D^k і X^k, які є аналогами множин D_V і X_V відповідно. Клас $O^k \in \Pi_O$ визначає блок *LUTerk*, що представляється СБФ:

$$D^k = D^k(\tau^k, X^k). \tag{12}$$

Остаточні значення ФЗП задаються СБФ:

$$D = D(D_V, D^1, D^2, ..., D^K). \tag{13}$$

Кожна функція $D_r \in D$ представлена системою диз'юнкцій $D_r = D_r^V \vee D_r^1 \vee D_r^2 \vee ... \vee D_r^K$.

Додаткові змінні $v_r \in V$ і $\tau_r \in \tau$ задаються наступними СБФ:

$$V = V(T); \tag{14}$$

$$\tau = \tau(T). \tag{15}$$

Система (13) визначає функціональний асемблер *LUTerT*. Функції (14) — (15) визначають блок перетворювача адрес МК *LUTerτV*. Мікрокоманди та додаткові функції y_0 та y_E зберігаються в КП, представленій блоком *EMBer*. Всі ці блоки визначають архітектуру *F*-КМПУ U_2 (рис. 4).

КМПУ U_2 функціонує у такій послідовності. Сигнал *Start* ініціює запис нульової адреси до ЛА. Ця адреса надходить до *EMBer*. Залежно від режиму адресації формується змінна $y_0 = 1$ або $y_0 = 0$. У першому випадку адреса визначається рівнянням (3). Для формування адреси переходу блок САМ не використовується. Якщо код виходу $y_0 = 0$, ОЛЛ формується блоком *LUTerτV*. В результаті один із блоків першого рівня логіки (*LUTerF, LUTer*1, …, *LUTerK*) формує часткові ФЗП, які надходять у блок *LUTerT* і перетворюються на функції $D_r \in D$. Ці функції надходять на входи тригерів лічильника всередині блоку *LUTerT*. За певним фронтом *Clock* функції $D_r \in D$ перетворюються на адресні змінні $T_r \in T$.

Функціонування продовжується до формування сигналу y_E. Цей сигнал блокує надходження сигналів синхронізації до ЛА. Після цього стан ЛА не змінюється (ФЗП не може змінити адресу).

У статті пропонується метод синтезу схеми *F*-КМПУ U_2. Метод містить такі етапи:

1. Формування множини ОЛЛ за ГСА Г.
2. Розбиття множини O(Г) на множини O_V і O_T.
3. Природна адресація МК у межах кожної ОЛЛ $\alpha_g \in \tilde{N}$.
4. Кодування виходів $o_g \in O_V$ частковими кодами $K(o_g)$.
5. Формування таблиці блоку *LUTerF* та СБФ (10).
6. Розбиття множини виходів O_T на класи $O^k \in \Pi_O$.
7. Кодування виходів $o_g \in O^k$ частковими кодами $C(o_g)$.
8. Формування таблиці блоків $LUTer1 - LUTerK$ і СБФ (12).
9. Формування таблиці блока *LUTerT* і СБФ (13).
10. Формування таблиці блока *LUTerτV* і СБФ (14) — (15).
11. Формування таблиці блока *EMBer*.
12. Реалізація схеми КМПУ U_2 з використанням внутрішніх ресурсів мікросхеми *FPGA*.

Далі наведено приклад синтезу КМПУ U_2. Ми не розглядаємо крок остаточної реалізації, оскільки він вимагає використання таких пакетів САПР, як *Vivado* [18] або *Quartus* [19].

Приклад синтезу схеми КМПУ

Нехай алгоритм управління представлений ГСА Γ_1 (рис.5). Нехай для реалізації схеми використовуються елементи *LUT* із числом входів S_L = 4 та блоки *EMB* із конфігурацією < 5, 8 >. Такий блок *EMB* може зберігати до 32 МК, що мають не більше восьми розрядів.

Як випливає з рис. 5, ГСА Γ_1 має M = 18 операторних вершин. Таким чином, маємо множину $B = \{b_1, ..., b_{18}\}$. Використовуючи (2), отримаємо R = 5. Умова (5) виконується. Аналіз ГСА Γ_1 дозволяє знайти множини $X = \{x_1, ..., x_4\}$ і $Y = \{y_1, ..., y_6\}$, при цьому N + 2 = 8. Отже достатньо одного блоку *EMB* для реалізації схеми КП. Оскільки R = 5, маємо множини $T = \{T_1, ..., T_5\}$ і $D = \{D_1, ..., D_5\}$.

Використовуючи методику з [1], побудуємо множину ОЛЛ $C = \{\alpha_1, ..., \alpha_7\}$, де $\alpha_1 = < b_1, b_2 >$, $\alpha_2 = < b_3, b_4, b_5 >$, $\alpha_3 = < b_6, b_7, b_8 >$, $\alpha_4 = < b_9, b_{10}, b_{11} >$, $\alpha_5 = < b_{12}, b_{13}, b_{14} >$, $\alpha_6 = < b_{15}, b_{16} >$, $\alpha_7 = < b_{17}, b_{18} >$. Оскільки G = 7, то множина $O(\Gamma_1) = \{o_1, ..., o_7\}$. Ці виходи відповідають наступним вершинам: $o_1 = b_2$, $o_2 = b_5$, $o_3 = b_8$, $o_4 = b_{11}$, $o_5 = b_{14}$, $o_6 = b_{16}$, $o_7 = b_{18}$.

Для синтезу схеми використовуються *LUT*з S_L = 4. Очевидно, що умова (8) виконується для виходу o_1. З цього аналізу отримуємо множини $O_V = \{o_1\}$ і $O_T = \{O_2, ..., O_7\}$.

Використовуючи методику з [1], знайдемо адреси МК. Для нашого прикладу маємо: $A(b_1) = 00000$, $A(b_2) = 00001$, ..., $A(b_{18}) = 10001$.

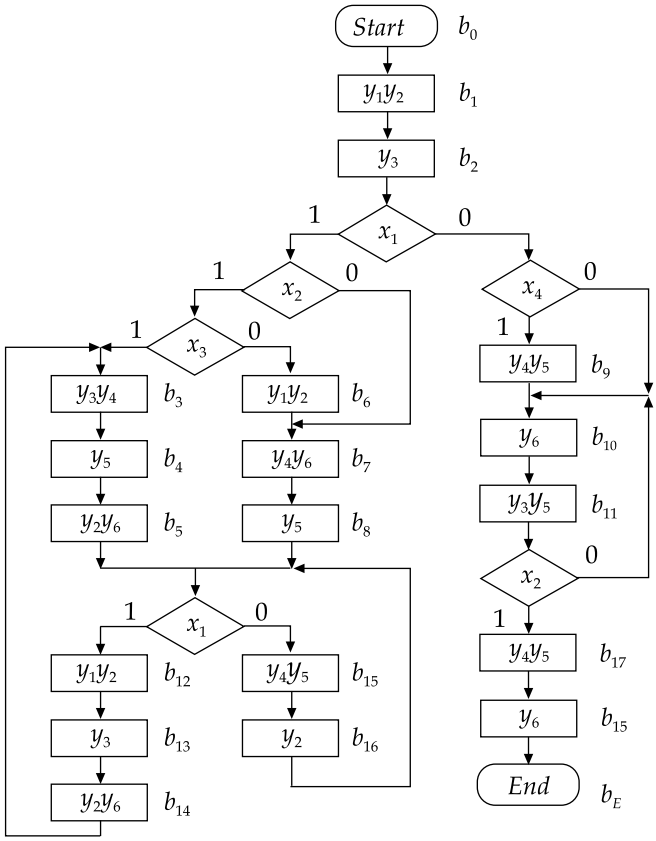


Рис. 5. Граф-схема алгоритма Γ_1

Вочевидь, умова (3) виконується для кожної пари сусідніх компонент всіх ОЛЛ $\alpha_g \in \tilde{N}$.

Оскільки $O_V = \{o_1\}$, то $M_V = |O_V| = 1$. З рівняння (9) отримаємо R_V=1, що дає $V = \{v_1\}$. Закодуємо вихід o_1 кодом $K(o_1) = 1$.

Побудуємо формулу переходу для виходу o_1 [12]:

$$b_2 \to x_1x_2x_3b_3 \vee x_1x_2\overline{x_3}b_6 \vee x_1\overline{x_2}b_7 \vee \overline{x_1}x_4b_9 \vee \overline{x_1}\,\overline{x_4}b_{10}\,. \qquad (16)$$

Ця формула визначає таблицю блоку *LUTerF*. Таблиця має стовпці o_g, $K(o_g)$, b_m, $A(b_m)$, X_h, D_h, h. Стовпець b_m містить вершини формули переходу, стовпець $A(b_m)$, складається з адрес МК. Стовпець X_h включає кон'юнкції логічних умов, що визначають переходи. Стовпець D_h складається з ФЗП, що дорівнюють одиниці для запису в ЛА адреси $A(b_m)$. Для прикладу блок *LUTerF* поданий табл.1.

Число рядків у табл.1 дорівнює числу термів у формулі (16). Принцип формування інформації в стовпцях b_m — D_h є очевидним.

Таблиця блоку *LUTerF* є основою формування СБФ (10). Щоб підкреслити, що ці часткові ФЗП формуються блоком *LUTerF*, ми використовуємо верхній індекс «0». Для нашого прикладу з табл. 1

отримані такі функції:

$$D_1^0 = 0; \quad D_2^0 = v_1\overline{x_1}; \quad D_3^0 = v_1 x_1;$$
$$D_4^0 = v_1 x_1 \overline{x_2} \vee v_1 \overline{x_1 x_4}; \quad D_5^0 = v_1 x_1 x_2 \overline{x_3}.$$

Для пошуку розбиття Π_O використовується методика з робіт [20, 21]. Розбиття виконується так, щоб для кожного класу $O^k \in \Pi_O$ виконувалася умова $R_k + L_k \le S_L$. Крім того, кількість класів K сумісних виходів має бути мінімальною.

Для нашого прикладу отримуємо розбиття $\Pi_O = \{O^1, O^2\}$ із числом класів K = 2. Кожен клас має M_k = 3 виходів: $O^1 = \{o_2, o_3, o_6\}$ і $O^2 = \{o_4, o_5, o_7\}$. Використовуючи (11), отримаємо $R_1 = R_2 = 2$, $\tau^1 = \{\tau_1, \tau_2\}$, $\tau^2 = \{\tau_3, \tau_4\}$, $\tau = \{\tau_1, \ldots, \tau_4\}$.

Закодуємо співвідношення $o_g \notin O^k$ кодом 00, а виходи — природним способом: $C(o_2) = C(o_4) = 01$, $C(o_3) = C(o_5) = 10$ и $C(o_6) = C(o_7) = 11$. Використовуючи ці часткові коди, адреси МК та формули переходу між вершинами ГСА Γ_1, отримаємо таблиці блоків *LUTer*1 та *LUTer*2.

З ГСА Γ_1 маємо такі дві системи формул переходів:

$$o_2, o_3, o_6 \to x_1 b_{12} \vee \overline{x_1} b_{15}, \tag{17}$$

$$o_4 \to x_2 b_7 \vee \overline{x_2} b_{10}; \; o_5 \to b_3; \; o_7 \to b_E. \tag{18}$$

Система (17) визначає таблицю блоку *LUTer*1 (табл. 2). Система (18) визначає таблицю блоку *LUTer*2 (табл. 3). Ці таблиці мають такі самі стовпці, як і табл. 1, тільки стовпець $K(o_g)$ замінюється стовпцем $C(o_g)$.

З табл. 2 формується наступна СБФ:

$$D_1^1 = 0; \quad D_2^1 = \tau_1 \vee \tau_2; \quad D_3^1 = \tau_2 \overline{x_1} \vee \tau_1 \overline{x_1};$$
$$D_4^1 = \tau_1 x_1 \vee \tau_2 x_1; \quad D_5^1 = D_2^1, \tag{19}$$

Таблиця 1. **Таблиця блока *LUTerF***

o_g	$K(o_g)$	b_m	$A(b_m)$	X_h	D_h	h
o_1	1	b_3	00010	$x_1 x_2 x_3$	D_4	1
		b_6	00101	$x_1 x_2 \overline{x_3}$	$D_3 D_5$	2
		b_7	00110	$x_1 \overline{x_2}$	$D_3 D_4$	3
		b_9	01000	$\overline{x_1} x_4$	D_2	4
		b_{10}	01001	$\overline{x_1 x_4}$	$D_2 D_4$	5

Таблиця 2. **Таблиця блока *LUTer*1**

o_m	$C(o_m)$	b_m	$A(b_m)$	X_h	D_h	h
o_2	01	b_{12}	01011	x_1	$D_2 D_4 D_5$	1
		b_{15}	01101	$\overline{x_1}$	$D_2 D_3 D_5$	2
o_3	10	b_{12}	01011	x_1	$D_2 D_4 D_5$	3
		b_{15}	01101	$\overline{x_1}$	$D_2 D_3 D_5$	4
o_6	11	b_{12}	01011	x_1	$D_2 D_4 D_5$	5
		b_{15}	01101	$\overline{x_1}$	$D_2 D_3 D_5$	6

а з табл. 3 — СБФ:

$$D_1^2 = 0; \quad D_2^2 = D_5^2 = \overline{\tau_3}\tau_4\overline{x_2};$$
$$D_3^2 = \overline{\tau_3}\tau_4 x_2; \quad D_4^2 = \tau_3\overline{\tau_4}. \tag{20}$$

У системах (19)—(20) верхній індекс відповідає номеру блока *LUTerk*. Система (19) використовується для реалізації блока *LUTer*1, система (20) —блока *LUTer*2.

Блок *LUTerT* представляється таблицею зі стовпцями $O_V, O^1, ..., O^K$ та рядками $D_1 - D_R$. Якщо $D_r^k \neq \varnothing$, то на перетині рядка D_r та стовпця O^k (або O_V) записується одиниця. У цьому прикладі блок *LUTerT* поданий табл. 4.

З табл. 4 можна отримати наступну СБФ:

$$D_1 = 0; \quad D_2 = D_2^V \vee D_2^1 \vee D_2^2; \quad D_3 = D_3^V \vee D_3^1 \vee D_3^2;$$
$$D_4 = D_4^V \vee D_4^1 \vee D_4^2; \quad D_5 = D_5^V \vee D_5^1 \vee D_5^2.$$

Ця СБФ описує схему блока *LUTerT*.

Для формування СБФ (14)—(15) необхідно побудувати таблицю блоку *LUTerτV*. Цей блок перетворює адреси МК на часткові коди $K(o_g)$ і $C(o_g)$. Таблиця має стовпці o_g, $A(b_m)$, $K(o_g)$, $C(o_g)$, V_g, τ_g, g. Стовпець V_g містить змінні $v_r \in V$, рівні одиниці у коді $K(o_g)$. Стовпець τ_g містить змінні $\tau_r \in \tau$, рівні одиниці у коді $C(o_g)$. Для нашого прикладу блок *LUTerτV* поданий табл. 5.

Таблиця 3. **Таблиця блока *LUTer*2**

o_m	$C(o_m)$	b_m	$A(b_m)$	X_h	D_h	h
o_4	01	b_7	00110	x_2	D_3D_4	1
		b_{10}	01001	$\overline{x}_2$	D_2D_5	2
o_5	10	b_3	00010	1	D_4	3
o_7	11	b_E	00000	1	—	4

Таблиця 4. **Таблиця блока *LUTerτT***

D_r	O_V	O^1	O^2
D_1	0	0	0
D_2	1	1	1
D_3	1	1	1
D_4	1	1	1
D_5	1	1	1

Таблиця 5. **Таблиця блока *LUTerτV***

o_g	$A(b_m)$	$K(o_g)$	$C(o_g)$	V_g	τ_g	g
o_1	00001	1	00	v_1	—	1
o_2	00100	0	01	—	τ_2	2
o_3	00111	0	10	—	τ_1	3
o_4	01010	0	01	—	τ_4	4
o_5	01101	0	10	—	τ_3	5
o_6	01111	0	11	—	$\tau_1\tau_2$	6
o_7	10001	0	11	—	$\tau_3\tau_4$	7

З табл. 5 маємо СБФ:

$$v_1 = \overline{T_1 T_2 T_3 T_4}; \tag{21}$$

$$\begin{aligned} &\tau_1 = \overline{T_1} T_3 T_4 T_5; \quad \tau_3 = \overline{T_1} T_2 T_3 \overline{T_4} T_5 \vee T_1 \overline{T_2 T_3 T_4} T_5; \\ &\tau_2 = \overline{T_1 T_2} T_3 \overline{T_4 T_5} \vee \overline{T_1} T_2 T_3 T_4 T_5; \quad \tau_4 = \overline{T_1} T_2 \overline{T_3} T_4 \overline{T_5} \vee T_1 \overline{T_2 T_3 T_4} T_5. \end{aligned} \tag{22}$$

Як випливає із систем (21) – (22), функції v_1, τ_1 мають по 4 змінних. Інші функції залежать від п'яти змінних. Тому схема блока *LUTerτV* має два рівні елементів *LUT*.

Таблиця блока *EMBer* містить стовпці *Адреса*, b_m, y_0, y_E, y_1, …, y_N. Заповнення таблиці проводиться на основі аналізу ГСА Г та множини $C = \{\alpha_1, ..., \alpha_G\}$. Якщо вершина b_m не є виходом ОЛЛ, за адресою $A(b_m)$ записується y_0. Якщо вершина b_m пов'язана з вершиною b_E, за адресою $A(b_m)$ записується y_E. Для нашого прикладу фрагмент вмісту КП наведено у табл. 6.

Після цього кроку отримано всю інформацію для реалізації схеми КМПУ. Зазначимо, що для системи (22) необхідно виконати функціональну декомпозицію функцій τ_2 – τ_4.

Аналіз запропонованого методу

Основною метою запропонованого методу є зменшення кількості елементів *LUT* та їх міжз'єднань у блоці адресації МК. Метод застосовується, якщо для ГСА Г виконується умова (1). При цьому ГСА є лінійною [1] і потрібна декомпозиція функцій збудження пам'яті, що визначається умовою (6).

Ми пропонуємо використовувати два ядра часткових функцій відповідно до умови (8) У результаті одне ядро засноване на функціональній декомпозиції [8]. Питання оптимізації цієї частини схеми адресації ми не розглядаємо. Для вирішення цієї проблеми є ефективні методи.

Ми пропонуємо метод оптимізації ядра, для якого умова (8) порушується. Як альтернатива функціональный декомпозиції пропонується використовувати структурну декомпозицію [9]. Як відомо [22], структурна декомпозиція призводить до схем, характеристики

Таблиця 6. **Фрагмент таблиці блока *EMB***

Адреса	b_m	y_O	y_E	y_1	y_2	y_3	y_4	y_5	y_6
0000	b_1	1	0	1	1	0	0	0	0
0001	b_2	0	0	0	0	1	0	0	0
0010	b_3	1	0	1	0	1	1	0	0
0011	b_4	1	0	0	0	0	0	1	0
0100	b_5	0	0	0	1	0	0	0	1

яких краще, ніж у еквівалентних схем, заснованих на функціональній декомпозиції.

Як випливає з рис.4, запропонована організація КМПУ має три рівні елементів *LUT*. Розглянемо шляхи оптимізації блоків КМПУ U_2.

Перший рівень схеми складається з K блоків елементів *LUT*. Для синтезу цього блока виконується розбиття багатьох виходів ОЛЛ на класи сумісних виходів. Відповідно до [22], кожна часткова функція реалізується одним елементом *LUT*.

Єдиний шлях оптимізації схеми блока *LUTerk* — зменшення числа функцій, що генерує цей блок. Переходи з виходів ОЛЛ відбуваються або у входи ОЛЛ, або в кінцеву вершину b_E. Для цього необхідно збільшити кількість нульових розрядів адрес входів. Цей підхід є напрямом наших подальших досліджень.

Схема блока *LUTerT* є оптимальною у разі виконання умови:

$$K \le S_L. \tag{23}$$

У цьому випадку блок *LUTerT* складається з R елементів *LUT*, де значення R визначається формулою (2).

Якщо умова (23) порушується, то схема блока *LUTerT* стає багаторівневою. Кількість рівнів можна зменшити, якщо кожна функція $D_r \in D$ складається з $K(D_r)$ часткових функцій, і виконується умова $K(D_r) \le S_L$. У разі виконання цієї умови для всіх ФЗП схема блока *LUTerT* має один рівень. У подальших дослідженнях ми плануємо розробити метод, що дозволяє виконати цю умову для якомога більшої кількості ФЗП $D_r \in D$.

У разі виконання умови $R > S_L$ схема блока *LUTer*т має кілька рівнів. З такою ситуацією ми мали справу в прикладі.

Для покращення характеристик блока *LUTerтV* необхідно зменшувати кількість аргументів у функціях (14), (15). Цього можна досягти за допомогою урахування надлишковості блока *EMB*. За виконання умови $\Delta_A = 2^{S_A} - M > 0$ в КП є Δ_A осередків, у яких не записані МК. Цей факт можна врахувати під час виконання адресації. Розробка такого методу також є спрямуванням наших подальших досліджень.

Висновки

Запропонований у роботі метод можна застосувати, якщо виникає проблема декомпозиції функцій схеми адресації мікрокоманд КМПУ із загальною пам'яттю [1]. Ми розглядаємо ситуацію, коли схема КМПУ реалізується у базисі *FPGA*. При цьому всі комбінаційні блоки реалізуються за допомогою елементів *LUT*.

Необхідність у запропонованому методі виникає, якщо для виходів деяких ОЛЛ виконується умова (8). Для таких виходів слід застосовувати методи функціональної декомпозиції. У цій роботі ми пропонуємо один із можливих шляхів оптимізації схеми КМПУ.

У статті пропонується гетерогенний підхід до формування часткових функцій. Для цієї мети у схемі виділяються два ядра часткових функцій. Одне ядро засноване на функціональній декомпозиції. Друге ядро засноване на адаптації методів подвійного кодування станів [21] до особливостей КМПУ. Практично виходи ОЛЛ виконують функції станів, а адреси МК — функції кодів станів.

У процесі синтезу КМПУ із двома ядрами часткових функцій виникає низка оптимізаційних завдань. Ця необхідність викликається дисбалансом між: 1) числом класів розбиття множини ОЛЛ та числом входів елемента *LUT*, а також 2) числом адресних змінних та числом входів елемента *LUT*. Ми проаналізували ці ситуації та визначили відповідні їм умови. У подальших дослідженнях ми маємо намір розробити метод зменшення впливу зазначених факторів.

Окрім КМПУ із загальною пам'яттю відомі й інші архітектури КМПУ [1]. Крім подвійного кодування станів відомі інші підходи до структурної декомпозиції схем. У подальших наших дослідженнях планується розробка структур та методів синтезу схем КМПУ з іншою архітектурою, що ґрунтується на різних відомих методах структурної декомпозиції.

ПОВІДОМЛЕННЯ:

1) Внесок авторів: Баркалов О.О.: основна ідея, методологія, оригінальна чернетка; Тітаренко Л.О.: узагальнення, концептуалізація, методологія; Матвієнко О.В.: формальний аналіз, ресурси, написання, рецензування та редагування; 2) ШІ та інші інструменти під час написання статті не використовувалися; 3) Конфлікти інтересів відсутні ;4) Гранти або фінансова підтримка не використовувалися.

ЛІТЕРАТУРА / REFERENCES

1. Barkalov A., Titarenko L. Logic Synthesis for Compositional Microprogram Control Units. *Lectures Notes in Electrical Engineering*, Springer, 2008, Vol. 22, 272 p. https://doi.org/10.1007/978-3-540-69285-0
2. Barkalov A. Microprogram control unit as composition of automate with programmable and hardwired logic. *Automatics and Computer Science,* 1983, Vol. 17, 36–41.
3. Feng W., Greene J., Mishchenko A. Improving FPGA Performance with a S44 LUT Structure. *ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (NewYork,NY,USA), FPGA'18*, 2018, Association for Computing Machinery, 61–66. https://doi.org/10.1145/3174243.317427
4. Kuon I., Tessier R., Rose J. FPGA Architecture: Survey and Challenges. *Foundations and Trends in Electronic Design Automation*, 2008, Vol 2 (2), 135–253. https://doi.org/10.1561/1000000005
5. DeMicheli G. *Synthesis and optimization of digital circuits*. New York: McGraw-Hill, 1994, 576 p.
6. Ruiz-Rosero J., Ramirez-Gonzalez G., Khanna R. Field Programmable Gate Array Applications—A Scientometric Review. *Computation*, 2019, Vol. 7 (4), Article 63. https://doi.org/10.3390/computation7040063
7. Czerwinski R., Kania D. Synthesis method of high speed finite state machines. *Bulletin of the polish academy of sciences. Technical sciences*, 2010, Vol. 58 (4), 635–644. https://doi.org/10.2478/v10175-010-0067-6

8. Kubica M., Opara A., Kania D. *Technology Mapping for LUT- based. FPGA*. Springer, 2021. https://doi.org/10.1007/978-3-030-60488-2
9. Barkalov A., Titarenko L., Mielcarek K., Chmielewski S. Logic Synthesis for FPGA–Based Control Units. *Structural Decomposition in Logic Design*. *Lecture Notes in Electrical Engineering*, Springer, 2020, Vol. 636. https://doi.org/10.1007/978-3-030-38295-7
10. Grout I. *Digital systems design with FPGAs and CPLDs*. Elsevier, Amsterdam, 2008, 784 p. https://doi.org/10.1016/B978-0-7506-8397-5.X0001-3
11. Barkalov O., Titarenko L., Saburova S., Golovin, O., V. Matvienko O. Optimization of a composite microprogram control device scheme with a basic architecture. *Cybernetics and Computer Technologies,* 2024, Issue 4, 121–133. https://doi.org/10.34229/2707-451X.24.4.11
12. Baranov S. *Logic synthesis for control automata*. Dordrecht: Kluwer Academic Publishers, 1994, 312 p. https://doi.org/10.1007/978-1-4615-2692-6
13. Chapman K. Multiplexer Design Techniques for Datapath Performance with Minimized Routing Resources. *Xilinx All Programmable*, 2014. URL: https://docs.amd.com/api/khub/documents/9pOn~3NV8ApAbwglqp6MJQ/content [Accessed Jan. 2022]
14. Trimberg S. Three ages of FPGA: A retrospective on the first thirty years of FPGA technology. *IEEE Proceedings 103*, 2015, Vol. 3, 318–331. https://doi.org/10.1109/JPROC.2015.2392104
15. Tiwari A., Tomko K. Saving power by mapping finite state machines into embedded memory blocks in FPGAs. *Design, Automation and Test in Europe Conference and Exhibition,* Paris, France, 2004, Vol. 2, 916–921. https://doi.org/10.1109/DATE.2004.1269007
16. Senhaji-Navarro R., Garcia-Vargas I., Jimenes-Moreno G., Civit-Balcells A., Guerra-Gutierres P. ROM-based FSM implementation using input multiplexing in FPGA devices. *Electronics Letters*, 2004, Vol. 40 (20), 1249–1251. https://doi.org/10.1049/el:20046007
17. Xilinx. URL: https://www.amd.com/en/products/adaptive-socs-and-fpgas/fpga.html#overview [Accessed Jan. 2025]
18. Vivado Design Suite. URL: https://www.xilinx.com/products/design-tools/vivado.html,2020 [Accessed Jan. 2025]
19. Quartus II. URL: https://www.intel.com/content/www/us/en/products/details/fpga/development-tools/quartus-prime/resource.html [Accessed Jan. 2025]
20. Barkalov O., Titarenko L., Mielcarek K. Hardware reduction for LUT based Mealy FSMs. *International Journal of Applied Mathematics and Computer Science*, 2018, Vol. 28 (3), 595–607. https://doi.org/10.2478/amcs-2018-0046
21. Barkalov A., Titarenko L., Mielcarek K. Hardware reduction for LUT–based Mealy FSMs. *International Journal of Applied Mathematics and Computer Science,* 2018, Vol. 28 (3), 595 – 607. https://doi.org/10.2478/amcs-2018-0046
22. Opara A.; Kubica M.; Kania D. Decomposition Approaches for Power Reduction. IEEE Access 2023, 11, 29417–29429

Отримано/Received 18.05.2026
Прийнято/Accepted 11.07.2026
Опубліковано/Published 25.08.2026

O.O. BARKALOV, DSc (Engineering), Professor,
University of Zielona Góra,
ul. Licealna 9, 65-417, Zielona Góra, Poland
https://orcid.org/0000-0002-4941-3979; A.Barkalov@iie.uz.zgora.pl
L.O. TITARENKO, DSc (Engineering), Professor,
University of Zielona Góra,
9, Licealna Str., Zielona Gora, 65-417, Poland
Kharkiv National University of Radioelectronics,
14, Science ave., Kharkiv, 61166, Ukraine
https://orcid.org/0000-0001-9558-3322; L.Titarenko@iie.uz.zgora.pl
O.V. MATVIIENKO, Research Associate,
Glushkov Institute of Cybernetics of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0000-0003-1838-1422; avmatv@ukr.net

SYNTHESIS OF A COMPOSITIONAL MICROPROGRAM
CONTROL UNIT WITH TWO CORES OF PARTIAL FUNCTIONS

Introduction. Digital systems consist of combinational and sequential blocks. The most important sequential blocks include control units (CU). The circuits of CUs are not standard library components in CAD systems, so designing a particular CU circuit is a more labor-intensive process than implementing systems from common blocks such as registers, counters, arithmetic blocks, and logic blocks.

The quality of a digital system depends on the optimal characteristics of the CU. When synthesizing a CU circuit, it is necessary to solve a number of optimization problems: reducing the chip area occupied by the CU, increasing performance, and reducing power consumption. It is believed that solving the first of these problems allows improving other characteristics of the CU circuit.

Purpose of the work. The main focus of this article is the development of effective methods for optimizing the parameters of CU circuits when implemented on an FPGA (field-programmable gate array) basis.

Methods. A method for structural decomposition of a Compositional Microprogram Control Unit (CMCU) circuit in an FPGA is proposed. The method is based on the identification of two cores of partial functions. One core is based on the functional decomposition and generates functions for which the number of arguments exceeds the number of LUT inputs. The second core is based on the adaptation of twofold state assignments methods to the specifics of CMCU. This core generates functions based on the encoding of operator linear chains.

Results. An CMCU architecture with two cores of partial functions and a method for synthesizing the CMCU circuit are proposed. The FPGA implementation of the CMCU circuit used look-up tables (LUTs) and embedded memory blocks (EMBs). Since AMD Xilinx is the dominant FPGA chip manufacturer, the method proposed in this article is tailored to FPGAs from this company.

An example of synthesizing a CMCU circuit with two cores is presented. The conditions for applying this approach are discussed. Possible solutions to optimization problems associated with imbalances in the characteristics of the control algorithm and LUT elements are demonstrated.

Conclusion. During the synthesis of a CMCU with two cores of partial functions, a number of optimization problems arise. This is necessitated by an imbalance between: 1) the number of classes in the operator linear chains set partitioning and the number of LUT element inputs, and 2) the number of address variables and the number of LUT element inputs. This article analyzes these situations and identifies the corresponding conditions. In our future research, we intend to develop a method for mitigating the impact of these factors.

Keywords*: partial function, kernel, CMCU, LUT, EMB, synthesis, structural decomposition.*

INTELLECTUAL INFORMATION TECHNOLOGIES
ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

https://doi.org/10.15407/intechsys.2026.03.030
УДК 004.8

С.Л. КРИВИЙ, д-р фіз.-мат. наук, професор,
каф. Інтелектуальних програмних систем, ф-т. комп'ютерних наук та кібернетики,
Київський національний університет імені Тараса Шевченка,
просп. Акад. Глушкова, 4Д, Київ, 03022, Україна
https://orcid.org/0000-0003-4231-0691
sl.krivoi@gmail.com
Л.М. ГРИДНЄВА, канд. філолог. наук, доцент,
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»,
Берестейський просп., 37, Київ, 03056, Україна
grid_l@ukr.net
Т.К. СКРИПНИК, старш. викладач, каф. комп'ютерних наук,
Хмельницький національний університет,
вул. Інститутська, 11, Хмельницький, 29016, Україна
https://orcid.org/0000-0002-8531-5348
tkscripnik1970@gmail.com

ІТЕРАЦІЙНИЙ ЛОГІКО-ЛІНГВІСТИЧНИЙ МЕТОД АНАЛІЗУ ПРИРОДНОМОВНИХ ТЕКСТІВ

Пропонується триетапний ітераційний метод добування знань із природномовних текстів, використовуючи формально-логічний і синтактико-семантичний аналіз, тлумачні словники, енциклопедії, спеціальну літературу. Логічгий підхід до такого ґрунтується на використанні дескриптивних логік та засобів, якими оперують ці логіки. Метою такого аналізу є побудова несуперечних онтологічних баз знань, поповнення баз новими фактами, та перевірка сумісності бази. Основним завданням в цьому процесі є перевірка виконуваності концептів, несуперечності фактів, поповнення множини фактів новими фактами, які неявно присутні в тексті з метою успішного проведення їхнього формально логічного аналізу. На першому етапі аналізу збирається вся інформація з тексту, яка в цьому тесті явно присутня. На другому етапі в разі необхідності (яка диктується роботою різонерів) виконується додатковий аналіз тексту для пошуку неявно присутньої в ньому інформації. Для успішної роботи засобів логічного аналізу фактів виникає потреба у пошуку інформації, яка знаходиться за межами аналізованої області. Пошук потрібної (релевантної) інформації виконується

Цитування: Кривий С.Л., Гриднєва Л.М., Скрипник Т.К. Ітераційний логіко-лінгвістичний метод аналізу природномовних текстів. Information Technologies and Systems. 3 (9). 2026. 30—46. https://doi.org/10.15407/intechsys.2026.03.030

на третьому останньому етапі аналізу. Зокрема, цей пошук може використовувати засоби систем штучного інтелекту, різного роду енциклопедичні словники тощо.

Ключові слова: *аналіз тексту, вилучення знань, онтологічна база знань.*

Вступ

У роботі розглянуто підхід до аналізу прродномовного тексту шляхом ітераційного покрокового способу пошуку фактів та поповнення ними системи формально-логічного аналізу. На підставі результатів аналізу будується база знань з перевіркою виконуваності концептів і несуперечності бази знань на основі дескриптивних логік. У пропонованому підході виділено три етапи побудови онтологічної бази знань (БЗ). На даний час побудовано декілька онтологічних баз знань, найвідомішими з них є *Bdpedia* [1], *Freebase* [2], *YAGO* [3] та інші.

Побудова цих БЗ ґрунтується на понятті графа знань (ГЗ) (*knowledge-graph*) [4], у якому вершини асоціюються з концептами реального світу або абстрактними концептами, а ребра — з відношеннями, які описують семантико-логічні зв'язки між цими концептами. Оскільки знання в часі можуть еволюціонувати і змінюватися, то були впроваджені динамічні графи знань [5], темпоральні графи знань [6], а також їх інтеграція за великими мовними моделями [7] тощо. Побудова БЗ на основі графів знань, який на даний час є домінуючим, та застосування онтологічних БЗ детально описано у огляді [8].

Порівняння перерахованих систем між собою ведеться за засобами логічної мови, яка використовується, її виразністю та доступністю до інших джерел інформації, зокрема до систем штучного інтелекту. З цього погляду онтологічні БЗ поділяються на пропозиційні (логіка висловлювань), модальні (модальна логіка), темпоральні (темпоральна логіка), ймовірнісні (рекомендаційні системи) тощо.

Одним з основних питань при роботі з онтологічною БЗ є питання видобування нових знань та поповнення ними БЗ з метою розширення можливостей самої БЗ. Оскільки задекларовані знання і видобуті нові знання не завжди можуть бути абсолютно істинними, то в роботі [9] розглядалися можливості залучення багатозначних і нечітких логік до генерації наслідків з можливістю оцінки ступеня їхньої логічної істинності. Стосовно логіки, яку пропонується використовувати в даній роботі, то це багатозначна (зокрема тризначна) логіка. Крім того, тут основна увага приділятиметься способам побудови БЗ, виконання аналізу отриманих фактів, несуперечності поповнення новими фактами (знаннями) існуючих та простий спосіб застосування тризначної логіки при перевірці виконуваності запитів. Як зазначалося вище такий процес реалізується у три етапи.

На першому етапі виконується побудова множин концептів, фактів і відношень між концептами, які явно фігурують у тексті, що аналізується (перше наближення результатів аналізу).

На другому етапі знайдені множини концептів поповнюються похідними концептами, фактами і відношеннями, які з'являються в

процесі перевірки виконуваності концептів та логічного аналізу знайдених фактів.

На третьому етапі до БЗ додаються концепти, факти і відношення, добуті з тлумачних словників, енциклопедій, спеціалізованих словників.

З метою добування знань, які в них акумульовані, формально логічний аналіз природномовних текстів потребує логічної повноти множини знайдених фактів, оскільки в разі цієї неповноти методи такого аналізу стають незастосовними [10, 12]. Розв'язання цієї проблеми вимагає поповнення БЗ фактами, яких бракує для успішного проведення логічного аналізу. Результати аналізу залежать від точності перекладу знайдених фактів на мову тієї чи іншої математичної логіки (вибір математичної логіки залежить від складності тексту). У разі повноти множини фактів логічний аналіз виконує перевірку на суперечність/несуперечність цієї множини фактів. Проблема неповноти виникає практично завжди, оскільки добуті факти, як правило, завжди неповні. Це природно, тому що в тексті можуть фігурувати посилання на інші тексти, архівні дані, аудіо записи, інтерв'ю тощо. Під час аналізу тексту можуть бути потрібні факти, які в ньому явно не фігурують, і тоді виникає потреба внесення їх у систему аналізу, чого вимагає формально-логічний аналіз. На допомогу приходить синтактико-семантичний аналіз тексту, що дає змогу використовувати тлумачні словники, словники аналізованого тексту, глибинні семантичні характеристики понять, термінів, словосполучень тощо.

Основним об'єктом, який нас цікавитиме в цій роботі, є **знання.** Поняття знання ми будемо розуміти згідно з таким загальним визначенням.

Визначення 1. Знання — це філософська категорія для позначення упорядкованого в систему і підтвердженого практикою результату пізнання дійсності навколо нас. Предметними формами існування знання, як відображення об'єктивної дійсності, є такі категорії, як поняття, судження (міркування), гіпотези, теорії, факти тощо [12].

Логіка лінгвістична та логіка математична у системах аналізу текстів

Для аналізу природно мовних текстів застосовують два типи логік: синтактико-семантичну логіку і формальну математичну логіку.

Синтактико-семантична логіка передбачає пошук алогізмів у текстах, повторень, тавтологій у визначеннях тощо, які є надлишковими. Видалення надлишковості спрощує (симпліфікує) текст. Синтактико-семантичний аналіз тексту (особливо наукового) пов'язано зі *знанням логічних законів побудови* тексту. Цей аналіз потребує уваги до термінологічного апарату і правил визначення термінів. Саме за допомогою визначення розкривається значення (семантика) термінів.

Визначення 2. Термін — це лексична одиниця для спеціальних цілей, яка позначає загальне, конкретне або абстрактне поняття (концепт) певної галузі знань [13].

У цьому визначенні наголошується на тому, що, **по-перше**, терміни мають ті семантичні й формальні ознаки слів і словосполучень, що і слова природної мови; **по-друге**, терміни функціонують у лексиці мови тільки для спеціальних цілей; **по-третє**, терміни служать для позначення спеціальних понять. Можна тільки додати, що до термінів ставляться нормативні вимоги, які розрізняють термін і нетермін. Основних рис терміна, які відрізняють його з-поміж інших лексичних одиниць, є декілька.

1. *Однозначність*: термін має позначати тільки одне наукове або технічне поняття, а поняттю повинен відповідати тільки один термін.

2. *Системність*: будь-який термін — член певної терміносистеми, отже, значення терміна фіксується в системі й підтримується параметрами, що використовуються в ній.

3. *Мотивованість*: значення терміна визначається всією системою понять і приписується йому за допомогою дефініції; мотивованість терміна сприяє його запам'ятовуванню, полегшує зв'язок з іншими термінами.

4. *Лінгвістична правильність*: точність терміна значною мірою забезпечується завдяки правильному використанню словотворчих засобів.

5. *Термінологічна упровадженість*: під час укладання термінологічних рекомендацій перевага надається терміну, який має ширше розповсюдження, більш тривалу традицію використання поколіннями спеціалістів.

На відміну від звичайної побутової лексики терміни мають соціально-побутовий характер, тому що в них відображаються факти, що їх спостерігає дослідник, а також їх теоретичне осмислення. Кожний крок дослідження закріплюється у термінах — продуктах мисленнєвої діяльності людини.

Однозначно визначити термін важко тому, що це залежить від предметної області, до якої він належить. В разі логічного визначення терміна на перше місце ставиться його зв'язок із поняттям: з одного боку, будь-який термін називає поняття, з іншого — виражає його, але характер цього зв'язку ще досі нез'ясований [2, 7]. Тут важливими є дві обставини:

1) поняття, яке позначається терміном, взаємопов'язане з іншими поняттями тієї самої предметної галузі та є елементом системи понять;

2) термін є елементом термінологічної системи, і є взаємопов'язаним з іншими термінами.

Математична логіка спершу потребує перекладу об'єктів (концептів), які фігурують у тексті, зв'язків об'єктів між собою (відношень), ознак самих об'єктів з природної мови на формальну мову математичної логіки. Тільки після цього методи логічного аналізу застосовуються до результатів такого перекладу. Завдання математичної логіки полягає в тому, щоб виявити в отриманій інформації формально-логічні суперечності/несуперечності, повноту/неповноту термінології та фактів, і знайти нове знання у вигляді наслідків.

Розглянемо різницю між визначенням у лінгвістиці і у формальній логіці.

Визначення 3. Визначення у лінгвістиці — це така логічна операція, за допомогою якої:

• розпізнається зміст якогось терміну;

• описується значення (семантика) якогось слова чи словосполучення;

• стає можливим відрізнити один термін від інших термінів [13, 15].

Результатом цієї логічної операції є об'єкт, який визначається (*дефінієндум*) і засіб визначення (*дефінієнс*). При цьому намагаються слідувати Арістотелевим правилами [14, 15] .

Математична логіка максимально конкретизує ці закони і правила, оскільки в ній семантика визначається однозначно і правила, на підставі яких вона побудована, вже не залежать від природномовного тексту за умови точного перекладу всіх понять і зв'язків між ними на мову формальної логіки.

Далі в роботі використовується сім'я дескриптивних логік, зокрема логіка *ALC* та її теоретико-множинна семантика [11]. Дескриптивні логіки будують за допомогою введення конструкторів, які застосовують до множин первинних концептів (нотація ***CN***) і відношень (нотація ***RN***). Основними конструкторами у *ALC* логіці є заперечення концепту — $\neg C$, перетин концептів — $C \text{Ç} D$, об'єднання концептів — $C \cup D$, квантори $\exists R.C$ і $\forall R.C$, де R – атомарна роль, C, D – довільні концепти.

У мовах дескриптивної логіки під **концептом** *розуміють клас індивідних об'єктів, що можуть мати деякі прості властивості, які називають атрибутами* [16]. Усі концепти мають наповнення (обсяг). Один і той самий концепт, яким позначається певний клас *об'єктів*, нічого не говорить про його обсяг. Для того щоб добути цю інформацію, застосовують операцію поділу (обсягу, наповнення) концептів. *Поділ поняття* — це операція, за допомогою якої розкривається наповнення родового поняття через перелік його сортів (видів) або елементів.

Між концептами вводяться бінарні відношення R_1, R_2, ….R_n, які характеризують зв'язки між ними. Концепти і відношення поділяють на атомарні та похідні. Атомарний концепт (відношення) — це первинний клас об'єктів (відношень), за допомогою яких визначаються нові концепти і відношення, які називають похідними [11, 16]. Формалізація похідних концептів і їхні властивості описуються за допомогою термінологічних аксіом (*TBox — Terminological Box*) та фактів (*ABox — Assertion Box*).

Визначення 4. Термінологічною аксіомою називають вираз $C \subseteq D$ або $C \equiv D$, де C, D — довільні концепти. Термінологією (*TBox*) називають скінченну множину термінологічних аксіом деякої предметної області.

Вираз $C \subseteq D$ означає скорочення концепт C «міститься» в концепті D, а вираз $C \equiv D$ — скорочення концепти C і D «еквівалентні». Системою фактів *ABox* називають скінченну множину $\boldsymbol{A}$ тверджень такого вигляду $a{:}C$ і aRb, де a ,b — деякі індивіди, C — довільний концепт, R — довільне відношення.

Твердження $a{:}C$ і aRb означають, що індивід a належить концепту C, і що індивіди a, b зв'язані відношенням R відповідно.

Семантику логіки *ALC* визначає інтерпретація $I = (\Delta, f)$, де Δ — область інтерпретації, f — функція інтерпретації. Функція інтерпретації ставить у відповідність

— кожному атомарному концепту A підмножину (його наповнення в області Δ) $A^f \subseteq \Delta$;

— кожній атомарній ролі R — (і її наповнення в області D) $R^f \subseteq \Delta \times \Delta$.

Інтерпретація I розповсюджується індукцією за побудовою концепту у такий спосіб:

— $T^f = D$, $\bot^f = \varnothing$, $\neg C^f = \Delta \setminus C^f$, (де $T(\bot)$ — істинний (хибний) концепт);

— $(C \cup D)^f = C^f \cup D^f$, $(C \cap D)^f = C^f \cap D^f$;

— $\exists(R.C)^f = \{e\, \Delta \mid \exists d \in D\colon (e, d) \in R^f \wedge d \in C^f\}$;

— $(\forall R.C)^f = \{e \in D \mid \forall d \in \Delta\colon (e, d) \in R^f \to d \in C^f\}$.

Визначення 5. У дескриптивній логіці визначенням називається введення нового концепту за допомогою конструкторів і операцій цієї логіки через атомарні концепти та відношення і раніше визначені (похідні) концепти та відношення.

Термінологію $\boldsymbol{T}$ називають системою визначень, якщо всі її аксіоми мають вигляд $A \equiv C$, де A — атомарний, а C — довільний концепт, причому в $\boldsymbol{T}$ немає двох різних аксіом з однаковою лівою частиною. Самі аксіоми вигляду $A \equiv C$ називають визначеннями.

Аксіома $C \subseteq D$ ($C \equiv D$) істинна за інтерпретації I, якщо $C^I \subseteq D^I$ ($C^I \equiv D^I$). I в такому разі називається моделлю цієї аксіоми, Інтерпретацію I називають моделлю термінології $\boldsymbol{T}$, якщо вона є моделлю для всіх аксіом із $\boldsymbol{T}$. Термінологія $\boldsymbol{T}$ називається **сумісною** або **виконуваною**, якщо вона має непорожню модель.

Концепт C виконується відносно термінології $\boldsymbol{T}$, якщо існує модель I термінології $\boldsymbol{T}$ така, що $C^I \neq \varnothing$.

Нехай $\boldsymbol{T}$ — система визначень. Поділимо атомарні концепти, які зустрічаються в $\boldsymbol{T}$, на дві категорії:

— **базові** (атомарні, первинні), які не належать до лівої частини жодної з аксіом із $\boldsymbol{T}$;

— **похідні** (ті, що визначаються), які належать до лівої частини хоча б однієї аксіоми із $\boldsymbol{T}$.

Базовою називають інтерпретацію $\boldsymbol{J}$, яка інтерпретує лише базові концепти.

Нехай $\boldsymbol{J}$ — базова інтерпретація, а I — довільна інтерпретація. I є розширенням інтерпретації $\boldsymbol{J}$, якщо області їх інтерпретації збіга-

ються $D^I = D^J$ і вони однаково інтерпретують базові концепти, тобто для кожного базового концепту B справедливо $B^I = B^J$.

Систему визначень $\boldsymbol{T}$ називають **коректною**, якщо для довільної базової інтерпретації $\boldsymbol{J}$ існує єдине розширення I, яке є моделлю термінології $\boldsymbol{T}$.

Термінологія дає можливість записувати загальні знання про концепти і ролі. Але часто існує необхідність записувати знання про конкретні індивіди: якому класу належить індивід, якими відношеннями (ролями) вони зв'язані між собою. Це виконується в тій частині бази знань, яку називають системою фактів про індивіди або *ABox*. Із цією метою, крім множини $\boldsymbol{CN}$ атомарних концептів і множини RN атомарних ролей, тобто імен для класів і відношень, вводять також **скінченну множину $\boldsymbol{IN}$ імен індивідів**. Факти про індивідів є двох типів:

— твердження про належність індивіда a до концепту C ($a{:}C$);

— твердження про зв'язок двох індивідів a і b роллю R (aRb).

Семантика *ABox* визначається за допомогою інтерпретації. Візьмемо довільну інтерпретацію $I = (\Delta, f)$ і розширимо її на індивіди: кожного індивіда $a \in IN$ зіставляємо з елементом області інтерпретації $a^I \in \Delta$.

Факт $a{:}C$ або aRb справедливий в інтерпретації I, якщо $a^I \in C^I$ або $(a^I, b^I) \in R^I$. У такому разі інтерпретацію I називають **моделлю** цього факту. Інтерпретацію I називають *моделлю системи фактів* $\boldsymbol{A}$, якщо вона є моделлю всіх фактів з $\boldsymbol{A}$. *ABox* називають *виконуваним* у термінології $\boldsymbol{T}$, якщо $\boldsymbol{A}$ має модель (яка одночасно є моделлю термінології $\boldsymbol{T}$).

Визначення 6. Базою знань (БЗ)} називають пару $\boldsymbol{K}=(\boldsymbol{T}, \boldsymbol{A})$, де $\boldsymbol{T}$ — довільна термінологія (*TBox*), а $\boldsymbol{A}$ — довільна система фактів (*Abox*). Інтерпретацію I називають моделлю бази знань $\boldsymbol{K}$, якщо I є моделлю $\boldsymbol{T}$ і $\boldsymbol{A}$. БЗ називають **виконуваною** або **несуперечною**, якщо вона має непорожню модель.

Факт α (вигляду $a{:}C$ або aRb) випливає з $\boldsymbol{K}$, якщо α виконується в довільній моделі I бази знань $\boldsymbol{K}$.

У логіці *ALC* може порушуватися лише Арістотелеве правило заборони циклу у визначеннях. Справа в тому, що можуть існувати термінологічні аксіоми вигляду

ОСОБА ≡ ССАВЕЦЬ ∩ ∀ має.батька **ОСОБА,**

у яких є цикл. Такого типу цикли розв'язуються за допомогою операції «блокування точки», яка розриває цикл [11]. Насправді ліва і права частини, де фігурує концепт ОСОБА, мають різні семантичні значення (різне наповнення).

Перейдемо до ілюстрації ітераційного методу аналізу тексту, побудови бази знань та проблем, які виникають в процесі такого аналізу на конкретному прикладі.

Приклад аналізу тексту і побудови його бази знань

Розглянемо приклад тексту, на якому продемонструємо етапи аналізу, роль логіки в цьому аналізі та способи видобування понять, термінології, відношень та фактів, рисутніх у ньому.

Приклад 1. «СІМ'Я І ШКОЛА» *(*текст, взятий в інтернеті з оповідання невідомого автора, який не хотів відкривати своє прізвище*).*

«В тихому мальовничому селищі, яке притулилося одним боком до лісу, а другим до огорожі місцевої птахофабрики та невеличкого клаптика поля, жила сім'я Петренків. Сім'я складалася з батька Семена Петровича, матері Олени Степанівни та двох доньок Іринки та Яни. Сім'я була звичайна, як більшість українських сімей. Діти ходили до школи. Іринка була старша і вчилася уже в сьомому класі, а Яна була меншою в сім'ї і вчилася у третьому класі селищної школи-десятирічки. Загалом у школі навчалося 82 учні, серед яких 42 учні навчалися у початкових класах, а решта - у старших класах. Учителів у школі було небагато і тому деякі учителі викладали по декілька предметів у різних класах. Зокрема математику і фізику викладала Марія Петрівна, біологію і хімію – Петро Іванович, Степан Іванович – фізкультуру та військову справу. Стеха Романівна – природознавство, екологію, Семен Петрович – працю та народознавство, Петро Юрійович – історію, Микола Миколайович – українську та зарубіжну літературу, решта вчителів викладали домоводство, етику, психологію, співи. Всього у школі працювало 11 учителів, які забезпечували навчально-виховний процес. Їм у цьому допомагали інженерно технічні працівники: електрик Михайло Микитович, сантехнік Павло Павлович, завідувач шкільним господарством Микола Михайлович та дві прибиральниці – Марина Тихонівна та Тамара Степанівна. На допомогу цьому колективу приходили батьки учнів та представники птахофабрики (в особі директора та членів професійної спілки підприємства), яка була основним роботодавцем для населення селища.

Іринка вчилася старанно на відміну від Яни, яка ще не зовсім розуміла, навіщо вивчати арифметику чи правопис, якщо сучасні комп'ютерні системи це зроблять краще, ніж вона. Тому Ірина часто допомагала молодшій сестрі у навчанні і не тільки. Іринка мала багато подруг у своєму класі і у старших класах. Яна теж дружила зі всіма у своєму класі, через те у неї і виникали проблеми з навчанням, оскільки вона віддавала перевагу іграм з друзями, а не читанню скучних підручників. Серед учнів були такі, які віддавали перевагу тим, чи іншим предметам і тому деякі ***класи мали певну предметну орієнтацію****. ….»*

Яку інформацію можна одержати з наведеного тексту і як її упорядкувати та поповнити так, щоб можна було прослідкувати життя школи, її сучасний стан, учнів, учителів, батьків та інших учасників навчально-виховного процесу у школі ?

Перший етап аналізу

Аналіз наведеного тексту дозволяє виділити концепти, які безпосередньо фігурують у наведеному тексті, а саме:

— селище, школа, птахофабрика,
— учні,
— учителі,
— інженерно-технічний склад працівників (ІТП),
— батьки, діти,
— стать,
— представники підприємства;
— предмети навчання.

Отже, маємо таку множину концептів: ***CN*** = ОСОБА ∪ ОБ'ЄКТ, де

ОСОБА ≡ {УЧЕНЬ, УЧИТЕЛЬ, ІТП, БАТЬКИ, ДІТИ, ПРЕД-ПІДПР} ∪ {ЖІН-СТАТЬ}

ОБ'ЄКТ ≡ {ПТАХОФАБРИКА, ШКОЛА, СЕЛИЩЕ, ПРЕДМЕТИ, ПРОФЕСІЯ},

які ***є атомарними концептами***.

Цю множину потрібно класифікувати (поділити) і наповнити конкретними об'єктами та відношеннями між ними, оскільки різні об'єкти цієї множини мають різні професії, різні завдання і функції тощо. Ця класифікація в такому разі виконується шляхом введення відношень, на підставі яких створюється термінологія. Як це відбувається?

Вводяться відношення такого типу:

учень — це особа яка вивчає якісь предмети;

учитель — це особа, яка викладає якісь предмети;

ІТП — це особи, які забезпечують умови успішного проведення (навчального) процесу;

батьки — це особи, які мають дітей, і ці діти навчаються в школі;

працівники підприємства — це особи, які сприяють успішному проведенню (навчального) процесу у школі і працюють на підприємстві.

Отже, дістаємо ***таку множину (атомарних) відношень*** *RN*:

— R_1 = працює-у-школі,
— R_2 = **представник –підприємства = працює-на-підприємстві,**
— R_3 — **стать-особи,**
— R_4 = **має-дітей**,
— R_4^1 — **має-батьків,**
— R_5 = **викладає-предмет**,
— R_6 **= фах-особи,**
— R_7 = **вивчає-предмет**,
— R_8 = **навчається-у-школі.**

Елементи множин *CN* і *RN* графічно пов'язані такими відношеннями (рис. 1).

Тепер за цими відношеннями будується термінологія (*TBox*):

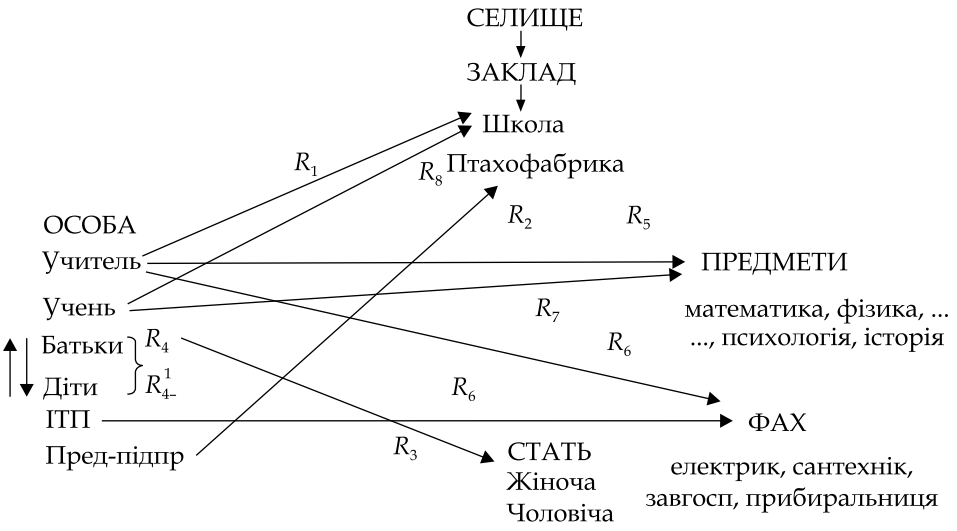


Рис. 1. Граф-схема концептів і відношень між ними

УЧЕНЬ ≡ ОСОБА ∀ вивчає-предмет. ⊤**УЧИТЕЛЬ**≡ОСОБА ∩ ∀викладає-предмет.⊤

ПРЕДМЕТИ≡{математика, арифметика, фізика, біологія, хімія, фізкультура, військова справа, екологія, природознавство, праця, історія, домоводство, правопис, етика, психологія, українська-література, зарубіжна-література};

ІТП ≡ ОСОБА ∩ ∀ професія (* електрик, сантехнік, завгосп, прибиральниця *) — це

індивіди;

БАТЬКИ≡ОСОБА ∩ ∃УЧЕНЬ(має-дітей(ОСОБА,УЧЕНЬ));

ДІТИ ≡ ОСОБА ∩ ∀має-батьків.⊤;

РОДИНА ≡ БАТЬКИ ∪ ДІТИ;

ПРОФЕСІЯ ≡ ФАХ;

ПРЕД-ПІДПР ≡ ОСОБА ∩ ∃ПІДПРИЄМСТВО(пред-підп(ОСОБА, ПІДПРИЄМСТВО)) — це теж можуть бути індивіди.

Далі з наведеного тексту знаходимо (часткову) інтерпретацію (наповнення) знайдених концептів. У даному випадку областю інтерпретації є така множина

D { ДІТИ = {Іринка, Яна, ще принаймні ≥ 80 осіб**}.**

УЧЕНЬ={Іринка, Яна, ще 80 індивідів},

УЧИТЕЛЬ={Марія Петрівна, Петро Іванович, Степан Іванович, Стеха Романівна, Семен Петрович, Петро Юрійович, Микола Миколайович, ВЧ1, ВЧ2, ВЧ3,ВЧ4}.

ІТП=(Михайло Микитович, Павло Павлович, Микола Михайлович, Марина Тихонівна, Тамара Степанівна).

БАТЬКИ=(Семен Петрович, Олена Степанівна, та ще не більше 80 осіб).

ПРЕД-ПІДПР = [директор, профспілка].

ПІДПРЄМСТВО={птахофабрика, школа}.

Далі виконується наповнення (інтерпретація) відношень (*Abox*):

вивчає={(Іринка, математика), (Іринка, українська мова), (Іринка, фізика), (Іринка, хімія), (Іринка, біологія), …, (Яна, правопис), (Яна арифметика),...)};

навчається-у-школі = {(Іринка, 7), (Яна, 3),… };

викладає-предмет={ (Марія Петрівна, математика), (Марія Петрівна, фізика), (Петро Іванович, біологія), (Петро Іванович, хімія), (Степан Іванович, фізкультура), (Степан Іванович, військова справа), (Стеха Романівна, англійська мова), (Стеха Романівна, екологія), (Семен Петрович, праця), (Семен Петрович, природознавство), (Петро Юрійович, історія), (Микола Миколайович, українська мова), (Микола Миколайович, зарубіжна література), (ВЧ1,домоводство), (ВЧ2, етика), (ВЧ3, психологія), (ВЧ4, співи)};

фах-особи = УЧИТЕЛЬ ∪ **ІТП**{електрик(Михайло Микитович), сантехнік (Павло Павлович), завгосп(Микола Михайлович), прибиральниця1(Марина Тихонівна), прибиральниця2(Тамара Степанівна);

має-фах = фах-особи;

має-дітей = {(Семен Петрович, Іринка), (Семен Петрович, Яна), (Олена Степанівна, Іринка), (Олена Степанівна, Яна), (x_1,y_1)…};

пред-підпр = {директор, профспілка}.

Такий вигляд мають **результати першого етапу аналізу** без подальшої деталізації, які утворюють Базу Знань для цього фрагменту тексту.

Запитами до такої БЗ є формули вигляду *a:C* або *aRb*, де *C* — концепт, а *R* — відношення, які відповідно означають що об'єкт *a* є елементом концепту *C* і що об'єкти *a* і *b* пов'язані відношенням *R*.

Наприклад, запит:

чи вивчає Яна математику і чи має вона батьків?

набуває такого вигляду у термінології, що наведена вище:

Яна: (ОСОБА ∩ ∃.вивчає(ОСОБА.математика)) ∩ ∃.має-дітей (ОСОБА,УЧЕНЬ)).

Застосуємо алгоритм, за допомогою якого отримуємо відповідь на запит, який називають алгоритмом семантичного табло (СТ) [11].

Яна: (ОСОБА∩∃.вивчає(ОСОБА.математика))∩∃.має-дітей(ОСОБА, УЧЕНЬ)).

↓

Яна: (ОСОБА∩∃.вивчає(ОСОБА.математика)), Яна : ∃.має-дітей (ОСОБА, УЧЕНЬ)).

↓

Яна: ОСОБА, Яна:вивчає(ОСОБА,математика)), Яна : ∃.має-дітей (ОСОБА,УЧЕНЬ)).

↓

Яна: ОСОБА∩∅∩ Яна : ∃.має-дітей(ОСОБА, УЧЕНЬ)) = ⊥.

↓

Яна: ⊥.

Отримали суперечність з тим, що Яна належить до порожньої множини. А це означає, що моделі, де йдеться про вивчення Яною математики, немає, оскільки Яна віддає перевагу іграм.

Розглянемо питання несуперечності отриманої бази знань. Згідно з означенням несуперечної БЗ потрібно показати, що вона має непорожню модель. З наведеного вище випливає непорожність моделі БЗ, тобто її несуперечність. Можна було б окремо переконатися у справедливості кожної термінологічної аксіоми і факту у цій моделі.

Другий етап аналізу

Зафіксувавши термінологію і знайдені факти у вигляді БЗ, можна виконувати пошук нових фактів (знань) як логічних наслідків зафіксованих фактів. Це завдання ускладнюється тією обставиною, що деяка кількість концептів і відношень можуть мати невизначену інтерпретацію. Отже, разом з відомою оцінкою ступеня істинності одних концептів, існують концепти, ступінь істинності яких за цієї інтерпретації невідомий. У нашому прикладі інтерпретація концепту

$$C = (\text{ОСОБА} \setminus \{\text{Іринка}\}) \cap \exists.\text{вивчає}(\text{ОСОБА}.\text{математика})),$$

який означає: *чи вивчає ще хто-небудь, крім Іринки, математику*? Нам точно відомо, що концепт $\exists.вивчає(ОСОБА.математика)$ виконується, оскільки існує непорожня модель, яка міститиме особу Іринка, як і концепт $\exists.\neg вивчає(ОСОБА.математика)$, яка має непорожну модель, яка містить особу Яна. Але виконуваність концепту C не визначена, оскільки хто ще з 80 учнів школи вивчає математику нам з тексту невідомо.

Алгоритм перевірки виконуваності концепту C в такій ситуації вимагає додавання нового індивіда y до множини індивідів IN, наприклад індивіда Ольга. Але ***додавання нового індивіда чи концепту мусить супроводжуватися перевіркою несуперечності*** такого поповнення. У такому разі необхідно переконатися в тому, що така особа як Ольга є серед учнів школи і ця особа вивчає математику. Глибший аналіз тексту дає підказку, яка виражається словами «*класи мали певну предметну орієнтацію*». Звідси можна зробити висновок, що разом з Іринкою в її класі (предметно орієнтованого на вивчення математики) є ще особи, які вивчають математику (наприклад, Ольга).

Але можлива ситуація, коли з яких-небудь причин ми не можемо перевірити несуперечність такого поповнення. Тоді ми змушені працювати в умовах невизначеності і тут у пригоді стає тризначна логіка (у даному випадку — логіка Лукасєвича), яку позначають L_3 [11]. У цій логіці є три логічні значення: 1 — *ALC*-формула істинна, 1/2 — значення (ступінь істинності) *ALC*-формули невизначено, 0 — *ALC*-формула хибна. Якщо можливий діалог з БЗ та її творцями, то такого типу невизначеності частково розв'язуються за допомогою прямого діалогу.

У протилежному випадку всі добуті факти градуюються значеннями логіки L_3 і залишається сформулювати правила градуювання наслідків, отриманих після застосування правил побудови моделі у алгоритмі семантичного табло [11, 16]. Це зробити неважко, оскільки якщо ступінь істинності деякої підформули *ALC*-формули невизначено, то цей ступінь зберігається й у тих підформулах, до яких ця формула належить.

Сформулюємо правила градуювання формул у процесі застосування L_3-логіки. Позначимо $v(A)$ значення *ALC*-формули A. Тоді

— якщо $v(A) = x$, то $v(\neg A) = 1 - v(A) = 1-x$;

— якщо $v(A \cap B) = 1$, то $v(B) = v(A) = 1$;

— якщо $v(A \cap B) = 0$, то замкнути гілку;

— якщо $v(A \cap B) = 1/2$, то $v(B)=x$, $v(A)=y$, де x,y — значення формул A і B;

— якщо $v(A \cup B = 0$, то $v(B) = v(A) = 0$;

— якщо $v(A \cup B) = 1/2$, то $v(B) = v(A) = 1\backslash 2$;

— якщо $A \cup B) = 1$, то $v(A) = 1$ коли A несуперечний і $v(B) = 1$ коли B несуперечний;

$v(A) = 1$ коли A несуперечний і $v(B) = 1/2$ коли B невизначений;

$v(A) = 1$ коли A несуперечний і замкнути гілку B коли $v(B) = 0$;

$v(B) = 1$ коли B несуперечний і $v(A) = 1/2$ коли A невизначений;

$v(A) = 1$ коли B несуперечний і замкнути гілку A коли $v(A) = 0$;

– якщо $v(\exists R.A) = x$, то ввести індивіда a до концепту A і aRb. Якщо a в A немає, то виконати перевірку несуперечності такого поповнення. Якщо поповнення суперечне, то замкнути гілку у СТ, інакше покласти $v(b:A)=v(aRb)=x$.

– якщо $v(«R.A) = x \neq 0$, то ввести всіх індивідів a до концепту A таких, що aRb, якщо a належить до A. Якщо a в A немає, то виконати перевірку несуперечності такого поповнення. Якщо поповнення суперечне, то замкнути гілку у СТ, інакше покласти $v(a:A)=v(aRb)=x$ для всіх таких $a \in D$.

Наприклад, концепт

$$C = (\text{ОСОБА} \setminus \{\text{Іринка}\}) \cap \exists. \text{вивчає}(\text{ОСОБА.математика}))$$

матиме значення 1/2. А алгоритм семантичного табло побудує дві формули

$$a{:}\text{ОСОБА} \wedge a \neq \text{Іринка і } a{:} \text{ вивчає}(\text{ОСОБА.математика}),$$

які набувають значень 1/2, оскільки про індивіда a в аналізованому тексті явно нічого не говориться.

Третій етап аналізу

На цьому етапі уточнюється та розширюється множина концептів і відношень, з використанням тлумачних словників, енциклопедій тощо. Зокрема, із Тлумачного Словника української мови [17] дістаємо уточнення таких концептів:

• ЗНАННЯ: *знання — це обізнаність у чому-небудь, наявність відомостей про кого небудь;*

— це сукупність відомостей з якої-небудь предметної галузі, набуті у процесі навчання, дослідження тощо;

— пізнання дійсності в окремих її проявах та в цілому.

• ШКОЛА: *школа — це навчальний заклад, в якому навчаються учні;*

— це навчальний заклад середньої освіти;

— це приміщення, де навчаються учні та працюють учителі;

• ОСВІТА: *освіта — це сукупність знань, здобутих у процесі навчання в навчальному закладі (школі, інституті,університеті тощо)*

• ШКОЛА+ДЕСЯТИРІЧКА≡СЕРЕДНЯ-ШКОЛА: *— це школа, в якій учні навчаються протягом десяти років;*

• ШКОЛА ПОЧАТКОВА: *— це школа, в якій учні навчаються протягом перших чотирьох років;*

• СІМ'Я: сім'я *— це батьки і діти цих батьків;*

• ІТП: *інженерно-технічні працівники — це електрик, сантехнік, завгосп, прибиральниця.*

• УЧИТЕЛЬ: *учитель — це особа, яка є авторитетом у своїй галузі,*

— це особа, яка передає свій досвід знання,

— це особа, яка впливає на інших і є для них прикладом.

• ДИРЕКТОР *— це особа, яка є керівником підприємства або навчального закладу.*

• НАВЧАЛЬНИЙ ЗАКЛАД ≡ ШКОЛА.

• ПРИМІЩЕННЯ≡{приміщення-пта-ф, школа}:

• СПЕЦІАЛЬНІСТЬ ≡ФАХ

Подальший аналіз тексту розширює множину концептів і відношень, які були отримані на попередніх етапах, так званими *смисловими концептами і відношеннями*. Наприклад, КІЛЬК(школа, учнів), ЛОК(птахофабрика, селище), ЛОК(школа, селище), СПЕЦ(учитель, предмет). СПЕЦ1(ітп, спеціальність), ПРИНАЛ(приміщення, школа), ЗВ'ЯЗ(школа, птахофабрика), СУМІСНИК(особа, підприємство). Ці відношення описують кількість учнів, які навчаються у школі, місце знаходження школи, спеціальність учителя, спеціальність інженерно-технічного працівника, яке приміщення належить школі, зв'язок школи і птахофабрики тощо.

Такі додаткові концепти і факти дають можливість точніше і повніше відповідати на запити до БЗ, формувати нові знання, які не фігурують у початковому тексті, поповнювати множини концептів і фактів, які необхідні для завершення роботи систем логічного аналізу, та формувати посилання на джерела, де відповідні об'єкти описуються або використовуються.

З огляду на сказане, сформулюємо проблеми, які виникають в процесі створення БЗ:

1) автоматизація повного або часткового поповнення БЗ (які мають бути правила, засоби і механізми);

2) автоматизації процесу пошуку фактів, яких бракує для успішного завершення перевірки виконуваності концептів;

3) поповнення БЗ метафоричними даними;

4) оброблення інформації, яка ї невизначеною (формули зі значеннями 1/2).

Підсумки

Розглянуто застосування результатів семантико синтаксичного аналізу та мов математичної логіки до видобування знань та перевірку отриманих знань на суперечність/несуперечність. За результатами семантико синтаксичного аналізу тексту на основі мов дескриптивної логіки будуються бази знань, а за допомогою мов тризначної логіки отримуємо ступені істинності висновків в умовах невизначеності.

ПОВІДОМЛЕННЯ:

Внесок авторів: *Кривому С.Л. належить ідея статті, розробка математичного апарату, Гриднєвій Л.М. – застосування синтактико-семантичної логіки для пошуку алгоритмів з метою симпліфікації тексту; Скрипник Т.К. – реалізація окремих частин алгоритму семантичного табло.*

Застосування ШІ: *автори не використовували засобі ШІ при підготовці статті.*

Конфлікти інтересів: *немає конфлікту інтересів.*

ЛІТЕРАТУРА/ REFERENCES

1. Morsey M., Lehmann J., Auer S., Stadler C., Hellmann S. DBpedia and the live extraction of structured data from Wikipedia. Program: electronic library and information systems, 2012. 46 (2), pp. 157–168.
2. Bollacker K., Evans C., Paritosh P., Sturge T., and Taylor J. Freebase: a collaboratively created graph database for structuring human knowledge, in *Proc. of SIGMOD*, 2008. pp. 1247–1250.
3. Suchanek F.M., Kasneci G., and Weikum G. Yago: a core of semantic knowledge. In *Proc. of WWW*, 2007. pp. 697–678.
4. Hogan A., Blomqvist E., Cochez M., et. al. Knowledge graphs. *ACM Computing Surveys (CSUR)*, 2021. V. 54. N 4. pp. 1–37.
5. Wang Q., Mao Z., Wang B., and Guo L. Knowledge graph embedding: A survey of approaches and applications, *IEEE Transactions on Knowledge and Data Engineering*, 2017. v. 29. pp. 724–2743.
6. Xu C., Nayyeri M., Alkhoury F., Yazdi H., and Lehmann J. Temporal knowledge graph completion based on time series gaussian embedding, in *Proc. of ISWC*, 2020. pp. 654–671.
7. Qiao Z., et al. A survey on augmenting knowledge graphs with large language models. *AI Open*, 5, 2024. pp. 230–252.
8. Ge H., et al. (2025). On the evolution of knowledge graphs: A survey and perspective. 125 p.
9. Kryvyi S., Hoherchak G. Analyzing Natural Language Kniwledge in Uncertainty on the base of manyvalued Logic. Cybernetics and Systems Analysis, Vol. 60, № 1, Jan, 2024. pp. 32–47.

10. Kryvyi S., Darchuk N., Skrypnyk T. Analyzing natural languages: antimems, contradiction, ontologies. *Cybernetics and Systems Analysis,* 2023, Vol. 59 (2), 177–189. https://doi.org/10.1007/s10559-023-00553-7
11. Kryvyy S.L. *Elements of non-classical mathematical logic*. VTS «Kafedra», Kyiv, 2026. Publishing and Printing Center «Kyiv University», Kyiv, 2026 2024, 608 p. [In Ukrainian] [Кривий С.Л. Елементи некласичної математичної логіки. Київ: ВПЦ «Київський університет». 2024. 608 с.]
12. Article "Knowledge". *Ukrainian Soviet Encyclopedia (URE),* Kyiv, 1979, Vol 4, 2-th ed., 286 p. [In Ukrainian] [Стаття «Знання». *Українська Радянська Енциклопедія,* Головна редакція УРЕ, Київ, 1979, Том 4, вид. 2-ге, с. 286.]
13. Darchuk N.P., Sorokin V.M. *Term in the linguistic information science*. Publishing and Printing Center «Kyiv University», Kyiv, 2012, 143 p. [In Ukrainian] [Дарчук Н.П., Сорокін В. М. *Термін в лінгвістичній інформатиці*. ВПЦ «Київський університет», Київ, 2012, 143 с.]
14. Toftul M.H. *Logic.* Textbook, 2-th ed., Academy, Kyiv, 2008, 400 p. [In Ukrainian] [Тофтул М.Г. Логіка: підручник, 2-ге вид., доповнене. К.: Академія, 2008. 400с.]
15. Gridneva L.M. Logical analysis of terminological dictionaries and scientific texts. Ukrainian linguistics. Taras Shevchenko National University of Kyiv, 2015. Issue 45/1. P. 111–117. [In Ukrainian] [Гриднєва Л.М. *Логічний аналіз термінологічних словників і наукових текстів*. Українське мовознавство. Київський національний університет імені Тараса Шевченка, 2015. Вип. 45/1. С. 111–117].
16. Baader F., Calvanese D., McGuinness D.L. et al. *The Description Logic Handbook*. Cambridge: University Press, 2010, 601 p.
17. *Explanatory dictionary of the Ukrainian language in 11 volumes*. Naukova Dumka, Kyiv, 1970, 1978. [In Ukrainian] [*Тлумачний словник української мови в 11-ти томах*. Київ: Наукова думка, 1970, 1978]

Отримано/Received 15.01.2026
Прийнято/Accepted 18.06.2026
Опубліковано/Published 25.08.2026

S.L. KRYVYI, Doctor of Physical and Mathematical Sciences, Professor,
Department of Intelligent Software Systems, Faculty of Computer Science and Cybernetics,
Taras Shevchenko National University of Kyiv,
40 D, Acad. Glushkova ave., Kyiv, Ukraine, 03022
https://orcid.org/0000-0003-4231-0691
sl.krivoi@gmail.com

L.M. GRYDNEVA, Ph.D Philologist Sciences, Associate Professor,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
37, Beresteysky ave., Kyiv, 03056, Ukraine
grid_l@ukr.net

T.K. SKRYPNYK, Senior Lecturer,
Computer Science, Khmelnytskyi National University,
11 Instytutska St., Khmelnytskyi, 29016, Ukraine
https://orcid.org/0000-0002-8531-5348
tkscripnik1970@gmail.com

ITERATIVE LOGICAL-LINGUISTIC METHOD
OF ANALYZING NATURAL LANGUAGE TEXTS

Introduction. A three-stage iterative method of extracting knowledge from natural language texts is proposed, using formal-logical and syntactic-semantic analysis, explanatory dictionaries, encyclopedias, and special literature. The logical approach to this is based on the use of descriptive logics and the tools that these logics operate with. The purpose of such analysis is to build consistent ontological knowledge bases, supplement the bases with new facts, and check the compatibility of the base.

The main task in this process is to check the feasibility of concepts, the consistency of facts, and supplement the set of facts with new facts that are implicitly present in the text in order to successfully conduct their formal logical analysis. At the first stage of analysis, all information from the text that is explicitly present in this test is collected. At the second stage, if necessary (which is dictated by the work of reasoners), additional text analysis is performed to search for information implicitly present in it. For the successful operation of the logical analysis of facts, there is a need to search for information that is outside the aPurpose nalyzed area. The search for the necessary (relevant) information is performed at the third and last stage of analysis. In particular, this search can use the tools of artificial intelligence systems, various types of encyclopedic, dictionaries etc.

Purpose. The main task in proposed paper are methods of building the feasibility of concepts, the consistency of knowledge base, and supplement the set of facts with new facts that are implicitly present in the text in order to successfully conduct their formal logical analysis.

Methods. A three-stage iterative methods of extracting knowledge from natural language texts is proposed, using formal-logical and syntactic-semantic analysis, using systems of AI (as oracle) explanatory dictionaries, encyclopedias, and special literature.

Results. Proposed an approach to used three-valued logic for estimation of truth-values conclussions. For the successful operation of the logical analysis of facts, there is a need to search for information that is outside the analyzed area. The search for the necessary (relevant) information is performed at the stage of analysis.

Conclusions. We proposed the three stage methods of extraction of new facts and completion of such new facts of knowledge base, checking its consistency.

Keywords: *Text analysis, knowledge extraction, ontological knowledge base.*

https://doi.org/10.15407/intchsys.2026.03.047
UDC 623.746

O.Ye. VOLKOV, PhD (Engineering), Senior Researcher, Director,
Institute of Information Technologies and Systems of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0000-0002-5418-6723
alexvolk52@ukr.net
I.V. POPOV, Senior Researcher, PhD Student,
Institute of Information Technologies and Systems of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0009-7961-9431
popigor7@gmail.com

ENERGY-CENTRIC CONTROL FOR AUTONOMOUS MOBILE NODES TO ENHANCE FUNCTIONAL STABILITY UNDER TURBULENT

This paper proposes a conceptual approach to the autonomous takeoff and landing control of autonomous mobile nodes (AMN) based on the Total Energy Control System (TEC_dology. The study aims to enhance the operational efficiency and survivability of unmanned aviation by utilizing the aircraft's energy state as a fundamental control invariant. The proposed approach overcomes the limitations of traditional systems, specifically their high sensitivity to stochastic disturbances and degraded stabilization accuracy under atmospheric turbulence. The control algorithm is optimized based on two criteria: minimizing the deviation of the AMN total energy from the reference flight trajectory and minimizing the imbalance between kinetic and potential energies to stabilize the rate of descent (or climb). Simulation results demonstrate that the implementation of this method provides robust resilience to external dynamic disturbances, mitigates the human factor, and enables mission execution under adverse weather conditions without rigid dependence on ground-based airfield infrastructure. Future research will focus on scaling the approach to multi-agent systems, integrating adaptation methods based on random projections, and field testing on fixed-wing platforms.

Keywords: *autonomous mobile nodes, autonomous takeoff and landing (ATOL), total energy control system (TECS), energy state, atmospheric turbulence, functional stability, aircraft survivability.*

Cite: Volkov O.Ye., Popov I.V. Energy-centric Control for Autonomous Mobile Nodes to Enhance Functional Stability under Turbulent. *Information Technologies and Systems*. 3 (9). 2026. 47—61. https://doi.org/10.15407/intechsys.2026.03.047

Introduction

In recent years, unmanned aerial vehicles have evolved into a distinct class of complex dynamic systems characterized by high functional density and scalability in application. The integration of advanced sensory instruments, including multispectral and inertial measurement subsystems, has enabled the continuous generation of large data arrays regarding flight parameters, onboard system status, and environmental characteristics.

A key factor in this qualitative transition has been the implementation of high-performance onboard computing and communication complexes capable of real-time processing, aggregation, and interpretation of sensory information using filtering, state estimation, and adaptive forecasting methods. This has significantly reduced latency within the control loop and enhanced the reliability of information support for decision-making.

Consequently, the necessary prerequisites have been established for a substantial increase in flight efficiency through the development and implementation of high-precision automatic control systems. A defining feature of autonomous mobile nodes (AMNs) is the ability to perform autonomous maneuvering, following a defined route. This alleviates the need for ground station operators to constantly monitor numeros motion parameters (flight in the case of UAVs, movement in the case of ground systems, surface and underwater travel in the case of water-based AMNs, etc.). Instead, they start with the initial, final and intermediate points of the route along with several additional characteristics of the AMN movement. The remaining parameters are computed by the onboard control system and transmitted to the respective actuators.

Autonomous UAV flight encompasses stages such as automatic take-off and landing, trajectory calculation, and subsequent path following, integrated with high-level decision-making processes depending on mission objectives. Every flight includes two stages characterized by both intensive maneuvering and limited control resources required to reach specific terminal states. Every nominal UAV flight is inherently accompanied by the essential stages of launch (take-off) and landing.

For modern aviation complexes, a degradation in control precision can be observed during take-off and landing under atmospheric turbulence, manifesting as increased deviations from set flight regimes and reduced stability in regulation loops. Such systems demonstrate insufficient adaptability to high-frequency turbulent effects, leading to accumulated control errors, increased load on actuators, and a decline in overall flight stabilization efficiency.

Literature Review

Currently, considerable attention is paid to the UAV take-off and landing methods development and implementation. There are several main methods of UAV take-off: hand launch; use of a catapult; vertical take-off; “aircraft-style” take-off [3–6].

Launching a UAV glider using human physical strength, without specialized devices, is carried out when the UAV weighs less than 5 kg. The main advantage of the method is simplicity, but at the same time the main disadvantage is safety for both the glider itself and the operator at the UAV launch.

Today, a significant number of UAVs are launched using catapults. But this method has both advantages and disadvantages. For example, a gunpowder catapult, for all its positive characteristics, such as simplicity, reliability and power availability also has significant disadvantages, such as lack of stealth, increased danger to service personnel. A gunpowder catapult is practically irreplaceable during the launching of heavy UAVs with a jet engine, but its use for launching mini UAVs is not advisable [6, 7].

Another take-off method is a vertical take-off. Among the existing UAVs, a special group is made up of UAVs that have the ability to take-off and land vertically. This ability of UAVs not only significantly simplifies the problem of its basing, but also expands the capabilities of UAVs both in terms of areas of application and tactics of its usage. When designing automatic control systems for such UAVs, difficulties arise in ensuring their stabilization around the center of mass. Additionally, there is a large fuel consumption during the vertical take-off procedure, which shortens the radius of application of the UAV [8].

Take-off according to the aircraft pattern can be carried out automatically or under the operator control. Known methods of UAV landing [9, 10] can be reduced to such basic schemes as: landing like an airplane (on a runway); landing like a helicopter (on a site); landing with a parachute; landing in a capture device.

For aircraft-type UAVs, classic landing systems are used that are also used for a manned aircraft landing, for example, such as the course-glide system and centimeter-range landing systems.

The landing process is divided into five stages: descent, leveling, hold-off, and rollout. During the descent, the UAV approaches the ground at a safe speed. The flare stage is designed to offset the vertical rate of descent, during which the UAV is transferred to horizontal flight mode. During the holding phase, the flight speed at a constant altitude is further offset due to an increase in the drag coefficient. The developed technology for autonomous take-off of aircraft-type UAVs conditionally divides the take-off process into three phases, showing the sequence of the main stages of UAV take-off from the beginning of the ground roll to the transition to the route (Fig. 1).

In order to land at a designated or intended location, operators perform complex calculations to maneuver the UAV horizontally and vertically during the landing procedure [10].

Methods for systems that provide autonomous take-off and landing of various type UAVs are proposed at [11, 12]. Such systems are called ATOL, which is an acronym for the words Autonomous Take-Off and Landing. Take-off and landing without operator intervention will sig-

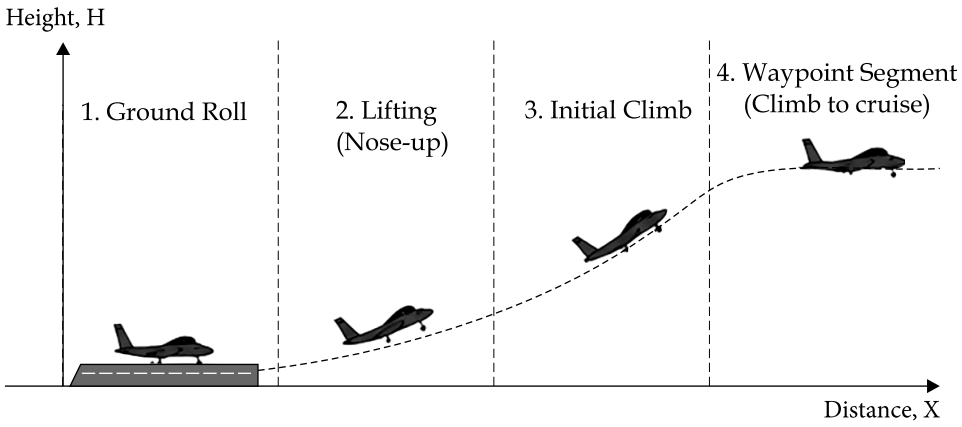


Fig. 1. Stages of UAV take-off

nificantly simplify the simultaneous use of several vehicles. The autonomous take-off and landing function will in the future become a standard function in an advanced ground control system for UAVs. This function minimizes errors caused by the human factor during the take-off and landing stages of UAVs and reduces the cost of operator training.

It should be noted that at the core of the conflict within non-autonomous aviation complexes lies the degradation of control precision under atmospheric turbulence, which leads to a decrease in the operational efficiency of unmanned aviation. Classical approaches, oriented toward rigid adherence to predefined trajectories, demonstrate insufficient adaptability to high-frequency stochastic environmental disturbances [13]. To resolve this issue, an approach based on the intellectualization of take-off and landing processes is proposed, transitioning from trajectory-based to energy-centric control [14]. Unlike traditional systems that focus on the geometric parameters of motion, such as the virtual glide slope, the proposed concept utilizes the aircraft's energy state as a fundamental control invariant. This approach provides inherent robustness to the system by minimizing the imbalance between the kinetic and potential components of total energy, rather than attempting direct compensation for every individual disturbance [15]. The implementation of energy-centric control achieves a comprehensive systemic effect, ensuring the intelligent compensation of external disturbances by interpreting them as fluctuations in the system's energy budget. This reduces the human factor by delegating complex tasks to algorithms and enhances the overall survivability of unmanned aerial vehicles by transforming adverse meteorological conditions from a category of critical constraints into a category of controllable environmental parameters. Thus, autonomous energy-state management serves as a systemic mechanism for increasing the autonomy and functional stability of unmanned aircraft systems in conditions of uncertainty.

Autonomous Control of the Uav on the Take-Off Stage

At the take-off stage, it is critically important to ensure efficient acceleration within the runway (RWY) limits, followed by a transition to a safe climb gradient as determined by airworthiness standards and the presence of obstacles along the flight path. Simultaneously, during the final landing phase, there arises a need for the precision dissipation of kinetic energy to a level that ensures safe taxiing and the accident-free termination of the flight mission. Both stages are viewed as processes of dynamic transformation of the aircraft's energy state under conditions of limited temporal and spatial resources.

To ensure the theoretical rigor of the proposed approach, the optimization criteria for synthesizing the control laws are formalized within the UAV state space. The total energy of the aircraft's motion is defined as the sum of its kinetic and potential components:

$$E_{tot} = 1/2mV^2 + mgh.$$

The cost function of the adaptive algorithm is formulated as a problem of minimizing a quadratic performance index over a finite time interval:

$$J = \int_{t_0}^{t_f} \left(\alpha \Delta E_{tot}^2(t) + \beta \Delta E_{bal}^2(t) + \gamma u^2(t) \right) dt,$$

where:

- J is the cost function (generalized performance index) that the UAV onboard computer attempts to minimize;
- [t_0, t_f] is the time interval over which the integral computes the cumulative "cost" of all errors and control expenditures;
- $\Delta E_{tot}(t) = E_{tot}(t) - E_{ref}(t)$ represents the total energy error of the aircraft, reflecting the deviation of the UAV's actual total energy from the target value defined by the virtual glide slope;
- $\Delta E_{bal}(t)$ is the energy imbalance, which accounts for how the energy is distributed between its kinetic and potential components;
- $u(t)$ is the control energy, represented as a control signal vector consisting of changes in control surface positions (pitch) and engine thrust;
- α, β, γ, are the autopilot tuning coefficients (weighting factors).

The parameter $\Delta E_{tot}(t)$ represents the current deviation of the total energy from the reference profile of the virtual glide slope, whereas $\Delta E_{bal}(t)$ determines the instantaneous imbalance between the airspeed (kinetic) and altitude (potential) channels. The control vector $u(t)$ forms coordinated commands for adjusting engine thrust and the pitch angle, while the weighting coefficients α, β, γ ensure the asymptotic stability of the closed-loop system under high-frequency stochastic atmospheric disturbances. The developed technology for autonomous take-off of aircraft-type UAVs conditionally divides the take-off process into three phases, illustrating the sequence of the main stages of UAV take-off from the beginning of the ground roll to the transition to the route (Fig. 1).

Phase I lasts from the beginning of the runway run-up to the set of take-off speed V_{to} = 30 m/s. During this stage, the UAV roll angle γ and pitch υ are stabilized at zero by the control laws until the take-off from the runway moment. The thrust value is set to the take-off value.

Phase II begins of the stage occurs when the UAV reaches the take-off speed V_{to} = 30 m/s. The UAV takes off from the runway. In this case, the pitch angle is set to 5°. The roll angle is controlled to stabilize the UAV flight path (ψ), which at this stage should be equal to the runway course (ψ_{rw}). The end of the stage occurs when the take-off height H_{to} = 50 m is reached. The thrust retains the take-off value.

Phase III begins after reaching the take-off altitude, the UAV is controlled using algorithms that are provided for UAV flight control. Namely, altitude and speed control can be performed using the UAV full energy control method, which produces pitch angle control signals υ_{cmd} and engine thrust δ_{th}, trajectory control can be performed using nonlinear adaptive roll angle control logic, which operates in the UAV flight mode along waypoints and produces UAV roll angle control signals (γ_{cmd}).

Autonomous Control of Unmanned Aerial Vehicle on the Landing Stage

Any UAV landing system, regardless of the chosen implementation strategy, must ensure the resolution of two fundamental systemic tasks. First is the task of precision guidance of the UAV to a specified spatial point, while adhering to the boundary values of orientation angles, as well as linear and angular velocities, which corresponds to the classical formulation of the terminal control problem. Second is the task of the complete dissipation of the aircraft's residual kinetic energy, provided that its structural integrity and functionality are preserved.

The instrumental framework used for the informational support of the landing stage for fixed-wing UAVs includes acoustic sensors (sonars) and laser rangefinders for high-precision altitude determination, satellite navigation system receivers, as well as video cameras for visual orientation or the implementation of computer vision systems, which collectively form the data field for automatic landing. The implementation of the energy-centric approach allows for the integration of data from these heterogeneous sensors into a unified energy-state model, ensuring control stability even under conditions of temporary degradation of individual information channels.

The developed UAV landing technology is designed to perform UAV landing in autonomous mode when the UAV control system is given an approach command at any time and at any flight trajectory interval. A significant difference between the developed technology and those described in [11-15] is that such technology uses algorithms implemented in widely used autopilots to calculate the landing maneuver before the UAV leveling stage. For example, altitude and speed control can be performed

using the UAV full energy control method, which produces pitch angle control signals υ_{cmd} and engine thrust δ_{th}. Trajectory motion control can be performed using nonlinear adaptive roll angle control logic that produces the UAV roll angle control signals γcmd.

To enable autonomous landing, the UAV autopilot generates an array of virtual glide slope parameters based on the runway (RWY) threshold coordinates, heading, glide slope intercept altitude, and the rollout point. These data are essential for ensuring the stable operation of the UAV control algorithms, spatial synchronization, and the formation of the landing course according to the virtual glide slope geometry (Fig. 2). Additionally, the following key trajectory nodes are defined programmatically: the landing decision point — the UAV's location at the moment the approach command is received, which triggers the nonlinear adaptive roll control logic to intercept the pre-landing flight level; and the touchdown point—a point on the runway where the virtual glide slope passes at a distance d from the threshold. The distance d is determined by the specified glide slope angle and flare altitude, and is calculated using the following formula:

$$d = h_в / tg\mu,$$

where $h_в$ — leveling height (height above the runway end point at which the UAV leveling (flare) phase begins); μ — virtual glide slope angle;

• glidepath point is the point of UAV entry into the virtual glidepath, which is located at the height h_{ge} of the virtual glidepath.

The developed autonomous UAV landing technology works with the following parameters: $h_в$ = 3m, μ = 4, d = 42.9 m.

The glide slope intercept point and the rollout point define a functional spatial segment essential for ensuring the UAV's precision entry into the virtual glide slope window at a target altitude h_{ge}, aligned with the runway (RWY) vector. The length of this interval is a dynamic parameter adapted to the temporal constraints of the landing operation. It is determined by the UAV's approach angle relative to the RWY axis and its maneuvering capabilities; specifically, a sharper intercept angle requires a longer distance to complete transition processes and achieve course stabilization, though it must not fall below the technical minimum required for the turn. The target flight altitude within this segment is fixed at the glide slope entry level h_{ge}, allowing for the minimization of energy state fluctuations before the commencement of the final descent.

To prevent runway excursions or off-runway landings, the nonlinear adaptive roll control logic is integrated with a dynamic lateral offset compensation mechanism (activated after passing the glide slope intercept point). This mechanism provides precision heading adjustments to align the aircraft parallel to the longitudinal axis of the RWY with minimal lateral deviation. As a result of the synergetic operation of both algorithms, the UAV stabilizes on the final approach path after passing the glide slope point, maintaining the trajectory under zero-roll and zero-sideslip con-

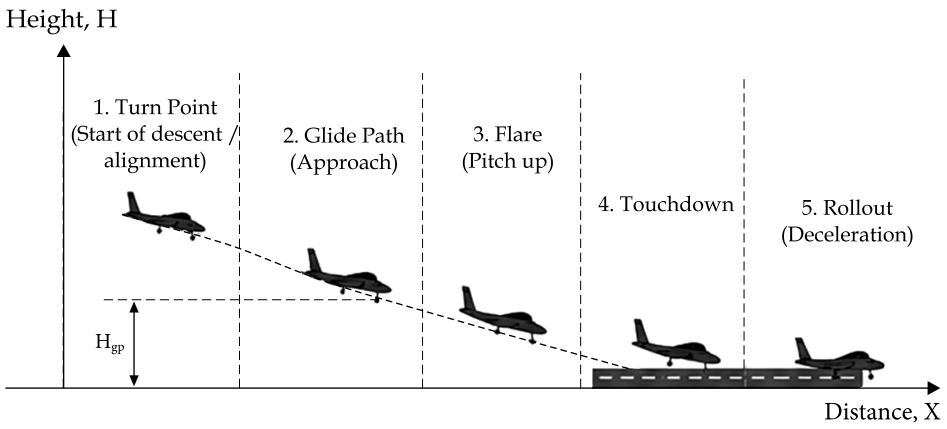


Fig. 2. Stages of UAV landing

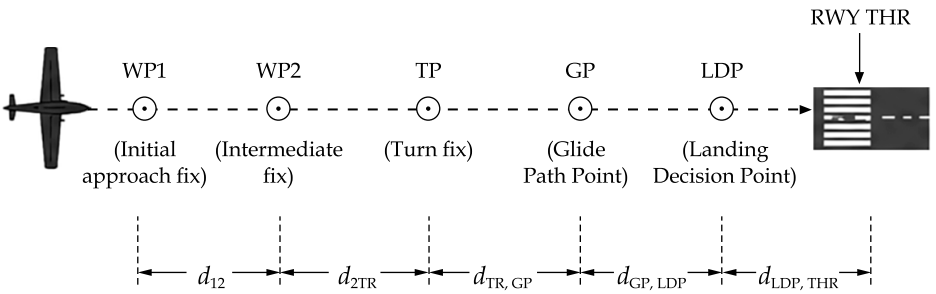


Fig. 3. Horizontal structure of the UAV landing approach route

ditions to ensure a safe touchdown. Such intelligent stabilization is critical for neutralizing the impact of sudden lateral wind gusts, which the system interprets as energetic perturbations of the motion vector.

A diagram of the UAV trajectory control is represented on Figure 3. In this case, UAV 1 and UAV 2 flew along a given trajectory at waypoints. At the moment of passing waypoint 1 for UAV 1 and waypoint 3 for UAV 2, a command to land was received. The dashed lines show the new automatically calculated approach trajectories in the UAV control system, in which the next waypoint is chosen also as the turn point.

The nonlinear adaptive roll control logic initiates the aircraft's transition onto a virtual trajectory connecting the decision point with the rollout point. Upon reaching a distance of 150 m, an iterative waypoint switching procedure is activated: first, to intercept the segment between the rollout point and the glide slope intercept point, and subsequently, to guide the UAV to the final touchdown location (Fig. 4). Simultaneously, in the vertical plane, the Total Energy Control System (TECS) performs precision monitoring of altitude and airspeed, ensuring motion stabilization along the target profile throughout all stages of the landing operation. Vertical descent parameters are determined by the platform type and its dynamic potential, while the flight itself is executed at a constant landing speed $V = V_{set}$.

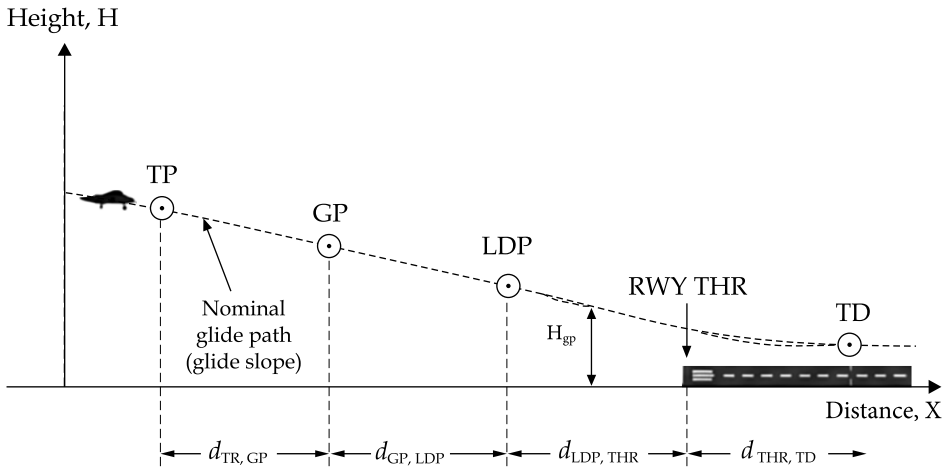


Fig. 4. Vertical profile of the UAV landing approach

After passing the runway end point, the control algorithm sets the pitch angle value to 0° and operates in the mode of holding this value, the engine thrust is set to 0 ($\delta_{thr} = 0$). Upon passing the end of the runway, the target flight speed of the UAV drops to zero (Fig. 4).

During the holding phase, due to increasing drag, the speed and flight altitude decrease, the UAV touches the runway surface, performs the run-up phase and makes a final stop within the runway.

Analysis of the Efficiency of Autonomous Uav Total Energy Control During the Takeoff Phase

The implementation of autonomous control algorithms based on the principles of controlling the UAV's energy status allows moving from the manual control stochastic nature to a deterministic process with a high level of repeatability. A feature of the proposed approach is the distribution of control logic according to the phases of flight dynamics.

During the I and II stages, the main advantage is to minimize the risk of accidents caused by untimely reaction to crosswinds during the run. The key parameters are identified at Table 1:

• Runway heading error ($\Delta\psi_{rw}$), defined as the angular difference between the direction of actual UAV movement (track angle) and the run-

Table 1. **Take- off stages performance metrics**

Take-off stage	Name, measurement units of the parameter	Manual control	Autonomous control
I stage	Runway flight path error ($\Delta\psi_{rw}$), °	± 3.0…5.0	± 0.5…1.0
II stage	Pitch angle accuracy ($\Delta\upsilon$), °	± 2.0…3.0	± 0.2…0.5
III stage	Full energy error ΔE_{tot}, (m²/s²)	± 15…20	± 2.0…4.0

way axis, which characterizes the accuracy of trajectory maintenance during the run-up, including the impact.

• Pitch angle error ($\Delta\upsilon$) is defined as the absolute deviation of the current pitch angle from the set value υ_{ref} at the lift-off moment, which is important to prevent a stall or tail strike.

On the stage III of take-off and during landing, the Total Energy Control System (TECS) method was applied [16], where the key metrics were defined as:

• Total energy error (ΔE_{tot}): defined as the deviation between the set and actual values of the total mechanical energy of flight ($E_{tot} = E_{pot} + E_{kin}$), which characterizes the efficiency of thrust and pitch control within the TECS under the influence of external disturbances.

Traditional control systems can enter a mode where the altitude contour requires an increase in pitch, and the speed contour requires a thrust increase that leads to overshooting and irrational energy consumption. Therefore, to increase the UAV durability, it is appropriate to use a full-energy control system. Its difference is that the altitude and speed control channels do not operate in isolation, TECS integrates them into a single energy contour. It allows the algorithm to harmonize the operation of the engine ($\Delta\delta_{th}$) and elevator ($\Delta\upsilon_{cmd}$), considering the vehicle as a holistic system that exchanges kinetic energy for potential and vice versa. This approach eliminates the "conflict" of contours in a turbulent environment, prevents overshooting and ensures a stable flight profile under difficult meteorological conditions.

In general, the transition to energy-centric autonomous control provides a significant unmanned aircraft operational efficiency increase. Quantitative analysis of the indicators confirms that the accuracy of trajectory maintenance and the softness of the landing touchdown increase compared to manual control mode. It not only reduces the working load of the operator, but also directly affects the technical resource of the glider.

The implementation of autonomous energy state control algorithms allows to transfer the takeoff and landing process from the category of subjectively controlled operations to the dimension of high-precision technological processes. The considered approach to automation provides rigid stabilization of spatial position and course that reduces risks associated with untimely operator reaction. This guarantees high repeatability of takeoff and minimizes the probability of emergency situations, such as premature stalling or runway overrun.

Discussion of the Results

The integration of autonomous take-off and landing algorithms demonstrates a qualitative transition from stochastic manual control to a deterministic technological process. The analysis shows that during I and II stages the algorithm provides rigid stabilization of roll and pitch that minimizes the risks associated with the human factor.

The transition to stage III and the subsequent landing phase highlight the main advantage of the full energy control system, where, unlike traditional PID-based architectures, TECS harmonizes the pitch (Δv) and thrust ($\Delta\delta_{th}$) control signals. By considering the UAV as a single energy system that balances kinetic and potential energy, the algorithm eliminates control conflicts in a disturbed environment.

The results of the conducted analysis indicate a significant reduction in total energy error (ΔE_{tot}) and the stabilization of the vertical descent rate during landing, demonstrating the high predictability of the developed algorithms. These improvements directly translate into increased operational efficiency and overall UAV survivability under conditions of high environmental uncertainty. By neutralizing the human factor and effectively compensating for stochastic external disturbances, the proposed technology enables the reliable execution of missions in complex meteorological conditions that are typically critical for manual control or traditional automatic systems. A detailed experimental verification of the landing phase and the validation of the proposed mathematical models are the subjects of a separate extended study currently in preparation for publication.

To objectively evaluate the scientific novelty of the proposed technology, an analytical comparison was conducted between the developed energy-centric method — based on the Total Energy Control System (TECS) — and conventional Model Reference Adaptive Control (MRAC), as well as modern intelligent algorithms based on Reinforcement Learning (RL). Unlike AI-based methods, which exhibit high sensitivity to the completeness of the training dataset and present a "black box" problem due to the low physical interpretability of their models, the energy-centric approach is rooted in fundamental physical invariants of motion. This enables the achievement of a high level of robustness to critical wind gusts without requiring significant computational resources from the onboard computer. Compared to MRAC algorithms, which are prone to error accumulation and high-frequency oscillations during intensive maneuvering in a turbulent environment, the proposed logic ensures natural disturbance rejection through its direct interpretation as fluctuations in the system's energy budget (Table 2).

Despite the demonstrated efficiency, the operation of the proposed energy-centric control loop is constrained by several critical boundary conditions of both aerodynamic and hardware nature. First, the system's capacity for energy fluctuation compensation is directly limited by the actuator saturation effect and the dynamic range of the propulsion system. The algorithm operates under the assumption that the aerodynamic control surfaces and the engine possess sufficient power margins; therefore, in cases where wind-induced stochastic disturbances exceed the maximum available thrust of the propulsion system ($T_{\max}$), a degradation in flight stabilization quality inevitably occurs. Second, the stability of the non-linear adaptive roll control logic critically depends on the

Table 2. **Comparison of Adaptive Control Methods**

Control Approach	Computational Cost of Onboard Computer	Data/Training Dependency	Robustness to Wind Gusts	Physical Interpretability of Models
Conventional MRAC	Moderate	Low (Requires plant model)	Moderate (Prone to high-frequency oscillations)	High
AI/ Reinforcement Learning (RL)	Extremely High	Critically High (Massive datasets required)	High (Strictly within the trained domain)	Low ("Black box" problem)
Proposed Energy-Centric (TECS)	Low	None (Physics-invariant)	High (Inherent robustness)	Excellent (Direct energy-state control)

update frequency of the sensory subsystems, as continuous state estimation requires a minimum sampling rate of the information fusion matrix at 50 Hz to prevent phase lag under turbulent atmospheric conditions. Finally, a significant limitation is the aerodynamic configuration of the aircraft, since the current mathematical model is tailored exclusively for fixed-wing UAVs and their inherent monotonic profiles of kinetic and potential energy interchange, which precludes its direct transfer to multirotor platforms without a complete restructuring of the power distribution matrices.

Conclusions

The paper proposes a conceptually new approach to the autonomous take-off and landing of unmanned aerial vehicles (UAVs) based on the energy-centric control paradigm. By applying the energy-based flight control method, the developed technology eliminates the drawbacks of traditional systems, such as low precision in turbulent atmospheric conditions and stability degradation under high-frequency stochastic disturbances. The control criteria in this approach are the minimization of total energy deviation from the reference value set by a virtual glide slope, and the minimization of the imbalance between the kinetic and potential components of total energy, effectively utilizing the aircraft's energy state as a fundamental physical invariant. This approach provides inherent robustness to the autonomous system through the intelligent interpretation of external disturbances as fluctuations in the energy budget. Furthermore, the findings demonstrate a reduction in human-factor errors during take-off and landing by delegating cognitively demanding stabilization tasks to automated algorithms, which lowers operator requirements and training costs. The developed technology does not require complex landing maneuvers and significantly enhances operational autonomy across a wide range of initial conditions by eliminating the mandatory reliance on ground-based airfield infrastructure. This substantially expands the per-

missible conditions for routine and emergency landings, transforming complex meteorological factors from critical constraints into controllable environmental parameters. Consequently, it increases the flexibility, efficiency, responsiveness, as well as the overall survivability and functional stability of the UAV in uncertain environments. Future work will focus on scaling the technology for multi-agent systems (UAV swarms) of the fixed-wing type, ensuring compatibility with a broader range of existing autopilots, and implementing rapid adaptation methods based on random projections to create a unified intelligent control loop.

DECLARATIONS.

O.Ye. Volkov developed the core conceptual approach based on the Total Energy Control System (TECS) methodology, defined the control invariants, supervised the research, and revised the manuscript for critical intellectual content.

I.V. Popov designed the control algorithms for the takeoff and landing stages, developed the simulation models, analyzed the performance metrics under atmospheric turbulence, prepared the figures and tables, and wrote the original draft of the manuscript.

AI and Tools Usage. The authors acknowledge the use of the Gemini (Model 1.5 Flash/Pro) artificial intelligence system during the preparation of this manuscript. The involvement of the AI system was strictly limited to technical and linguistic aspects of material preparation in the following sections:

• Section "Analysis of the Efficiency of Autonomous UAV Total Energy Control During the Takeoff Phase": The AI system was utilized for the translation of specialized technical terms, ensuring their correspondence with international aerospace standards, and for the stylistic refinement of the description of the energy-state control approach.

• Section "Discussion of The Results": The AI system was employed for the linguistic optimization of the English text, professional stylistic editing, and verification of aerospace terminology compliance with IEEE standards.

The authors declare that the use of AI was confined solely to technical and linguistic enhancements. All scientific content, mathematical formulations, interpretation of simulation results, formulation of conclusions, and final verification of data accuracy were performed personally by the authors. The authors bear full responsibility for the reliability and integrity of the submitted work.

Volkov O.Ye. has a potential conflict of interests as a Deputy Editor-in-Chief of the Journal. Popov I.V. has no known competing financial interests or personal relationships conflicts of interests.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

1. Volkov O., Komar M., Volosheniuk D. Devising an image processing method for transport infrastructure monitoring systems. *Eastern-European Journal of Enterprise Technologies*, 2021, Vol. 4 (2(112)), 18–25. https://doi.org/10.15587/1729-4061.2021.239084
2. Yang P. A Review of Unmanned Aerial Vehicle Control Technology: Methods, Applications and Development Trends. *Applied and Computational Engineering*, 2025, Vol. 218, 171–182. https://doi.org/10.54254/2755-2721/2026.TJ31062
3. Gu H., LyuX., Li Z., Shen Sh., Zhang F. Development and experimental verification of a hybrid vertical take-off and landing (VTOL) unmanned aerial vehicle (UAV). *International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, 2017, 160–169. https://doi.org/10.1109/ICUAS.2017.7991420

4. De Oca A.M., Flores G. Unified controller for take-off and landing for a fixed-wing aircraft. *International Conference on Unmanned Aircraft Systems (ICUAS),* Athens, Greece, 2020, 473–479. https://doi.org/10.1109/ICUAS48674.2020.9213878
5. Ładyżyńska-Kozdraś E., Sibilska-Mroziewicz A., Sławomir C., Krzysztof F., Sibilski K., Wróblewski W. Take-off and landing magnetic system for UAV carriers. *Journal of Marine Engineering & Technology*, 2017, Vol. 16 (4), 298–304. https://doi.org/10.1080/20464177.2017.1369720
6. Liu Y., Wang Y., Li H., Ai J. Runway-Free Recovery Methods for Fixed-Wing UAVs: A Comprehensive Review. *Drones,* 2024, Vol. 8 (9), Article 463. https://doi.org/10.3390/drones8090463
7. Xiong H., Li T., Li H., Yu C. A Preliminary Research on Performance Prediction Model of Catapult Launched Take-Off for a Large Wingspan Unmanned Aerial Vehicle. *Complex Systems Design & Management,* Springer, Cham, 2021, 467–467. https://doi.org/10.1007/978-3-030-73539-5_37
8. Zou Y., Meng Z. Coordinated trajectory tracking of multiple vertical take-off and landing UAVs. Automatica, 2019, Vol. 99, 33–40. https://doi.org/10.1016/j.automatica.2018.10.011
9. Klochan A.E., Al-Ammouri A., Abdulsalam H.I.S. Advanced UAV landing system based on polarimetrie technologies. *International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD),* IEEE, 2017, 147–150. https://doi.org/10.1109/APUAVD.2017.8308796
10. Muskardin T., Balmer G., Persson L. et al.. A novel landing system to increase payload capacity and operational availability of high altitude long endurance UAVs. *Journal of Intelligent & Robotic Systems,* 2017, Vol. 88 (2), 597–618. https://doi.org/10.1007/s10846-017-0475-z
11. Kügler M.E., Heller M., Holzapfel F. Automatic take-off and landing on the maiden flight of a novel fixed-wing UAV. *Flight Testing Conference,* 2018, Article 4275. https://doi.org/10.2514/6.2018-4275
12. Steinleitner A., Frenzel V., Pfeifle O., Denzel J., Fichter W. Automatic Take-Off and Landing of Tailwheel Aircraft with Incremental Nonlinear Dynamic Inversion. *AIAA SCITECH Forum,* 2022, Article 1228. https://doi.org/10.2514/6.2022-1228
13. El Mobaraky A., Kouiss Kh., Chebak A. Total energy control system-based interval type-3 fuzzy logic controller for fixed-wing unmanned aerial vehicle longitudinal flight dynamics, *Aerospace Science and Technology*, 2025, Vol. 162, 1270–9638. https://doi.org/10.1016/j.ast.2025.110253
14. Fossen T.I. *Handbook of Marine Craft Hydrodynamics and Motion Control*. John Wiley & Sons, Inc., Chichester, UK, 2011. https://doi.org/10.1002/9781119994138
15. Weiser Ch., Gertjan L., Ossmann D. Flight Testing Total Energy Control Autopilot Functionalities for High Altitude Aircraft. *AIAA SCITECH Forum*, 2024, Article 2204. https://doi.org/10.2514/6.2024-2204
16. Jimenez P., Lichota P., Agudelo D., Rogowski K. Experimental Validation of Total Energy Control System for UAVs. *Energies*, 2020, Vol. 13 (1), Article 14. https://doi.org/10.3390/en13010014

Received 19.06.2026
Accepted 20.07.2026
Published 25.08.2026

О.Є. ВОЛКОВ, канд. техн. наук, старш. дослідник, директор,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0000-0002-5418-6723; alexvolk52@ukr.net

І.В. ПОПОВ, наук. співроб., аспірант,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0009-7961-9431; popigor7@gmail.com

ЕНЕРГОЦЕНТРИЧНЕ КЕРУВАННЯ АВТОНОМНИМИ МОБІЛЬНИМИ ВУЗЛАМИ ДЛЯ ПІДВИЩЕННЯ ФУНКЦІЙНОЇ СТАБІЛЬНОСТІ В УМОВАХ ТУРБУЛЕНТНОСТІ

Вступ. За останні роки безпілотні літальні апарати перетворилися на окремий клас складних динамічних систем, що характеризуються високою функційною щільністю та масштабованістю в застосуванні. Інтеграція передових сенсорних приладів, включно з мультиспектральними та інерціальними вимірювальними підсистемами, дала змогу безперервно генерувати великі масиви даних щодо параметрів польоту, стану бортових систем та характеристик навколишнього середовища. Ключовим фактором цього якісного переходу стало впровадження високопродуктивних бортових обчислювальних та комунікаційних комплексів, здатних обробляти, агрегувати та інтерпретувати сенсорну інформацію в реальному часі з допомогою методів фільтрації, оцінювання стану та адаптивного прогнозування. Отже, створено необхідні передумови для суттєвого підвищення ефективності польоту завдяки розробленню та впровадженню високоточних систем автоматичного керування. Рух автономних мобільних вузлів (АМВ) охоплює такі етапи, як автоматичний зліт та посадка, обчислення траєкторії та подальше слідування за траєкторією, інтегровані з процесами прийняття рішень високого рівня залежно від цілей місії. Для сучасних авіаційних комплексів під час зльоту та посадки в умовах атмосферної турбулентності може спостерігатися погіршення точності керування, що проявляється збільшенням відхилень від заданих режимів польоту та зниженням стійкості в контурах регулювання. Такі системи демонструють недостатню адаптивність до високочастотних турбулентних впливів, що призводить до накопичення помилок керування, збільшення навантаження на виконавчі механізми та зниження загальної ефективності стабілізації польоту. Тому у статті запропоновано концептуальний підхід до автономного керування рухом АМВ на основі методології повного керування енергією (*TECS*).

Метою роботи є підвищення експлуатаційної ефективності та живучості безпілотної авіації завдяки використанню енергетичного стану апарата як фундаментального інваріанта керування.

Результати. Запропонований підхід нівелює обмеження традиційних систем, зокрема їх високу чутливість до стохастичних збурень та втрату точності стабілізації під час турбулентності. Алгоритм керування оптимізовано за двома критеріями: мінімізацією відхилення повної енергії АМВ від опорної траєкторії польоту та мінімізацією дисбалансу між кінетичною та потенційною енергіями для стабілізації швидкості зниження (сходження).

Висновки. Результати моделювання свідчать, що впровадження методу забезпечує стійкість до зовнішніх динамічних збурень, мінімізує вплив людського фактора та дає змогу виконувати місії за несприятливих метеоумов без жорсткої залежності від наземної аеродромної інфраструктури. Подальші дослідження спрямовані на масштабування підходу для багатоагентних систем, інтеграцію методів адаптації на основі випадкових проєкцій та натурне тестування платформ із фіксованим крилом.

Ключові слова: *автономний мобільний вузол, автономний зліт і посадка (ATOL), повне керування енергією (TECS), енергетичний стан, атмосферна турбулентність, функціональна стабільність, живучість літальних апаратів.*

https://doi.org/10.15407/intechsys.2026.03.062
УДК 004.274

В.О. БОРОВИК, провідний інженер-програміст,
відділ інтелектуального управління,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0000-0001-8860-616X
vadymborovyk@gmail.com
Р.В. СЕМЕНОГ, старш. наук. співроб., заст. зав. лаб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0000-0002-6714-6444
ruslansemenoh8@gmail.com

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ СТВОРЕННЯ СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ В РОЗПОДІЛЕНИХ КОМП'ЮТЕРНО-КОМУНІКАЦІЙНИХ СЕРЕДОВИЩАХ

Проведено комплексний аналіз сучасних інформаційних технологій, що використовуються для побудови систем інтелектуального керування в розподілених комп'ютерно-комунікаційних середовищах. Розглянуто сучасні концепції штучного інтелекту, методи забезпечення автономності інтелектуальних систем, підходи до прийняття рішень у складних динамічних середовищах, а також технології багатоагентної взаємодії. Особливу увагу приділено технологіям машинного навчання, глибокого навчання, підкріплювального навчання, експертним системам, інтелектуальним агентам та багатоагентним системам. Проаналізовано проблеми функціонування інтелектуальних систем у розподілених мережах, пов'язані із затримками передачі даних, невизначеністю, інформаційною безпекою та масштабованістю. Визначено перспективні напрями розвитку систем інтелектуального керування на основі технологій штучного інтелекту, цифрових двійників, периферійних обчислень та семантичних комунікацій.

Ключові слова: *штучний інтелект, інтелектуальне керування, розподілені системи, багатоагентні системи, машинне навчання, прийняття рішень, автономні системи, комп'ютерно-комунікаційні середовища.*

Цитування: Боровик В.О., Семеног Р.В. Інформаційні технології для створення систем інтелектуального керування в розподілених комп'ютерно-комунікаційних середовищах. *Information Technologies and Systems*, Київ, 2026, Том 3 (9), 62–72. https://doi.org/10.15407/intechsys.2026.03.062

Вступ

Стрімкий розвиток інформаційно-комунікаційних технологій, хмарних обчислень, інтернету речей та кіберфізичних систем призвів до появи нових вимог до процесів керування складними технічними об'єктами. Сучасні комп'ютерно-комунікаційні середовища характеризуються високою динамічністю, великими обсягами даних, неоднорідністю інформаційних ресурсів та необхідністю функціонування реальному часі.

У таких умовах традиційні методи автоматичного керування демонструють обмежену ефективність через неможливість повного врахування невизначеностей, змін параметрів середовища та складних взаємозв'язків між елементами системи. Це обумовлює активне впровадження технологій штучного інтелекту, здатних забезпечувати адаптацію, самонавчання та автономне прийняття рішень.

Метою статті є аналіз сучасних інформаційних технологій, що використовуються для створення систем інтелектуального керування в розподілених комп'ютерно-комунікаційних середовищах, а також визначення перспективних напрямів їх подальшого розвитку.

Сучасні концепції інтелектуального керування

Інтелектуальне керування є міждисциплінарною галуззю, яка поєднує методи теорії керування, штучного інтелекту, аналізу даних та теорії прийняття рішень.

Основною особливістю інтелектуальних систем є здатність до:

- накопичення та аналізу знань;
- адаптації до змін зовнішнього середовища;
- прогнозування розвитку ситуації;
- самонавчання;
- автономного прийняття рішень.

Сучасні підходи до побудови інтелектуальних систем базуються на концепції замкненого циклу «сприйняття — аналіз — планування — дія». Саме така архітектура використовується в автономних робототехнічних комплексах, безпілотних транспортних системах, системах кіберзахисту та інтелектуальних мережах.

Одним із ключових напрямів розвитку є створення розподіленого інтелекту, в якому окремі вузли системи здатні самостійно приймати рішення та координувати свої дії з іншими учасниками мережі.

Методи забезпечення автономності інтелектуальних систем

Автономність є базовою характеристикою сучасних інтелектуальних систем.

Для забезпечення автономного функціонування система повинна реалізовувати такі функції:

- сприйняття навколишнього середовища;
- інтерпретацію отриманої інформації;
- формування моделей ситуації;
- планування поведінки;
- прийняття рішень;
- контроль виконання дій.

Особливе значення автономність має для робототехнічних систем, безпілотних літальних апаратів та розподілених мережевих комплексів.

У сучасних дослідженнях автономність розглядається як здатність системи функціонувати за умов неповної інформації, обмежених ресурсів та невизначеності зовнішнього середовища. Одним із перспективних напрямів є використання регульованої автономності, коли рівень самостійності системи може змінюватися залежно від умов функціонування [3].

Технології штучного інтелекту в системах інтелектуального керування

Машинне навчання є однією з базових технологій сучасних інтелектуальних систем. Основними напрямами його застосування є:

- класифікація ситуацій;
- прогнозування станів;
- виявлення аномалій;
- оптимізація процесів керування;
- підтримка прийняття рішень.

Особливого поширення набули методи:

- дерева рішень;
- випадкові ліси;
- метод опорних векторів;
- ансамблеві методи;
- баєсівські моделі.

Глибокі нейронні мережі забезпечують можливість аналізу великих обсягів неструктурованих даних.

До найбільш поширених архітектур належать:

- згорткові нейронні мережі (*CNN*);
- рекурентні мережі (*RNN*);
- *LSTM*-мережі;
- трансформери.

Вони широко використовуються для аналізу потоків даних, комп'ютерного зору, обробки природної мови та прогнозування складних процесів.

Навчання з підкріпленням дає змогу агентам формувати оптимальні стратегії поведінки шляхом взаємодії із середовищем.

Особливо перспективним є багатоагентне навчання з підкріпленням, яке дає змогу реалізовувати колективне прийняття рішень у розподілених системах. Основними проблемами такого підходу за-

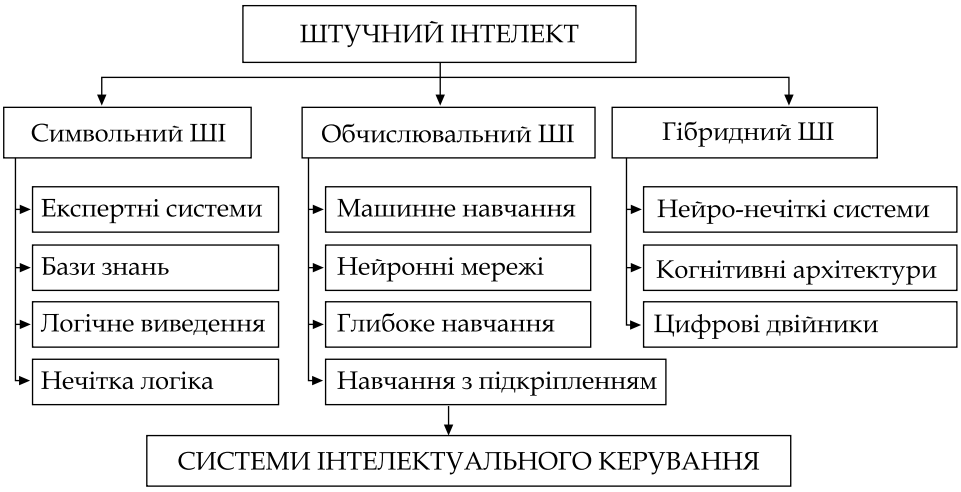


Рис. 1. Класифікація сучасних технологій штучного інтелекту, що використовуються при побудові систем інтелектуального керування

Таблиця 1. **Порівняльна характеристика основних технологій штучного інтелекту для систем інтелектуального керування**

Технологія	Переваги	Недоліки	Основні сфери застосування
Експертні системи	Пояснюваність рішень, використання знань експертів	Складність оновлення баз знань	Системи підтримки прийняття рішень
Нечітка логіка	Робота з невизначеністю	Потребує експертного налаштування	Автоматичне керування, діагностика
Штучні нейронні мережі	Висока точність прогнозування	Значні обчислювальні витрати	Розпізнавання образів, прогнозування
Машинне навчання	Адаптивність та самонавчання	Необхідність великих наборів даних	Аналітика даних, підтримка рішень
Глибоке навчання	Робота з неструктурованими даними	Складність інтерпретації результатів	Комп'ютерний зір, обробка мови
Інтелектуальні агенти	Автономність, гнучкість	Складність координації	Розподілені інформаційні системи
Багатоагентні системи	Масштабованість, відмовостійкість	Проблеми узгодження дій агентів	Мережецентричне керування
Навчання з підкріпленням	Оптимізація поведінки в реальному часі	Висока складність навчання	Робототехніка, автономний транспорт

лишаються координація агентів, масштабованість та нестабільність середовища.

Багатоагентні системи як основа розподіленого інтелекту

Однією з найбільш перспективних технологій інтелектуального керування є багатоагентні системи [7, 8].

Рис. 2. Узагальнена архітектура багатоагентної системи інтелектуального керування в розподіленому комп'ютерно-комунікаційному середовищі

Багатоагентна система являє собою сукупність автономних агентів, які взаємодіють між собою для досягнення спільної мети. Кожен агент має власні механізми сприйняття, аналізу інформації та прийняття рішень.

Основними перевагами багатоагентного підходу є:

- масштабованість;
- відмовостійкість;
- розподіленість обчислень;
- адаптивність;
- можливість самоорганізації [9].

Сучасні багатоагентні системи застосовують у:

- логістичних мережах;
- системах керування транспортом;
- промисловій автоматизації;
- енергетичних системах;
- робототехніці;
- військових системах керування [10].

Останні дослідження демонструють інтеграцію багатоагентних систем із технологіями інтернету речей та штучного інтелекту, що дає змогу створювати адаптивні мережеві екосистеми нового покоління.

Особливості функціонування інтелектуальних систем у розподілених комп'ютерно-комунікаційних середовищах

На відміну від централізованих систем керування, розподілені середовища характеризуються:

- затримками передачі інформації;
- втратами пакетів даних;

- неоднорідністю мережевої інфраструктури;
- високою динамічністю топології;
- інформаційною невизначеністю.

За таких умов ефективність функціонування системи залежить не лише від якості алгоритмів прийняття рішень, а й від здатності адаптуватися до змін параметрів мережі.

Особливого значення набувають технології периферійних обчислень (*Edge Computing*) та *Fog Computing*, які дають змогу переносити обчислювальні ресурси ближче до джерел даних і зменшувати затримки [11].

Одним із найбільш перспективних напрямів застосування технологій штучного інтелекту є побудова систем підтримки прийняття рішень. Такі системи призначені для аналізу великих масивів різнорідної інформації, формування рекомендацій та вибору найбільш ефективних альтернатив дій в умовах невизначеності.

На відміну від традиційних інформаційних систем, інтелектуальні системи підтримки прийняття рішень здатні не лише зберігати та обробляти дані, а й здійснювати їх інтерпретацію, прогнозування розвитку ситуації та формування обґрунтованих рекомендацій. Це особливо важливо для складних розподілених середовищ, де кількість можливих альтернатив може значно перевищувати можливості людини щодо їх оперативного аналізу.

Сучасні дослідження демонструють ефективність використання штучного інтелекту для ситуаційного аналізу, прогнозування розвитку подій, оцінювання ризиків та автоматизованого планування. Завдяки цьому забезпечується підвищення швидкості прийняття рішень, зменшення впливу людського фактора та покращення якості управління складними технічними системами.

Особливу роль у таких системах відіграють методи машинного навчання та інтелектуального аналізу даних, які дають змогу автоматично виявляти приховані закономірності у великих обсягах інформації та формувати моделі підтримки прийняття рішень у реальному часі.

Незважаючи на активний розвиток автономних технологій, людина залишається важливим елементом більшості сучасних систем керування. Тому одним із ключових напрямів розвитку інтелектуальних технологій є вдосконалення людино-машинної взаємодії.

Сучасний підхід передбачає формування концепції спільного інтелекту, відповідно до якої людина та система штучного інтелекту взаємодіють як єдина когнітивна система. При цьому інтелектуальна система забезпечує аналіз великих обсягів інформації, виконує прогнозування та генерує можливі варіанти рішень, тоді як людина здійснює стратегічну оцінку ситуації та приймає остаточне рішення.

Ефективність такої взаємодії значною мірою визначається рівнем довіри між користувачем та інтелектуальною системою. Саме тому останніми роками активно розвиваються концепції *Explainable Artificial Intelligence* (*XAI*) [12], спрямовані на підвищення прозорості

алгоритмів прийняття рішень та забезпечення можливості пояснення отриманих результатів.

Інтеграція людино-машинної взаємодії з технологіями штучного інтелекту дає змогу поєднати високу обчислювальну потужність сучасних інформаційних систем із когнітивними можливостями людини, що є особливо важливим для управління складними розподіленими системами.

Ефективність функціонування систем інтелектуального керування значною мірою залежить від якості оброблення вхідної інформації. У сучасних розподілених середовищах обсяги даних постійно зростають, що потребує використання спеціалізованих методів скорочення розмірності та структуризації інформації.

Одним із найбільш ефективних підходів є використання методів кластеризації даних. Кластеризація дозволяє автоматично групувати подібні об'єкти, параметри або атрибути, що суттєво зменшує складність подальших обчислень.

Особливу актуальність такі методи мають під час аналізу багатовимірних наборів даних, характерних для сучасних комп'ютерно-комунікаційних систем. У таких випадках традиційні методи скорочення розмірності часто виявляються недостатньо ефективними або потребують значних обчислювальних ресурсів.

Застосування кластеризації атрибутів дозволяє виявляти взаємозалежні параметри, об'єднувати подібні характеристики у групи та зменшувати кількість ознак, необхідних для прийняття рішень. У результаті досягається скорочення часу оброблення інформації, підвищення продуктивності інтелектуальних алгоритмів та покращення якості отриманих результатів.

Перспективним напрямом є поєднання методів кластеризації з алгоритмами машинного навчання та багатоагентними технологіями, що дозволяє створювати масштабовані системи підтримки прийняття рішень для складних розподілених комп'ютерно-комунікаційних середовищ.

Одним із сучасних напрямів розвитку інтелектуальних інформаційних технологій є перехід від концепції обчислювального мислення до концепції мислення на основі штучного інтелекту. Такий підхід передбачає використання не лише традиційних алгоритмів оброблення даних, а й механізмів роботи зі знаннями, контекстом та семантичними зв'язками між об'єктами предметної області.

На відміну від класичного обчислювального мислення, що орієнтується переважно на формалізацію задач та алгоритмізацію процесів їх вирішення, мислення на основі штучного інтелекту базується на використанні баз знань, типових сценаріїв, механізмів логічного виведення та аналізу неструктурованої інформації. Важливою складовою такого підходу є здатність враховувати контекст прийняття рішень та використовувати накопичений досвід попереднього функціонування системи.

Подальший розвиток цієї концепції пов'язаний із використанням когнітивних обчислень, які поєднують можливості машинного навчання, глибоких нейронних мереж, оброблення природної мови та інтелектуального аналізу даних. Когнітивні системи забезпечують не лише автоматизоване виконання окремих операцій, але й підтримку процесів формування знань, прогнозування розвитку ситуацій та вироблення рекомендацій щодо подальших дій.

Застосування когнітивних обчислень у розподілених комп'ютерно-комунікаційних середовищах дає змогу суттєво підвищити ефективність функціонування систем інтелектуального керування, особливо за умов невизначеності, неповноти інформації та високої динаміки зовнішнього середовища. Важливою тенденцією розвитку сучасних систем керування є перехід до мережецентричних архітектур, у яких функції збору інформації, оброблення даних, прийняття рішень та формування керуючих впливів розподіляються між численними вузлами комп'ютерно-комунікаційної мережі.

На відміну від централізованих систем, мережецентричне керування дозволяє забезпечити більш високий рівень живучості, масштабованості та адаптивності. Водночас ефективність таких систем значною мірою залежить від характеристик інформаційно-комунікаційного середовища.

Основою інформаційного обміну в сучасних комп'ютерних мережах є пакетна передача даних. Під час функціонування розподілених систем можливі втрати інформаційних пакетів, зміна порядку їх доставки, варіації затримок передачі та перевантаження окремих каналів зв'язку. Такі фактори можуть істотно погіршувати якість інтелектуального керування, особливо коли система функціонує в режимі реального часу.

Для підвищення стійкості функціонування інтелектуальних систем у розподілених середовищах доцільним є використання адаптивних алгоритмів керування, здатних враховувати поточний стан мережі та компенсувати вплив зовнішніх збурень. Важливу роль при цьому відіграють технології прогнозування мережевих затримок, механізми відновлення втрачених даних та алгоритми синхронізації розподілених інформаційних потоків.

Практична реалізація мережецентричного інтелектуального керування потребує використання розгорнутих баз знань щодо характеристик об'єктів керування, особливостей функціонування мережі та можливих сценаріїв розвитку ситуації. Класифікаційний аналіз поточних даних уможливлює структурну та параметричну адаптацію алгоритмів керування, забезпечуючи досягнення поставлених цілей навіть за умов значної невизначеності.

Перспективним напрямом подальших досліджень є інтеграція технологій штучного інтелекту, багатоагентних систем та програмно-конфігурованих мереж для створення високоефективних систем розподіленого інтелектуального керування нового покоління.

Проблеми інформаційної безпеки та довіри до інтелектуальних систем

Інтеграція штучного інтелекту в розподілені середовища породжує нові виклики у сфері кібербезпеки.

До основних загроз належать:

- підміна навчальних даних;
- атаки на моделі машинного навчання;
- витік конфіденційної інформації;
- компрометація агентів;
- маніпулювання результатами прийняття рішень [15].

У зв'язку з цим активно розвиваються напрями *Trusted AI*, *Explainable AI* та *Federated Learning*, орієнтовані на підвищення надійності та прозорості функціонування інтелектуальних систем.

Перспективні напрями розвитку

Проведений аналіз дозволяє виділити такі перспективні напрями досліджень:

- побудова систем розподіленого інтелекту на основі багатоагентних технологій;
- інтеграція штучного інтелекту з цифровими двійниками;
- розвиток семантичних комунікацій між агентами;
- використання федеративного навчання;
- створення адаптивних систем прийняття рішень у режимі реального часу;
- побудова мережецентричних систем керування нового покоління.

Особливий інтерес становлять семантичні мережі комунікацій, які орієнтовано не на передачу даних, а на передачу знань і намірів між інтелектуальними агентами [16].

Висновки

У статті проведено аналіз сучасних інформаційних технологій створення систем інтелектуального керування в розподілених комп'ютерно-комунікаційних середовищах.

Встановлено, що найбільш перспективними технологіями є машинне навчання, глибоке навчання, багатоагентні системи, навчання з підкріпленням та інтелектуальні агенти. Визначено, що подальший розвиток систем інтелектуального керування пов'язаний із впровадженням розподіленого інтелекту, семантичних комунікацій, цифрових двійників та федеративного навчання.

Отримані результати можуть бути використані як теоретична основа для розроблення нових архітектур інтелектуального керування складними розподіленими технічними системами.

ДЕКЛАРАЦІЇ

Внесок авторів: Боровик В.О. провів комплексний аналіз сучасних інформаційних технологій, що використовуються для побудови систем інтелектуального керування в розподілених комп'ютерно-комунікаційних середовищах. Семеног Р.В. проаналізував методи забезпечення автономності інтелектуальних систем.
ШІ та інструменти: Автори заявляють, що не використовували інструменти штучного інтелекту при підготовці даної статті.
Конфлікт інтересів: Автори заявляють, що вони не мають фінансових інтересів або особистих зв'язків, які могли б вплинути на представлену роботу.

ЛІТЕРАТУРА / REFERENCES

1. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. 4th ed., Pearson, 2021, 1166 P.
2. Wooldridge M. *An Introduction to MultiAgent Systems.* John Wiley & Sons, 2020, 365 P.
3. Cardoso R., Ferrando A. A Review of Agent-Based Programming for Multi-Agent computers10020016
4. Jaleel H., Stephan J., Naji S. Multi-Agent Systems: A Review Study. *Ibn Al-Haitham Journal for Pure and Applied Sciences,* 2020, Vol. 33 (3), 188–214. https://doi.org/10.30526/33.3.2483
5. Herrera M., Pérez-Hernández M., Parlikad A., Izquierdo J. Multi-Agent Systems and Complex Networks: Review and Applications in Systems Engineering. *Processes,* 2020, Vol. 8 (3), Article 312. https://doi.org/10.3390/pr8030312
6. Gronauer S., Diepold K. Multi-agent Deep Reinforcement Learning: A Survey. *Artificial Intelligence Review,* 2022, Vol. 55, 895–943. https://doi.org/10.1007/s10462-021-09996-w
7. Wong A., Back T., Kononova A., Plaat A. Deep Multiagent Reinforcement Learning: Challenges and Directions. *Artificial Intelligence Review,* 2023, Vol. 56, 5023–5056. https://doi.org/10.1007/s10462-022-10299-x
8. Volkov O., Tyshchuk O., Desiateryk O., Revunova E.,Rachkovskij D. A Linear System Output Transformation For Sparse Approximation. *Cybernetics And Systems Analysis*, 2022, Vol. 58 (5), 840−850. https://doi.org/10.1007/s10559-022-00517-3
9. Ma C. et al. *Trusted AI in Multi-agent Systems: An Overview of Privacy and Security for Distributed Learning*. ArXiv, 2022. https://doi.org/10.48550/arXiv.2202.09027
10. Guo S. et al. A Survey on Semantic Communication Networks: Architecture, Security, and Privacy. *IEEE Communications Surveys & Tutorials*, 2025, Vol. 27 (5), 2860–2894. https://doi.org/10.1109/COMST.2024.3516819.
11. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016, 800 P.
12. Weiss G. *Multiagent Systems*. MIT Press, 2013, 920 P.
13. Jennings N., Wooldridge M. Agent Technology: Foundations, Applications and Markets. Springer, 2012, 325 P.
14. Cao Y., Yu W., Ren W., Chen G. An Overview of Recent Progress in the Study of Distributed Multi-Agent Coordination. *IEEE Transactions on Industrial Informatics,* 2013, Vol. 9 (1), 427-438. https://doi.org/10.1109/TII.2012.2219061
15. Sutton R., Barto A. *Reinforcement Learning: An Introduction*. 2nd ed. MIT Press, 2018, 352 (338) P.
16. Bondar S.O., Kozhokhina O.V., Borovik V.O., Linder Ya.M., Korshunov M.V. Groups of unmanned aerial vehicles usage perspectives and peculiarities. *Control Systems and Computers*, 2018, Issue 5, 25–37. https://doi.org/10.15407/usim.2018.05.025

Отримано/Received 18.06.2026
Прийнято/Accepted 12.07.2026
Опубліковано/Published 25.08.2026

V.O. BOROVYK, Leading Software Engineer
Institute of Information Technologies and Systems of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0000-0001-8860-616X
vadymborovyk@gmail.com
R.V. SEMENOH, Senior Researcher, Deputy Head of laboratory
Institute of Information Technologies and Systems of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0000-0002-6714-6444
ruslansemenoh8@gmail.com

INFORMATION TECHNOLOGIES FOR CREATING INTELLIGENT CONTROL SYSTEMS IN DISTRIBUTED COMPUTER AND COMMUNICATION ENVIRONMENTS

Introduction. The increasing complexity of distributed computer and communication environments requires the development of advanced intelligent control technologies capable of operating under conditions of uncertainty, dynamic network topology, communication delays, and large-scale data processing. Traditional control approaches are often unable to provide the required level of adaptability and autonomy in such environments, which has led to the widespread adoption of artificial intelligence technologies.

The purpose of the paper is to analyze existing information technologies used for the development of intelligent control systems in distributed computer and communication environments and to identify promising directions for their further evolution.

Results. The paper reviews contemporary artificial intelligence technologies, including machine learning, deep learning, reinforcement learning, expert systems, fuzzy logic, intelligent agents, and multi-agent systems. Particular attention is paid to the issues of autonomous decision-making, distributed intelligence, adaptive control, and coordination of autonomous agents operating in network-centric environments. The advantages, limitations, and application domains of the considered technologies are analyzed and compared.

The study demonstrates that multi-agent architectures, reinforcement learning algorithms, and distributed artificial intelligence technologies provide the highest potential for the implementation of intelligent control functions in complex distributed environments. Furthermore, emerging approaches based on digital twins, edge computing, federated learning, and semantic communications significantly expand the capabilities of next-generation intelligent control systems.

Conclusions. The obtained results can serve as a theoretical foundation for the design and implementation of adaptive intelligent control systems capable of autonomous operation and real-time decision-making in distributed computer and communication infrastructures.

Keywords: *artificial intelligence, intelligent control systems, distributed computer and communication environments, distributed intelligence, machine learning, reinforcement learning, multi-agent systems, autonomous systems, decision support, network-centric control.*

CYBERSECURITY AND INFORMATION PROTECTION
КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

https://doi.org/10.15407/intechsys.2026.03.073
UDC 316.772.5

Ya.M. ANTONUK, Senior Researcher,
Institute of Information Technologies and Systems of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0005-7680-5950
ant@noc.irtc.org.ua
B.A. SHYIAK, Junior Researcher,
Institute of Information Technologies and Systems NAS Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0004-9130-7370
bosh@noc.irtc.org.ua
A.M. MATSAENKO, Senior Researcher, PhD (Engineering),
Institute of Information Technologies and Systems NAS Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0000-0003-1149-7318
matsaenko2015@gmail.com
S.L. ARKHANHELSKA, Researcher,
Institute of Information Technologies and Systems NAS Ukraine,
40, Hlushkova Akad. ave., 40, Kyiv, 03187, Ukraine
https://orcid.org/0009-0002-6889-8294
dep125@irtc.oeg.ua

FEATURES OF BUILDING A CYBER DEFENSE SYSTEM FOR A CAMPUS NETWORK OF A RESEARCH INSTITUTION

The paper examines the features of building a cyber-security system for a campus network of a research institution. The specifics of the functioning of the information and communication infrastructure of research institutions in comparison with corporate networks of commercial enterprises are analyzed. The main differences in architecture, user models, the nature of information flows and the profile of cyberthreats for research institutions are identified. A system of principles for building a cyber-security system for a campus network of a research institution is proposed, which includes adaptive network segmentation, a multi-level trust model, the principle of controlled openness, the principle of continuity of scientific services and distributed administration with centralized audit. The need to integrate organiza-

Cite: Antonyuk Ya.M., Shiyak B.A., Matsaenko A.M., Arkhanhelska S.L. PFeatures of Building a Cyber Defense System for a Campus Network of a Research Institution. *Information Technologies and Systems*. 3 (9). 2026. 73—84. https://doi.org/10.15407/intechsys.2026.03.073

tional, technical and procedural mechanisms for cyber-security within a single system for ensuring information security of a research institution is substantiated. A structural model of a cyber-security system for a campus network of a research institution is proposed, focused on ensuring the stability of the functioning of the information infrastructure in the conditions of modern cyberthreats.

***Keywords**: cyber-security, campus network, research institution, information security, network segmentation, Zero Trust, network monitoring.*

Introduction

Modern research activities critically depend on the stable functioning of information and communication infrastructure. Campus networks of scientific institutions provide access to scientific resources, electronic document management, specialized computing services, research results storage systems, cloud platforms, web resources, and international information systems for scientific interaction.

Simultaneously with the increase in the level of digitalization of scientific activity, the number of cyberthreats aimed at the information resources of scientific institutions is significantly increasing. The problem becomes particularly relevant in the context of hybrid cyberthreats, targeted attacks on scientific organizations, the spread of ransomware, compromise of accounts, and attacks on critical information infrastructure.

Unlike corporate networks of commercial enterprises, campus networks of research institutions have a number of specific features, including:

- open nature of academic interaction;
- a significant number of temporary users;
- the need for integration with external scientific resources;
- use of hybrid network infrastructure;
- availability of specialized laboratory segments;
- active use of wireless technologies and remote access;
- constant change in the configuration of network segments in accordance with scientific tasks.

Classic corporate cyber-security models, focused on rigid centralization, access restrictions, and static network structure, do not provide adequate efficiency in the conditions of scientific campus networks. This necessitates the development of adapted principles for building a cyber-security system for scientific and research institutions.

The purpose of the article is to study the features of the functioning of the campus network of a research institution and develop a system of principles for building cyberprotection for such a network, taking into account the specifics of scientific activity.

Analysis of Existing Approaches and Problem Formulation

The issue of ensuring cyber-security of information and communication systems is studied in a significant number of scientific works. The main attention is paid to the issues of network segmentation, access control,

perimeter protection, network activity monitoring, intrusion detection and building cyberincident response systems.

A significant part of modern approaches to building cyberdefense systems is based on corporate security models focused on commercial enterprises. Such models include:

- centralized administration;
- static network structure;
- clearly defined business processes;
- limited number of external integrations;
- minimizing external access;
- strict control of information flows.

For corporate networks, the priority is to ensure the confidentiality of financial, commercial, and service information. Accordingly, cyberdefense systems are focused on maximum isolation of information resources, centralized control, and minimizing changes in the network structure.

At the same time, research institutions operate in fundamentally different conditions. Campus networks of research institutions are characterized by:

— the need to ensure academic openness;
— high intensity of international information interaction;
— a significant number of mobile and temporary users;
— using users' own devices (BYOD);
— constant change in the structure of research segments;
— using heterogeneous software and hardware platforms;
— the availability of specialized scientific equipment.

A feature of scientific institutions is also the combination of administrative, scientific, laboratory and service infrastructure within a single information environment, usually in the form of a mixed campus network [1].

Thus, the use of classic corporate cyberdefense models without adaptation to the — specifics of scientific activity leads to:

— excessive difficulty in accessing information resources;
— reduction in the effectiveness of scientific interaction;
— reduced flexibility of network infrastructure;
— complexity of integrating external services;
— the emergence of a conflict between security requirements and the needs of scientific research.

Therefore, there is a need to develop a specialized approach to building a cyberprotection system for a campus network of a research institution.

Features of the Campus Network of a Research Institution

The campus network of a research institution is a complex multi-level information and communication system that ensures interaction between scientific departments, administrative services, laboratories, service systems, and external information resources.

A typical campus network structure of a research institution includes:

- core network segment;
- server infrastructure;
- user segments;
- wireless networks;
- guest segments;
- laboratory networks;
- remote access systems;
- cloud services;
- backup and archiving tools.

The core segment provides the functioning of backbone data channels, routing, centralized services, authentication and access control systems. It includes server equipment, routers, firewalls, monitoring systems, and backup systems.

The user segment combines employee workstations, laboratory equipment, mobile devices, and wireless access points. One of the features of scientific institutions is the significant number of non-unified software and hardware platforms used to conduct specialized research.

The wireless component of the network plays a particularly important role in the functioning of a modern scientific institution. The use of Wi-Fi networks ensures user mobility, supports guest access, connects mobile research complexes, and operates educational and scientific events.

At the same time, the widespread use of wireless technologies significantly increases the risks of unauthorized access, traffic interception, account compromise, and attacks on network infrastructure [2].

Another characteristic feature is the need to support open scientific interaction. Scientific institutions are actively integrating with external services, international computing platforms, scientific repositories, remote collaboration systems, and cloud resources.

Unlike commercial enterprises, where the concept of maximum isolation of information infrastructure prevails [3, 4], scientific institutions are forced to maintain controlled openness of the network.

Thus, the campus network of a scientific institution is characterized by:

— hybrid structure;
— high dynamism;
— multi-level architecture;
— mixed trust model;
— a significant number of external integrations;
— the need to simultaneously ensure the availability and security of resources.

Threats and Vulnerabilities of the Academic Campus Network

The specifics of the functioning of a campus network of a research institution form a special profile of cyberthreats and vulnerabilities.

The main organizational risks include:

— a significant number of temporary users;
— the difficulty of controlling the level of cyberhygiene of users;
— use of personal devices;
— decentralized administration of individual segments;
— insufficient software unification.

A feature of scientific institutions is the frequent change of user base. The network can be connected to graduate students, interns, participants in scientific projects, invited researchers, and representatives of third-party organizations.

Technical risks include:

— use of outdated equipment;
— the presence of unknown or specialized devices;
— use of open wireless networks;
— insufficient level of segmentation;
— connecting unauthorized equipment;
— use of vulnerable remote access services.

A separate problem is scientific equipment, which often operates under outdated operating systems or specialized software that does not support modern protection mechanisms.

The main information risks include:

— compromising the results of scientific research;
— leakage of confidential scientific data;
— violation of the integrity of scientific archives;
— unauthorized access to grant documentation;
— blocking of critical services by ransomware.

Particularly dangerous are ransomware attacks that can lead to loss of access to the results of many years of research, scientific archives and electronic document management systems, or leakage of personal data, as in the case of the University of Hawaii Cancer Center [5].

In addition, modern cyberthreats are characterized by a high level of automation and the use of artificial intelligence technologies to conduct phishing campaigns, compromise accounts, and bypass protection mechanisms [6].

In this regard, cyberdefense systems of scientific institutions must take into account not only classic threats to information security, but also specific risks associated with the functioning of an open scientific environment.

Principles of Building a Campus Network CyberDefense System

Taking into account the peculiarities of the functioning of research institutions, it is advisable to form a system of principles for building cyberprotection for the campus network.

Principle of adaptive network segmentation

Unlike corporate networks with a static structure, the campus network of a scientific institution must support the ability to dynamically form segments according to the needs of research groups and scientific projects.

Adaptive segmentation involves:

— isolation of critical services;
— separation of guest networks;
— allocation of laboratory segments;
— demarcation of administrative and scientific infrastructure;
— the possibility of rapid network reconfiguration.

The use of adaptive segmentation allows you to minimize the attack surface and limit the spread of cyber-security incidents between network segments.

The Principle of Multi-Level Trust

In a campus network, it is not possible to use a model of complete trust for internal nodes. Users, devices, and services must be treated as potentially untrusted regardless of their physical location on the network.

The implementation of this principle involves:

— using the Zero Trust concept [7];
— constant verification of user authentication;
— multi-factor authentication;
— node behavior control;
— access restrictions based on the principle of least privilege.

The multi-level trust model ensures increased resilience of the cyberdefense system to compromise of individual network segments.

The Principle of Controlled Openness

Scientific activity requires constant interaction with external information resources. Therefore, complete isolation of the network is impossible and contradicts the principles of functioning of the modern scientific environment.

The principle of controlled openness provides for:

— regulated external access;
— use of secure communication channels;
— control of access to public services;
— segmentation of external services;
— constant monitoring of external activity.

This approach allows for a balance between the openness of scientific infrastructure and the necessary level of cyberprotection.

The Principle of Continuity of Scientific Services

For a research institution, the continuity of services related to conducting research is of critical importance.

Critical services include:

— research results storage systems;
— electronic document management servers;
— backup systems;
— scientific repositories;
— computing clusters;
— web resources of scientific projects.

Ensuring continuity of operation involves:

— redundancy of critical components;
— regular backup;
— use of geographically remote copies;
— support for disaster recovery mechanisms;
— monitoring the status of the infrastructure in real time.

The Principle of Distributed Administration with Centralized Audit

In scientific institutions, individual laboratories and scientific units can use their own information resources and local administration mechanisms.

Complete centralization of management in such conditions is ineffective.

Therefore, it is advisable to use a distributed administration model with centralized audit, which provides for:

— local administration of individual segments;
— centralized event logging;
— centralized monitoring;
— unified security policies;
— centralized response to cyberincidents.

The Principle of Integration of Organizational and Technical Measures

The effectiveness of a cyberdefense system is determined not only by technical means, but also by the level of organizational support.

The organizational component should include:

— internal regulations;
— user instructions;
— incident response procedures;
— staff training;
— periodic audits;
— monitoring compliance with security policies.

The integration of organizational and technical mechanisms allows for a comprehensive approach to building a cyberdefense system.

Campus Network Cyber-security System Model

Based on the proposed principles, a multi-level model of the cyber-security system of the campus network of a research institution can be formed.

Structurally, this model includes:
1. Level of physical infrastructure.
2. Level of network interaction.
3. Level of services and information systems.
4. Access control level.
5. Level of monitoring and response.
6. Organizational level.

At the physical infrastructure level, protection is provided for server equipment, power supply systems, data transmission channels, and telecommunications equipment.

The level of network interaction includes:
- firewalls;
- VLAN segmentation;
- IDS/IPS systems;
- VPN technologies;
- network traffic control mechanisms.

The service level covers:
- postal systems;
- web resources;
- file storage;
- scientific information systems;
- cloud services.

The access control layer implements:
- centralized authentication;
- multi-factor authentication;
- privilege control;
- access policies.

The monitoring and response level includes:
- log collection systems;
- SIEM platforms;
- network activity analysis tools;
- incident response procedures.

The organizational level covers:
- regulatory documentation;
- audit procedures;
- user training;
- administration regulations.

The interaction of these levels forms a unified cyberdefense system aimed at ensuring the stability of the functioning of the information infrastructure of a scientific institution.

Practical Implementation of a CyberDefense System in a Scientific Institution

The practical implementation of a cyberdefense system should be based on a comprehensive approach that combines organizational, technical, and procedural mechanisms.

One of the key elements is the creation of a system support unit responsible for:

- network administration;
- infrastructure monitoring;
- incident response;
- user support;
- information security audit.

An important component of the system is the organization of centralized network monitoring. The monitoring system should provide:

- monitoring the status of network nodes;
- network traffic analysis;
- detection of abnormal activity;
- control of resource use;
- prompt informing of administrators.

Significant attention should be paid to logging security events. Centralized log storage allows:

- perform incident analysis;
- detect unauthorized access attempts;
- monitor user actions;
- generate statistics on security events.

To achieve rapid response and analysis of security incidents, it is advisable to implement an ontological expert incident management system [8].

To ensure the stability of the infrastructure, it is necessary to implement a backup system, which should include:

- regular backups;
- isolated storage of copies;
- backup data integrity control;
- periodic testing of recovery procedures.

An important aspect of ensuring cyber-security is increasing user awareness. Staff training should cover:

- cyberhygiene rules;
- detection of phishing attacks;
- safe use of email;
- rules for working with information resources;
- cyberincident response procedures.

In addition, it is necessary to conduct regular information security audits and testing of the security of the information infrastructure. It is also important to simulate social engineering attacks [9].

Conclusions

The article examines the features of building a cybersecurity system for a campus network of a research institution. It is shown that campus networks of research institutions differ significantly from corporate networks of commercial enterprises in terms of structure, user model, nature of in-

formation interaction and cyberthreat profile. It is established that the use of classical corporate models of cybersecurity without adaptation to the specifics of the scientific environment is not effective enough.

A system of principles for building cybersecurity for a campus network of a research institution is proposed, which includes the principle of adaptive network segmentation, of multi-level trust, of controlled openness, of continuity of scientific services, of distributed administration with centralized audit, and principle of integration of organizational and technical protection mechanisms.

The scientific novelty of the work lies in the formalization of the principles of building a cyber-protection system for a campus network of a scientific institution, taking into account the peculiarities of the academic information environment, the need to support open scientific interaction, and the dynamic structure of user segments.

The practical significance of the results obtained lies in the possibility of using the proposed approach to build and modernize cyberdefense systems in institutions of the National Academy of Sciences of Ukraine, higher education institutions, and other research organizations.

DECLARATIONS

***Author contributions*:** Antonyuk Ya.M. analyzed existing approaches to building cybersecurity systems for a campus network of a research institution and identified threats and vulnerabilities of an academic campus network. Shyak B.A. highlighted the features of a campus network of a research institution and the principles of building a campus network cyber protection system. Matsaenko A.M. demonstrated a model of a campus network cybersecurity system. Arkhanhelska S.L. presented a practical implementation of a cyber protection system in a scientific institution

***Use of AI and Tools Usage*:** The authors declare that artificial intelligence tools were used only for language editing and spell checking and were not used for scientific analysis of information and interpretation of results.

***Conflict of Interest*:** The authors declare that they have no financial interests or personal relationships that could influence the presented work.

REFERENCES

1. Antoniuk Ya.M., Shyiak B.A., Tkalya V.H., Arkhanhelska S.L. Telemetry As the Foundation of Predictable QoS in Hybrid Campus Networks. *Information Technologies and Systems*, 2026, Vol. 7 (1), 35–42. https://doi.org/10.15407/intechsys.2026.01.035
2. Scarfone K.A., Mell P.M. Guide to Intrusion Detection and Prevention Systems (IDPS). *National Institute of Standards and Technology Special Publication 800-94*, Gaithersburg, MD, 2007. https://doi.org/10.6028/NIST.SP.800-94
3. What Is Enterprise Network Security? A Complete Guide. URL: https://e.huawei.com/en/knowledge/2024/solutions/enterprise-network/enterprise-network-security [Accessed 25 May. 2026]
4. Enterprise Network Security: A Complete Guide. EPAM SolutionsHub. URL: https://solutionshub.epam.com/blog/post/enterprise-network-security [Accessed 25 May. 2026]
5. Data breach reported by University of Hawai‘i Cancer Center. UpGuard. URL: https://www.upguard.com/news/university-of-hawaii-cancer-center-data-breach-2026-03-02 [Accessed 25 May. 2026]

6. Zdrojewski K. AI-Powered Cyberattacks: A Comprehensive Review and Analysis of Emerging Threats. *Advances in IT and Electrical Engineering*, 2025, Vol. 31, 55–69.
7. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. *National Institute of Standards and Technology Special Publication 800-207*, 2020. https://doi.org/10.6028/NIST.SP.800-207
8. Rozlomii I.O., Babenko V.H., Holovnia V.M. Ontological expert system for identifying vulnerable components in security systems of critical infrastructure facilities. *Telecommunication and information technologies*, 2026, Issue 1, 180–187. https://doi.org/10.31673/2412-4338.2026.019017
9. Korshun N.V., Bondarchuk A.P., Skladannyi P.M., Sokolov V.Yu., Kryzhanivska T.M. Modeling and execution of social engineering attacks. *Telecommunication and information technologies*, 2026, Issue 1, 130–139. https://doi.org/10.31673/2412-4338.2026.019013

Received 26.05.2026
Accepted 20.07.2026
Published 25.08.2026

Я.М. АНТОНЮК, старш. наук. співроб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0005-7680-5950
ant@noc.irtc.org.ua
Б.А. ШИЯК, молодш. наук. співроб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0004-9130-7370
bosh@noc.irtc.org.ua
А.М. МАЦАЄНКО, канд. техн. наук, старший викладач,
ВІТІ імені Героїв Крут,
https://orcid.org/0000-0003-1149-7318
matsaenko2015@gmail.com
С.Л. АРХАНГЕЛЬСЬКА, наук. співроб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0002-6889-8294
dep125@irtc.oeg.ua

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ КІБЕРЗАХИСТУ КАМПУСНОЇ МЕРЕЖІ НАУКОВО-ДОСЛІДНОЇ УСТАНОВИ

Вступ. Сучасна дослідницька діяльність критично залежить від стабільного функціонування інформаційно-комунікаційної інфраструктури. Кампусні мережі наукових установ забезпечують доступ до наукових ресурсів, електронного документообігу, спеціалізованих обчислювальних сервісів, систем зберігання результатів досліджень, хмарних платформ, веб-ресурсів та міжнародних інформаційних систем для наукової взаємодії. Одночасно зі зростанням рівня цифровізації наукової діяльності значно зростає кількість кіберзагроз, спрямованих на інформаційні ресурси наукових установ. Проблема стає особливо актуальною в контексті гібридних кіберзагроз, цілеспрямованих атак на наукові організації, поширення програм-вимагачів, компрометації облікових записів та атак на критичну інформаційну інфраструктуру. На відміну від корпоративних мереж комерційних підприємств, кампусні мережі наукових установ мають низку специфічних особливостей. Класичні моделі корпоративної кібербезпеки, орієнтовані на жорстку централізацію, обмеження доступу та статичну структуру мережі, не забезпечують належної ефективності в умовах наукових

кампусних мереж. Це зумовлює необхідність розробки адаптованих принципів побудови системи кібербезпеки для науково-дослідних установ.

Метою статті є дослідження особливостей функціонування кампусної мережі дослідницької установи та розробка системи принципів побудови кіберзахисту для такої мережі з урахуванням специфіки наукової діяльності.

Методи. В статті сформовано систему принципів побудови кіберзахисту кампусної мережі.

Результати. Проведено аналіз специфіки функціонування інформаційно-комунікаційної інфраструктури наукових установ у порівнянні з корпоративними мережами комерційних підприємств. Визначено основні відмінності архітектури, моделі користувачів, характеру інформаційних потоків та профілю кіберзагроз для науково-дослідних установ. Запропоновано систему принципів побудови кіберзахисту кампусної мережі наукової установи, що включає адаптивну сегментацію мережі, багаторівневу модель довіри, принцип контрольованої відкритості, принцип безперервності наукових сервісів та розподіленого адміністрування з централізованим аудитом. Обґрунтовано необхідність інтеграції організаційних, технічних та процедурних механізмів кіберзахисту в межах єдиної системи забезпечення інформаційної безпеки наукової установи. Запропоновано структурну модель системи кіберзахисту кампусної мережі науково-дослідної установи, орієнтовану на забезпечення стійкості функціонування інформаційної інфраструктури в умовах сучасних кіберзагроз.

Висновки. Показано, що кампусні мережі наукових установ суттєво відрізняються від корпоративних мереж комерційних підприємств за структурою, моделлю користувачів, характером інформаційної взаємодії та профілем кіберзагроз. Встановлено, що використання класичних корпоративних моделей кібербезпеки без адаптації до специфіки наукового середовища є недостатньо ефективним.

Ключові слова: *кіберзахист, кампусна мережа, науково-дослідна установа, інформаційна безпека, сегментація мережі, Zero Trust, мережевий моніторинг.*

UDC 004.056:621.31
https://doi.org/10.15407/intechsys.2026.03.085

B.O. POKHODENKO, Senior Lecturer of the Department of Cybersecurity,
Kharkiv National Automobile and Highway University,
Yaroslava Mudrogo St., 25, Kharkiv, 61002, Ukraine
https://orcid.org/0000-0002-9995-7077
boris.pokhodenko@gmail.com

DEVELOPMENT OF RISK ASSESSMENT AND MINIMIZATION MODELS FOR CYBER INCIDENTS IN INTERCONNECTED AUTOMOTIVE AND POWER SYSTEMS

The paper investigates the critical problem of ensuring cyber resilience within the integrated ecosystems of automotive transport and energy infrastructure, which are becoming increasingly interdependent due to the mass adoption of electric vehicles and Smart Grid technologies. The study provides a comprehensive analysis of the threat landscape, focusing on specific attack vectors targeting electric vehicle charging stations (EVCS) and the communication protocols of the Vehicle-to-Grid (V2G) interface. It is demonstrated that vulnerabilities in the ISO/IEC 15118 and OCPP protocols can be exploited to initiate cascading failures that transcend the boundaries of the transport network and impact the stability of the regional power grid. The central contribution of this research is the development of a formalized mathematical model for multi-layer risk assessment, which utilizes a probabilistic approach to quantify the impact of cyber-physical attacks on system availability and data integrity. Unlike existing one-dimensional models, the proposed methodology accounts for the interconnectedness of nodes, where a security breach in a single vehicle or charging point acts as a catalyst for large-scale energy imbalances. The paper details a systematic risk minimization framework that integrates proactive and reactive measures: from the deployment of specialized intrusion detection systems (IDS) optimized for industrial control protocols to the implementation of adaptive load management algorithms that mitigate the effects of malicious demand-side manipulation. Simulation results presented in the study confirm that the proposed model effectively identifies high-risk convergence points with a sensitivity improvement of 15-20% compared to traditional NIST-based frameworks. The research findings provide a theoretical and prac-

Cite: Pokhodenko B.O. Development of Risk Assessment and Minimization Models for Cyber Incidents in Interconnected Automotive and Power Systems. *Information Technologies and Systems*. 3 (9). 2026. 85—101. https://doi.org/10.15407/intechsys.2026.03.085

tical basis for government agencies and critical infrastructure operators to develop robust cybersecurity strategies in the era of total digitalization of transport and energy assets. The developed models contribute to the creation of autonomous defense mechanisms capable of maintaining operational continuity under adversarial conditions.

Keywords: *cyber security, automotive transport, energy, risk assessment, Smart Grid, V2G, risk minimization, critical infrastructure, cascading effects, cyber resilience.*

Introduction

Relevance of the topic. The current stage of global economic development is characterized by a deep digital transformation of critical infrastructure, where the convergence of the automotive industry and the energy sector occupies a special place [1, 2]. The "Smart City" concept involves the massive introduction of electric vehicles (EVs) and the creation of an intelligent charging infrastructure that is not just a consumer of electricity but an active participant in the energy market through Vehicle-to-Grid (V2G) technology [3, 4].

However, this integration creates new vulnerabilities. A cyber-attack on the electric vehicle charging infrastructure or the communication protocols between the vehicle and the grid can lead not only to data leakage but also to physical destruction of equipment, disruption of power supply to entire regions, and threats to the life and health of citizens [5–7]. Modern challenges, such as the increase in the number of targeted attacks on IoT devices and industrial control systems (ICS), require the development of new approaches to assessing and minimizing risks that take into account the cascading nature of incidents in interconnected environments.

Analysis of recent research and publications. Issues of cybersecurity in the automotive industry are widely discussed in the works of international organizations and researchers, in particular in the ISO/SAE 21434 standard [8] and NIST recommendations [9, 10]. At the same time, the protection of the energy component (Smart Grid) is regulated by the IEC 62443 series of standards [11, 12]. However, most existing studies consider these systems in isolation. The synergy of risks arising during the interaction of EVs with the power grid remains insufficiently studied, especially in the context of implementing the new European NIS2 and DORA directives, which place high demands on the digital resilience of the transport and energy sectors [13].

Identification of previously unsolved parts of the general problem. A significant gap in current research is the lack of formalized mathematical models that allow for the quantitative assessment of risk as a single metric for an integrated system. Existing methods often do not account for the probabilistic nature of the transition of an attack from the transport protocol level to the physical level of energy distribution, which makes it impossible to effectively prioritize protective measures.

Formulation of the article's objectives. The objective of this study is to develop a comprehensive mathematical model for assessing and minimizing the risks of cyber incidents in interconnected automotive and pow-

er systems, which provides for the identification of critical nodes and the substantiation of adaptive protection methods to ensure the stability of critical infrastructure.

Analysis of the Current State and Architecture of Interconnected Transport and Energy Systems

Technological Convergence: V2X and Smart Grid Concepts. The modern integration of automotive transport into the energy sector is based on the V2X (Vehicle-to-Everything) concept, where the vehicle becomes an active participant in data and energy exchange [14]. Within this ecosystem, the Vehicle-to-Grid (V2G) component provides a bidirectional energy flow that allows electric vehicle (EV) batteries to be used for balancing peak loads in the grid [17]. Concurrently, the Vehicle-to-Infrastructure (V2I) framework enables continuous interaction with smart charging stations (EVSE) and road management systems [16], while the Smart Grid operates as an intelligent power network that coordinates thousands of these charging points by dynamically adapting to shifting demand [17]. From a cybersecurity perspective, this highly interconnected architecture creates a "distributed perimeter," where every single connection point of an EV to the grid serves as a potential entry point for an attacker [18].

Overview of Communication Protocols and Their Vulnerabilities. The security of interconnected systems depends on the reliability of data exchange protocols [19]. Among these, the ISO 15118 (Plug & Charge) international standard describes the interaction between the EV and the charging station, but although it involves the use of PKI (Public Key Infrastructure), the complexity of certificate implementation often leads to configuration errors [20]. Another primary mechanism is the OCPP (Open Charge Point Protocol), which operates between the charging station and the management system (CSMS), where vulnerable spots notably include the lack of encryption in legacy versions (1.6) and the risk of session hijacking [21].

Cybersecurity Regulatory Framework in Ukraine and the EU. In the context of this scientific work, it is important to consider modern requirements that are becoming mandatory for Ukrainian enterprises in the process of European integration. These frameworks include the NIS2 Directive (Network and Information Security), which establishes strict requirements for critical infrastructure entities in the energy and transport sectors. Additionally, the Cyber Resilience Act (CRA) requires that any digital product, including charging station controllers and onboard computers, has built-in protection based on the «security by design» principle. Finally, the ISO/SAE 21434 specialized cybersecurity standard for road vehicles regulates comprehensive risk management at all stages of the vehicle's life cycle [22].

Professional Standards and Industry Requirements. According to current professional standards in cybersecurity and automotive transport,

a specialist must not only possess methods of information protection but also understand the specifics of OT (Operational Technology) systems [23]. Risks in energy-transport systems differ from classic IT risks in that they have a direct impact on physical security (Safety) - for example, the possibility of causing a battery fire through manipulation of rapid charging parameters.

Detailed Information Flow Diagram in the "EV — EVSE — Smart Grid" System. Interaction in this system is multi-layered and covers several key interfaces , with the primary data flow aimed at ensuring user authentication, controlling charging parameters, and balancing the load on the power grid. Within these key nodes and communication channels, the EV ↔ EVSE (Electric Vehicle — Charging Station Interface) utilizes the ISO 15118 protocol to exchange data such as the State of Charge (SoC), maximum allowable current, contract identifier (Plug & Charge), and security certificates. Concurrently, the EVSE ↔ CSMS (Station — Cloud Management System Interface) relies on the OCPP 1.6/2.0.1 protocol to transmit point availability status, energy consumption records (MeterValues), error messages, and remote firmware updates. Furthermore, the CSMS ↔ DSO/DSO (Operator — Power Grid Interface) operates via the OpenADR or OSCP protocols to manage peak consumption forecasts, power limitation requests (Demand Response), and real-time tariffs. The complete flow diagram of this interaction proceeds as the electric vehicle initiates a request, after which the EVSE verifies the certificate via the CSMS, followed by the CSMS coordinating the power limit with the Smart Grid until the energy transfer finally begins.

Multi-level Analysis of V2G Network Architecture Vulnerabilities Based on the OSI Model. To understand the nature of cyber incidents in convergent systems, it is advisable to decompose the data exchange process between the EV and EVSE. Using the OSI reference model allows for clear localization of threats at each stage — from physical contact to application software.

The systematization of the main vulnerabilities, their corresponding protocols, and potential security consequences is presented in Table 1[24].

Detailed analysis of the data in Table 1.1 highlights critical system vulnerability points. Specifically, at lower layers (L1-L2), the primary danger lies in the physical accessibility of the equipment. The use of PLC (Power Line Communication) technology creates a specific "electromagnetic eavesdropping" vector, which is untypical for classic IT networks.

At the network and transport layers (L3-L4), session integrity is a critical aspect. Man-in-the-Middle (MitM) attacks at this stage can lead to the substitution of power limits transmitted from the power grid to the car, creating a risk of overloading local transformer substations.

The most significant risks are concentrated at the application layer (L7). Since the OCPP protocol uses web technologies (JSON via WebSockets), it inherits all vulnerabilities of modern web applications. SQL injection in this context is the most dangerous, as it allows an attacker to

gain control over the entire network of charging stations (EVSE) through the central management system (CSMS).

Experience in Implementing Monitoring Systems in Ukrainian Energy Companies. The implementation of cybersecurity monitoring systems (SOC — Security Operations Centers) in the Ukrainian energy sector has significantly accelerated after 2022. The main development vectors include the deployment of IDS/IPS at substations, where large distribution system operators (DSOs) have begun integrating intrusion detection systems specialized in industrial protocols (IEC 60870-5-104, IEC 61850) to detect anomalous commands to open breakers that could be simulated by attackers. Another critical vector is log centralization (SIEM) using SIEM-class systems (e.g., Splunk or ELK Stack), which allows for the correlation of events from charging hubs and general substations, thereby enabling the detection of "Distributed Energy Resource (DER) attacks" where massive simultaneous activation of charging stations could cause a frequency shift in the grid. Concurrently, cryptographic protection experience among Ukrainian companies shows a transition to using VPN tunnels with support for domestic encryption algorithms (according to DSTU) for communication between remote infrastructure objects and the central server. Finally, this process involves close cooperation with CERT-UA to ensure the constant monitoring of Indicators of Compromise (IoC), characteristic of attacks on energy systems (e.g., Industroyer2), integrated into automated corporate defense systems [25].

Threat Modeling and Mathematical Assessment of Cyber Risks

Formalization of the Adversary Model and Attack Vectors. To build a risk model, it is necessary to define a set of threats $T = t_1, t_2, ..., t_n$ and vulnerabilities $V = v_1, v_2, ..., v_m$ [26]. In convergent systems, we distinguish three specific vectors:

Table 1 . **Comparative Table of Threats by OSI Model Layers (V2G Context)**

OSI Layer	Protocol/Technology	Threat Type	System Consequences
Physical (L1)	PLC (HomePlug Green PHY)	Jamming, Eavesdropping	Interruption of charging session, signal interception
Data Link (L2)	Ethernet / Wi-Fi	MAC Spoofing, MitM attacks	Unauthorized access to the station network
Network (L3)	IPv6 (for ISO 15118)	IP Spoofing, Routing Attacks	Traffic redirection to rogue servers
Transport (L4)	TCP/TLS	TLS Inspection, Replay Attack	Compromise of encrypted auth keys
Application (L7)	OCPP, HTTP/JSON	SQL Injection, XML External Entity	Database access, free charging

1. "*EV-to-Grid*" Vector — manipulation of the energy consumption profile of thousands of electric vehicles to create resonance in the power grid.

2. "*Billing/Data*" Vector — compromise of personal data and payment transactions.

3. "*Availability*" Vector — DoS-type attacks on charging station controllers that block vehicle mobility.

Mathematical Model for Quantitative Risk Assessment. Risk R is defined as a function of the probability of successful threat realization and the magnitude of potential losses. Taking into account the specifics of interconnected systems, the following model is proposed:

$$R_{total} = \sum_{i=1}^{n} P(T_i) \times L(C_i) \times K_{casc}, \quad (1)$$

where: $P(T_i)$ — the probability of a successful attack on the *i*-th component (depends on the security level); $L(C_i)$ — direct losses (equipment cost, lost profit); K_{casc} — cascading impact coefficient (*Kcasc* ≥ 1), which accounts for the spread of the incident to an adjacent system (e.g., a charging station failure halting a logistics chain).

The cascading impact coefficient K_{casc} is defined as the ratio of the total losses of the integrated system to the direct losses of the primary target of the attack:

$$K_{casc} = 1 + \frac{L_{adjacent}}{L_{direct}}, \quad (2)$$

where L_{direct} represents the direct losses of the charging point operator (equipment cost, billing disruption), and $L_{adjacent}$ represents the cascading losses of the adjacent sector (the cost of electricity under-supplied to the grid, industrial downtime due to automatic frequency load shedding activation). For the calculation scenario for the city of Kharkiv presented in subsection 2.5, the direct losses of the CPO from blocking the stations are estimated at 1.2 million UAH (L_{direct}), while the cascading economic damage from the disconnection of residential and industrial areas resulting from a 50 MW deficit amounted to 4.8 million UAH ($L_{adjacent}$). Thus, for the convergent system of Kharkiv, the cascading impact coefficient is:

$$K_{casc} = 1 + \frac{4.8}{1.2} = 5.0, \quad (3)$$

which demonstrates a five-fold scaling of the cyberattack consequences during its transition from the transport to the energy level of the infrastructure.

The probability $P(T_i)$ is calculated based on expert assessments or using the Bayesian Belief Network method, where the nodes represent the security status of individual subsystems (onboard computer, cloud server, substation controller).

Algorithm for Identifying Critical Nodes. To minimize defense costs, it is necessary to determine the most vulnerable points through the application of graph theory, where nodes represent infrastructure objects, including the EV, EVSE, and Smart Meter, while edges represent the corresponding information and energy links. Within this framework, a node's risk is assessed through its centrality measure. Consequently, the node with the highest centrality, such as the central management server (CSMS), has the highest protection priority because its compromise maximizes the total risk R_{total}.

Methodology for Assessing Losses from Cascading Incidents. Losses in transport-energy systems are categorized into technical losses, such as battery degradation due to improper charging cycles and damage to power transformers, economic losses, including fines for non-compliance with the load schedule and costs of software recovery, and social losses, which manifest as delays in the operation of emergency services or public transport. To estimate $L(C_i)$, the report suggests using a risk matrix (5×5) adapted to the requirements of the ISO 31000 standard.

Hypothetical Scenario and Calculation Example of Cascading Risk. ***Scenario:*** A targeted attack on the cloud server of a Charging Point Operator (CPO) in Kharkiv. The goal of the attack is the simultaneous deactivation (or conversely, launching at maximum power) of 1,000 fast charging stations (EVSE) with a capacity of 50 kW each.

Input data:

• Total manipulative power (W = 1000 × 50 кВт = 50 МВт).

• Attack time (Peak hour (evening maximum) when the power system operates at the limit of reserves).

• Consequence (An instantaneous power deficit leads to the triggering of automatic frequency load shedding (AFLS) systems and the disconnection of residential areas).

Calculation of the probability of grid recovery within 1 hour (Prec):

We apply the exponential recovery model.

$$\Pr ec(t) = 1 - e^{-mt}, \tag{4}$$

where: m — recovery intensity (depends on the speed of cyber-incident localization and the availability of backup generation). For the Kharkiv power system under martial law, we assumed = 0.65 h^{-1}. t = 1 h.

Result: $Prec(1) = 1 - e^{-0.65\times1} = 1 - 0.522 = 0.478$ (or 47.8%).

Conclusion: The probability of full recovery in 1 hour is low (less than 50%), indicating a high level of risk R and the need for automated protection systems (IDS) capable of blocking an attacker's commands at the substation level in < 1 sec.

Attack Tree for the OCPP Protocol. To visualize the system compromise paths, we construct an attack tree where the root is "Full Takeover of Charging Network Management."

Assessing the Probability of Threat Realization Based on the System's Cybersecurity Maturity Level. To ensure high accuracy of the math-

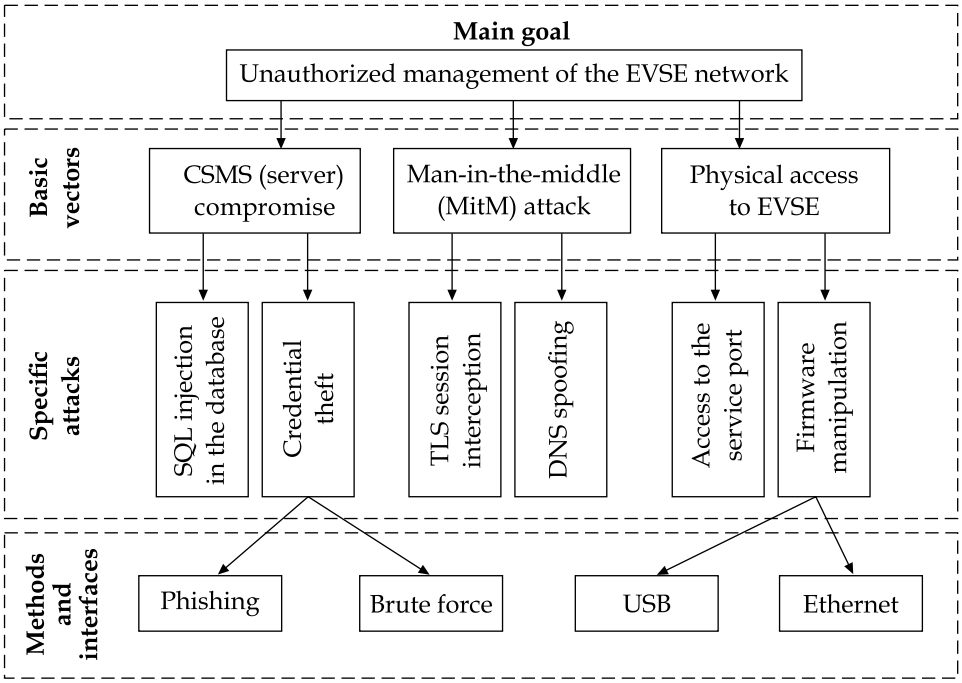


Fig. 1. Attack tree for the OCPP protocol aimed at unauthorized management of the charging station network (EVSE)

ematical risk model, it is necessary to determine the numerical values of the probability of successful threat realization $P(T)$. This indicator directly depends on the technical and organizational state of security of a specific object of transport-energy infrastructure.

Based on an adaptation of the Cybersecurity Capability Maturity Model, a probability scale has been developed that takes into account the

Table 2. **Parameters for the probability of a successful attack by maturity levels**

Maturity Level	Description of Cybersecurity Status	Estimated Annual Probability P(T)	Security Score (Resilience Coefficient)
L1: Initial	Chaotic measures, lack of policies, default passwords.	0.85-0.95	0.1
L2: Managed	Presence of antivirus, basic event logging, software updates.	0.50-0.65	0.4
L3: Defined	ISO 27001 implemented, network segmentation, regular pentests.	0.20-0.35	0.7
L4: Quantitatively Managed	Use of SIEM/SOC, real-time anomaly monitoring.	0.05-0.15	0.9
L5: Optimized	AI-based adaptive systems, full response automation.	<0.02	0.98

current level of implementation of protective measures. The parameters used in the calculation model are presented in Table 2.

The analysis of the data in Table 2 indicates a non-linear relationship between the level of investment in security and risk reduction. The most critical jump in resilience is observed during the transition from the initial (L1) to the defined (L3) level. This is explained by the implementation of basic standards (e.g., ISO/IEC 27001) and network segmentation, which blocks the most common attack vectors (brute force, simple SQL injections).

For critical infrastructure objects, such as the interconnected networks or city energy nodes, the target indicator is the quantitatively managed level (L4). At this level, the probability of a successful attack decreases to the 0.05–0.15 range due to the use of SIEM-class systems and rapid response to anomalies (SOC). Achieving the optimized level (L5) requires significant capital expenditures but provides almost complete automation of protection against "zero-day" attacks, minimizing the impact of the human factor on the security of transport-energy nodes.

Development of Methods and Measures for Cyber Risk Minimization in Convergent Systems

Technical Defense Strategies at the Protocol and Infrastructure Levels. To minimize risks associated with vulnerabilities in the OCPP and ISO 15118 protocols, the implementation of a comprehensive "Security-by-Design" defense system is proposed. Protection against CSMS (Server-side) compromise incorporates adaptive authentication, which involves the implementation of multi-factor authentication (MFA) for administrators and the use of short-lived access tokens (JWT) for inter-service interaction. Concurrently, it requires the deployment of a Web Application Firewall (WAF) to establish filtering screens in front of the management server to automatically block SQL injections and Cross-Site Scripting (XSS) attacks [27]. Furthermore, the cryptographic protection of communication channels is achieved through a transition to OCPP 2.0.1, as this standard supports the mandatory use of TLS 1.3 . This layer of security is reinforced by the implementation of mTLS (Mutual TLS), a method where not only the station verifies the server, but the server also requires a certificate from each station, thereby completely blocking the possibility of DNS spoofing or the creation of fake charging points (Rogue EVSE).

Algorithmic Methods for Preventing Cascading Failures in the Power System. Since the primary risk is load manipulation, it is necessary to implement "intelligent fuses" at the energy market level. This is achieved through decentralized load management, which involves the use of local controllers at substations that can ignore commands from a central cloud server if they contradict the stability parameters of the local network, such as a critical decrease in current frequency. Additionally, anomaly detection algorithms (IDS for OT) utilize machine learning-based systems to analyze historical consumption data, ensuring that if thousands of vehicles

simultaneously receive a "Stop Charge" command without economic or technical prerequisites, the system automatically switches to a secure mode.

Application of the Zero Trust Concept for Ensuring Integrity of Hardware Interfaces and Peripheral Equipment. The Zero Trust concept [28] is traditionally applied to network protocols; however, in the context of interconnected transport and energy systems, it must also be extended to the physical level. Since charging stations (EVSE) are located in public places without constant supervision, any physical port or device chassis should be considered potentially compromised.

The implementation of a Zero Trust strategy at the hardware level assumes that the system does not trust any connection (even service ones) until multi-level verification is performed. Key risk minimization measures at the physical level based on this approach are presented in Table 3.

Organizational Measures and Regulatory Compliance. Risk minimization is impossible without an organizational component that complies with European standards. This includes Cyber Resilience Act (CRA) compliance [29], which requires regular updates of the devices' "digital passport" and systematic reporting on identified vulnerabilities. Concurrently, it demands structured personnel training, which involves conducting targeted cyber-drills for power grid operators simulating the full or partial failure of transport infrastructure.

Feasibility Study and Prioritization of Cybersecurity Measures Based on Cost-Effectiveness Analysis. For the rational allocation of cybersecurity budgets under limited resources at energy and transport enterprises, a comprehensive assessment of the main risk minimization methods was conducted. Cost optimization is based on the principle of achieving the maximum security level (Security Score) with the minimum necessary capital investment (CAPEX) and operating expenses (OPEX) [30].

The results of the comparative analysis of technical protection tools tested within the study are presented in Table 4.

The analytical interpretation of the results allows for the formulation of a prioritization strategy. Specifically, the "quick wins" strategy is based on the fact that implementing multi-factor authentication and Secure Boot

Table 3. **Physical layer risk minimization measures and EVSE equipment integrity control**

Protection Object	Risk Minimization Measure	Effect
USB/Ethernet Port	Software disabling of ports after commissioning	Blocking local loading of malicious software
Firmware	Integrity control using Secure Boot	Prevention of modified software with backdoors
EVSE Chassis	Tamper switches	Instant disconnection of encryption keys upon chassis breach

mechanisms demonstrates the highest return on security investment. Due to their relatively low cost, these measures can neutralize up to 60% of common threats arising from the human factor or direct local interference with hardware.

At the same time, the deployment of high-cost systems, such as SIEM or specialized IDS for operational technologies, requires significant financial resources and expert support. However, for critical infrastructure objects, such as the Kharkiv energy networks, these costs are fully justified. This is due to the ability of these systems to identify complex cascading attacks at early stages, allowing for timely damage localization and prevention of systemic collapse.

Special attention should be paid to the balance between security level and operational complexity. The use of mTLS mutual authentication received a high efficiency rating, but its implementation is accompanied by significant difficulties in managing Public Key Infrastructure. In the development of logistics chains, this implies the need to create internal certification centers, which must be reflected in the project's investment plan in advance.

Based on the comparison, a phased implementation model is recommended for enterprises with limited funding. The priority task is to ensure mandatory two-factor authentication and firmware integrity control for controllers. The next stage should be the deployment of cryptographic protection for communication channels, and only after achieving base resilience is it advisable to transition to the final stage — integration into centralized real-time anomaly monitoring systems.

The quantitative assessment of the proposed defense framework's effectiveness was calculated based on the change in the resulting probability of system compromise. An enterprise with a maturity level of L2

Table 4. **Comparative analysis of technical protection tools by efficiency and economic feasibility criteria**

Protection Method	Efficiency (0-10)	Implementation Cost	Primary Target Threat	Maintenance Complexity
mTLS (Mutual TLS)	9	Medium	MitM, Rogue EVSE	High (PKI management)
SIEM System	10	High	Anomalies, APT attacks	High (requires analysts)
WAF / API Gateway	8	Medium	SQL injections, DDoS	Medium
Secure Boot	9	Low*	Firmware manipulation	Low (at production stage)
MFA (2FA)	7	Low	Phishing, Brute-force	Low
IDS for OT networks	9	High	Cascading Grid failures	Medium

**Note: The low cost of Secure Boot is relevant when purchasing new equipment; upgrading old equipment may be impossible.*

(Managed) was taken as the baseline, where the initial probability of a successful attack $P(T)_{L2}$ averages 0.57 (according to Table 2). After the sequential implementation of the first and second-phase technical measures (Table 3), namely mTLS, Secure Boot, and MFA, the system architecture transitions to the *L*4 (Quantitatively Managed) state. Concurrently, the integral probability of an attacker successfully breaching the perimeter decreases to the value of $P(T)_{L4} = 0.10$. The calculation of the relative risk reduction is expressed as:

$$\Delta \mathrm{P} = \frac{P(T)_{L2} - P(T)_{L4}}{P(T)_{L2}}, \tag{5}$$

where: $\Delta \mathrm{P}$ — is the coefficient of relative reduction in the probability of successful cyber threat realization; $P(T)_{L2}$ — is the integral probability of a successful attack on the system for the second level of cybersecurity maturity (Managed); $P(T)_{L4}$ — is the integral probability of a successful attack on the system after implementing the proposed set of measures and transitioning to the fourth level of maturity (Quantitatively Managed).

If we substitute the numerical values of the probabilities for the corresponding maturity levels *L*2 (Managed) and *L*4 (Quantitatively Managed) from Table 2 presented in the article, the calculation takes the following form:

$$\Delta \mathrm{P} = \frac{0.57 - 0.10}{0.57} \approx 0.8246 (\text{or } 82.46\%). \tag{6}$$

This mathematically proves the conclusion regarding the reduction of threat realization probability by more than 80%, provided there is a transition to a higher level of organizational and technical maturity.

Response Algorithm for a Detected Cyberattack in a V2G Network. In the event of an anomaly identified by the monitoring system (IDS), the action algorithm must be automated to prevent damage to power equipment and destabilization of the energy system. The proposed sequence of actions, presented in Figure 3, is based on the principle of minimizing the system's response time to a detected threat. The process begins with the anomaly detection stage, which may be expressed in atypical consumption spikes or massive simultaneous load shedding by thousands of nodes.

After identifying suspicious activity, the system performs an intelligent analysis to verify the nature of the event. If the parameter deviation does not match a cyberattack pattern, the algorithm directs efforts to check for technical network faults, such as power line accidents or power transformer failures. However, if targeted interference is confirmed, the isolation protocol is launched immediately.

In the first stage of incident localization, an automatic switch of the involved charging stations (EVSE) to autonomous mode is performed. This breaks the logical connection with the compromised management

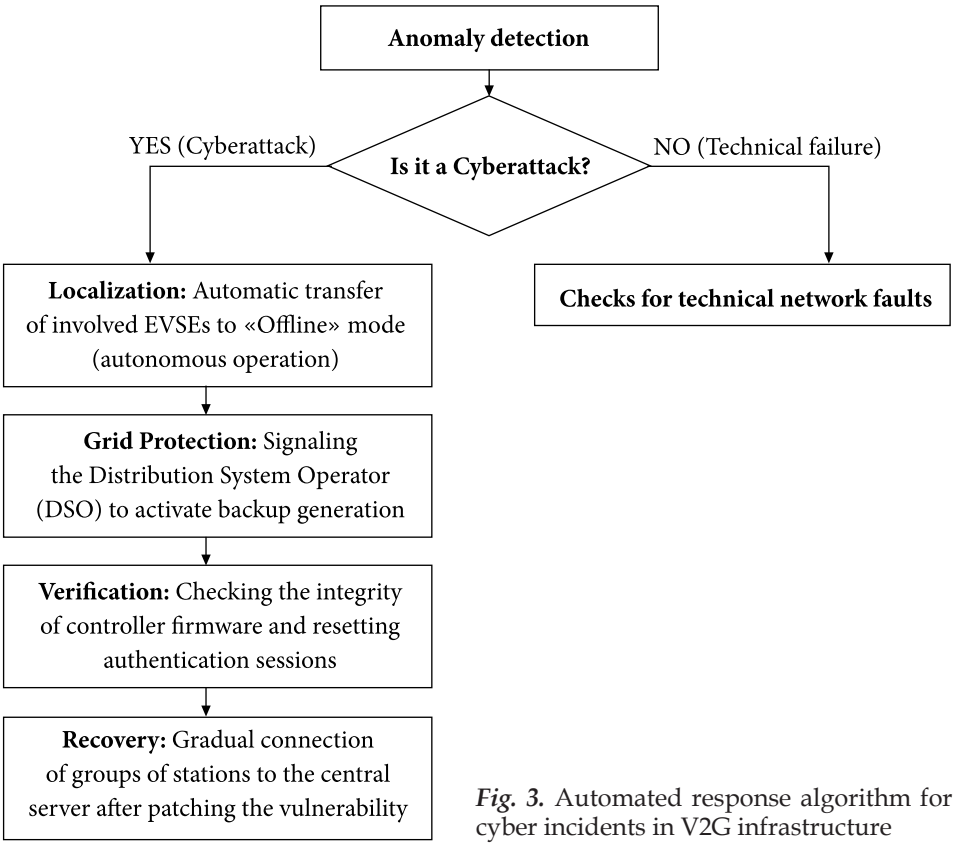


Fig. 3. Automated response algorithm for cyber incidents in V2G infrastructure

server and prevents the further spread of malicious commands. Simultaneously, the second step is taken to protect the power grid as a whole. It involves transmitting an emergency signal to the distribution system operator to activate backup generation or redistribute power flows.

The next verification phase consists of a deep check of controller firmware integrity and a forced reset of all active authentication sessions. This is necessary to completely eliminate the attacker's presence within the system perimeter. The final recovery stage involves a gradual, phased reconnection of station groups to the central system only after successful patching of identified vulnerabilities. This approach ensures that recovery occurs in a secure environment, excluding the possibility of a repeated successful attack using the same vector.

To verify the effectiveness of the proposed automated response algorithm, a simulation was conducted using the specialized MATLAB/Simulink software environment in conjunction with the CORE network traffic emulator. The mass attack scenario described in subsection 2.5 was modeled. The simulation results demonstrated that the deployment of an IDS for OT networks combined with the dynamic load limiting algorithm allows for a reduction in the peak power deficit in the grid during an attack from 50 MW to 8 MW, achieved by isolating the compromised nodes

within 0.8 seconds. A comparative analysis against the baseline NIST SP 800-82 security frameworks showed a 17.4% increase in sensitivity for detecting non-standard deviations, which ensures that the power grid frequency is maintained within acceptable technological limits.

Specifics of Protecting Ukrainian Logistics Chains Under EW Conditions. For Ukraine, and specifically for the Kharkiv region, the resilience of transport-energy systems to Electronic Warfare (EW) and associated cyber threats is of particular importance. The main challenges include GNSS spoofing, where EW tools can distort the coordinates of autonomous electric vehicles or logistics trucks, leading to errors in calculating routes and arrival times at charging hubs and ultimately destabilizing the grid load schedule. Another critical threat is communication channel jamming, where blocking 4G/5G or Wi-Fi communication between the EV and the charging station makes the online authentication and billing process impossible. To counter these vulnerabilities, the proposed protection methods include a "Local Autonomy" mode, which involves the implementation of algorithms that allow charging and identification of critical transport using local white-lists without contacting a cloud server during jamming. This is supplemented by the use of wired channels through a transition to PLC (Power Line Communication) directly via the charging cable, which is completely protected from external electronic interference. Finally, the integration of inertial navigation systems allows for supplementing GNSS modules with inertial sensors to effectively verify the real movement of the vehicle.

Conclusions

1. It has been proven that the convergence of the automotive and energy industries creates critical vulnerabilities, where a cyberattack on the transport infrastructure (EVSE) can trigger a cascading failure in the national power grid.

2. A hierarchical threat model (Attack Tree) for the OCPP protocol has been developed, which allowed for the identification of the most vulnerable nodes, specifically the CSMS management server and the physical interfaces of charging stations.

3. A mathematical model for risk assessment has been proposed, incorporating a cascading impact coefficient, which enables the prioritization of protective measures for critical infrastructure objects.

4. A set of risk minimization methods (mTLS, Secure Boot, IDS) has been substantiated, the implementation of which allows for reducing the probability of successful threat realization by 70–80% in accordance with cybersecurity maturity levels.

5. Specific resilience requirements for the logistics systems of Ukraine under the influence of electronic warfare (EW) have been defined, which is critically important for the functioning of the transport sector during special periods.

REFERENCES

1. 1. On Approval of the List of Critical Infrastructure Objects: Resolution of the Cabinet of Ministers of Ukraine dated 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п [Accessed 12 Sep. 2025]
2. Modern trends in digitization of automotive transport and challenges to information security : training manual / ed. S. V. Kovalenko. — Kyiv : Karavela, 2024. — 240 p.
3. On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine dated 05.10.2017 № 2163-VIII, Revised 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19 [Accessed 05 Sep. 2025]
4. Security Architecture for Electric Vehicle Charging Infrastructure. Idaho National Laboratory. URL: https://inl.gov/ [Accessed 12 Mar. 2026]
5. DSTU ISO/IEC 27001:2023. Information technology. Security methods. Information security management systems. Requirements.
6. DSTU ISO/IEC 27005:2022. Information technology. Security methods. Information security risk management.
7. DORA (Digital Operational Resilience Act) requirements for energy and transport finance sectors. URL: https://www.eiopa.europa.eu/ [Accessed 25 Mar.2026]
8. Kovalenko Yu.V. Mathematical models of viral attack propagation in wireless sensor networks. *Cybernetics and Systems Analysis*, 2024, Issue 4, 110–118.
9. Cyber Resilience Act: Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. — Brussels, 2024. URL: https://digital-strategy.ec.europa.eu [Accessed 15 Oct. 2025]
10. RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3 URL: https://datatracker.ietf.org/doc/html/rfc8446 [Accessed 05 Apr. 2026]
11. DSTU 3008:2015. Information and documentation. Reports in the field of science and technology. Structure and rules of design.
12. Cyber resilience manual for transport system operators. SSSCIP, Kyiv, 2025, 92 p. [Accessed 18 Apr. 2026]
13. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [Accessed 12 Sep. 2025]
14. Al-Sharif A.A. Cyber-Physical Security of Vehicle-to-Grid Systems. Review. IEEE Access, 2023, Vol. 11, 15432–15450.
15. Ivanova T.P. Estimation of cascading effects of cyber incidents in Smart Grid networks. *Energy and Automation*, 2024, Issue 3, 22–30.
16. Petrov V.V. Risk modeling in complex transport and energy systems. Monograph, KNAHU, Kharkiv, 2024, 215 p.
17. Smart Grid Cybersecurity Strategy Ytand Requirements. NIST IR 7628. URL: https://csrc.nist.gov/ [Accessed 15 Feb.2026]
18. Cybersecurity of Electric Vehicle Charging Infrastructure. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu [Accessed 05 Dec. 2025]
19. Korchenko O.H. *Construction of information protection systems*. Cybersecurity. Textbook, Naukova Dumka, Kyiv, 2023, 512 p.
20. ISO 15118-20:2022. Road vehicles. Vehicle to grid communication interface. Part 20: 2nd generation network and application protocol requirements.
21. Open Charge Alliance — Connecting the EV charging industry. URL: https://www.openchargealliance.org [Accessed 28 Oct. 2025]
22. ISO/SAE 21434:2021. Road vehicles. Cybersecurity engineering.
23. NIST SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security. NIST, 2023, 120 p.
24. IEC 62443-4-2:2019. Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.

25. Analysis of hacker groups' activity in the energy sector of Ukraine in 2024-2025. CERT-UA report. URL: https://cert.gov.ua/ [Accessed 10 Jan. 2026]
26. Methodology for cyber risk assessment of energy enterprises. Ed. Kozlov A.M., Lviv Polytechnic, Lviv, 2024, 140 p.
27. Hnatiuk S.O. Modern methods of counteracting MitM attacks in industrial networks. *Information Security*, 2024, Vol. 26 (2) 88–96.
28. Symonenko R.K. Implementation of the Zero Trust concept in OT environments. *Information Processing Systems*, 2025, Issue 1, 60–68.
29. Danylenko V.M. et al. Specifics of protecting intelligent transport systems under martial law. *Bulletin of KNAHU*, 2025, Issue 104, 45–52.
30. Smyrnov O.V. Authentication mechanisms in V2G networks based on Blockchain technology. *Modern information technologies in the field of security and defense*, 2025, Vol. 53 (2), 114–121.

Received 22.04.2026
Accepted 20.07.2026
Published 25.08.2026

ПОХОДЕНКО Б.О., старш. викл. каф.,
Харківський національний автомобільно-дорожній університет,
вул. Ярослава Мудрого, 25, Харків, 61002, Україна
https://orcid.org/0000-0002-9995-7077
boris.pokhodenko@gmail.com

РОЗРОБКА МОДЕЛЕЙ ОЦІНЮВАННЯ ТА МІНІМІЗАЦІЇ РИЗИКІВ КІБЕРІНЦИДЕНТІВ У ВЗАЄМОПОВ'ЯЗАНИХ СИСТЕМАХ АВТОМОБІЛЬНОГО ТРАНСПОРТУ ТА ЕНЕРГЕТИКИ

Вступ. У роботі проведено комплексне дослідження проблеми забезпечення кіберстійкості інтегрованих екосистем автомобільного транспорту та енергетичної інфраструктури, що стають дедалі більш взаємозалежними внаслідок масового впровадження електромобілів та технологій *Smart Grid*. Доведено, що вразливості у протоколах *ISO/IEC* 15118 та *OCPP* можуть бути використані для ініціювання каскадних відмов, які виходять за межі транспортної мережі та критично впливають на стабільність регіональної енергосистеми. Основним внеском даного дослідження є розробка формалізованої математичної моделі багаторівневого оцінювання ризиків, яка використовує ймовірнісний підхід для кількісного визначення впливу кіберфізичних атак на доступність систем та цілісність даних.

Метою статті провести комплексне дослідження проблеми забезпечення кіберстійкості інтегрованих екосистем автомобільного транспорту та енергетичної інфраструктури та розробити надійні стратегії кібербезпеки в умовах тотальної цифровізації транспортних та енергетичних активів.

Методи. У статті представлено детальний аналіз ландшафту загроз із фокусом на специфічні вектори атак, спрямовані на зарядні станції електромобілів (*EVCS*) та протоколи обміну даними інтерфейсу *Vehicle-to-Grid* (*V2G*).

Результати. У роботі детально описано системну структуру мінімізації ризиків, що інтегрує проактивні та реактивні заходи: від впровадження спеціалізованих систем виявлення вторгнень (*IDS*), оптимізованих для промислових протоколів управління, до реалізації адаптивних алгоритмів управління навантаженням, які нівелюють наслідки зловмисного маніпулювання попитом. Результати моделювання, представлені в дослідженні, підтверджують, що запропонована модель ефективно ідентифікує точки конвергенції з високим рівнем ризику, демонструючи покращення чутливості на 15—20 % порівняно з традиційними фреймворками на базі стандартів *NIST*.

Висновки. Отримані результати формують теоретичну та практичну основу для державних структур та операторів критичної інфраструктури щодо розробки надійних стратегій кібербезпеки в умовах тотальної цифровізації транспортних та енергетичних активів. Розроблені моделі сприяють створенню автономних механізмів захисту, здатних підтримувати операційну безперервність у деструктивних умовах. На відміну від існуючих одновимірних моделей, запропонована методологія враховує взаємопов'язаність вузлів, де порушення безпеки в одному транспортному засобі або точці зарядки виступає каталізатором масштабних енергетичних дисбалансів.

Ключові слова: *кібербезпека, автомобільний транспорт, енергетика, оцінювання ризиків, Smart Grid, V2G, мінімізація ризиків, критична інфраструктура, каскадні ефекти, кіберстійкість.*

https://doi.org/10.15407/intchsys.2026.03.102
UDC 004.056.53

A.V. MELNYCHENKO, PhD (Engineering), Assistant Lecturer,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
37, Beresteiskyi ave., Kyiv, 03056, Ukraine
https://orcid.org/0009-0000-3588-4772
artemxl@gmail.com

O.V. SHALDENKO, PhD (Engineering), Associate Professor,
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
37, Beresteiskyi ave., Kyiv, 03056, Ukraine
https://orcid.org/0000-0001-6730-965X
o.shaldenko@gmail.com

TWO-POINT AUTHORIZATION ENGINE WITH REVOCABLE SHARING FOR MULTITENANT ENVIRONMENTS

Multi-tenant software-as-a-service (SaaS) platforms that contain tenant-partitioned data require authorization systems which cover scenarios where classic flat role-based access control (RBAC) fails. Specifically, these systems need to provide access to individual resources rather than whole sets of resources, controlled cross-tenant sharing, and account-less share links which can be revoked at any time. We present access-kit, an in-process authorization engine for the .NET platform built on an explicit model: principals, "area:verb" actions, composable deny-wins policy statements with inheritance, and a resource hierarchy. Enforcement is a co-designed pair of mechanisms which consist of an application-pipeline gate that rejects unauthorized actions outright and an object-relational mapper (ORM) row filter that filters the data to only include rows which are permitted to the current principal. The gate publishes per-request scope which is consumed by row filter, and this scope keeps the two mechanisms in agreement and therefore keeping error reporting consistent. As a result, a write on a readable-but-not-writable resource is refused as a forbidden action rather than disguised as a missing resource, preventing the existence of the resource from being leaked. In the developed framework, each request acts in a single active tenant, so access resolves to one flat statement set. Cross-tenant access is achieved by pulling the grants the active tenant owns, and a caller switches workspace (re-minting its token) to act in another permitted tenant. Account-less sharing is implemented by issuing a revocable, table-backed capability token. We give an

Cite: Melnychenko A.V., Shaldenko O.V. Two Point Authorization Engine with Revocable Sharing for Multitenant Environments. *Information Technologies and Systems*. 3 (9). 2026. 102—102. https://doi.org/10.15407/intechsys.2026.03.102

analytic cost model and an evaluation measured on PostgreSQL: a batch chain-walk resolves effective access in a number of database round trips that is independent of how many grants a principal holds, and we compare it with a naive baseline and a single-query recursive-CTE alternative. The per-request cost is dominated by this resolution, while the in-memory gate adds negligible overhead; the cost model and measurements are given in Section 5. The engine is implemented as a generalized reference implementation with adapters for Entity Framework Core, MediatR, and ASP.NET Core.

Keywords: *access control; authorization; multi-tenancy; resource scoping; cross-tenant sharing; access tokens; row-level security; .NET.*

Introduction

Any system that allows more than one part to act on shared data must have a mechanism to decide who may do what actions on which data — the problem of access control. It is getting increasingly important where data is partitioned among many independent parties — for example, a multi-tenant software-as-a-service (SaaS) platform, which is one of the most common ways of delivering software to customers. SaaS serves many customer organizations (tenants) from one deployment and must isolate each tenant's data from the others [1], yet the same structure arises in any application that confines users to their own slice of a shared store. The dominant authorization model for such systems is role-based access control (RBAC) [2, 3]: a user is assigned a role, and the role carries a fixed set of permissions. RBAC helps to resolve the problem of "what kind of user is this?" by assigning a role to a user, and the role carries a fixed set of permissions. However, RBAC is not sufficient to address the problem of access control in multi-tenant environments.

Collaborative, data-centric platforms such as research data collection, analytics workspaces, document management often have authorization requirements that classic RBAC cannot express. For example:

- Partial, resource-scoped access. "This user may edit given N projects and read everything else inside tenant." In this case, the unit of authorization is an individual resource, not a role.
- Cross-tenant sharing. "Tenant B may manage one project that belongs to tenant A," without users of B becoming members of A or A's isolation weakening for anything else.
- Account-less sharing. "Anyone with given link may view the dashboard". The link should be revocable at any moment, with no account provisioned for the viewer.

These requirements also share a structural subtlety. While executing a single API operation, the code generally performs two actions: it performs an **action** (it reads, updates, or deletes), and it operates over a **set of data rows** (the resources the request reads or targets). Authorizing the request therefore has two distinct facets that must stay consistent: whether the principal may perform the action at all, and which rows the request is permitted to see or modify. In practice these facets are enforced by different mechanisms: a permission check inside the handler and a data-scoping

filter over the query. The issue is that these two mechanisms can drift apart and when they do, the system either leaks data (a row is returned that the action was not authorized to touch) or behaves confusingly (a write reaches a row the read path cannot see and returns a misleading response). Bolting partial, cross-tenant, and account-less access onto role checks produces scattered ad-hoc conditionals that compare the caller's role and are impossible to audit and easy to get subtly wrong - the class of defect catalogued by OWASP as Broken Object Level Authorization [4] and, historically, as the confused deputy [5].

This article presents access-kit, an in-process authorization engine that addresses these requirements. The engine has been extracted and generalized from a production multi-tenant research platform into a reusable. NET library. We describe its model, its co-designed two-point enforcement, its cross-tenant sharing and revocable capability tokens, and we evaluate it analytically and experimentally.

Analysis of Recent Research and Publications

RBAC and ABAC. RBAC [2, 3] groups permissions under roles. It does not natively express per-resource grants or sharing across administrative boundaries. Attribute-based access control (ABAC) [6] decides access from attributes of the subject, object, and environment, and is expressive enough to encode resource scoping in principle, but a general ABAC policy engine passes the row scoping responsibility to the query author and provides no built-in tenant isolation.

Relationship-based access control (ReBAC) and Zanzibar. Google's Zanzibar [7] models authorization as relationship tuples evaluated by a globally distributed service, and OpenFGA [8] is a widely used open-source implementation of the same idea. These systems are powerful and excel at deeply relational permission graphs, but they are out-of-process authorization services. Each decision is an API call, and row scoping is solved by reverse-expansion APIs that the application must wire into its queries separately from its database.

Policy libraries. Casbin [9] and Oso [10] are in-process policy engines (an enforcer over a model/DSL, and the Polar logic language, respectively). They decide whether an action is allowed but, like ABAC engines, leave row scoping and tenant isolation as application responsibilities. Auth0 FGA [11] is a managed Zanzibar-style service. Cloud IAM systems such as AWS IAM [12] combine RBAC and ABAC for control-plane resources but are not designed to be embedded as the data-plane authorization of a third-party SaaS application.

Policy languages: Cedar and OPA. The two closest in-process alternatives are AWS Cedar [13] and the Open Policy Agent (OPA) [14]. Cedar is an embeddable policy language with a formally verified evaluator and analysis tooling. OPA evaluates Rego policies and runs as a sidecar or embedded library. Both are decision engines: given a request and a policy

set they return permit/deny. Like Casbin and Oso they do not scope a database query, and they are typically deployed as a separate policy-decision point, so they carry the out-of-process trust boundary and per-check hop discussed in Section "System and threat model". Cedar's formal verification is an advantage our engine does not claim. The distinction is that access-kit co-designs the decision with an ORM row filter in the same process, trading that isolation for row scoping without an extra hop and automatic data scoping.

Capabilities and revocable tokens. Account-less sharing is a capability-security problem [15] where the link is the authority. Bearer capabilities are convenient but historically hard to revoke. Macaroons [16] add caveats and contextual confinement but remain self-contained bearer tokens that require an external check for revocation. Database row-level security [17] and ORM global query filters [18] provide the row scoping mechanism but not the policy model above them.

Against these systems, access-kit occupies a specific niche. It is in-process and co-designs the decision gate with an ORM row filter, so row scoping is implemented automatically and consistently with the gate rather than left to each query author; tenant isolation is the default; and account-less, instantly revocable cross-tenant sharing is built in. It does not aim to match the relationship-graph expressiveness of Zanzibar/OpenFGA, the formally verified analysis of Cedar, the policy-as-data central audit of OPA, or the hard out-of-process trust boundary those services provide — trade-offs revisited in Section "Discussion".

Problem Statement and Objective

Problem statement. The requirements of Section 1 and the gaps discussed in Section 2 define the problem addressed here: to design an in-process authorization engine for multi-tenant SaaS that makes resource-scoped, cross-tenant, and account-less access first-class, and that is designed to avoid data leaks. In particular, one whose action gate and data-scoping row filter do not disagree about the same request, neither returning a row the action was not authorized to touch nor disguising a forbidden action as a missing resource.

Objective. We design, implement, and evaluate such an engine. Its contributions are:

1. A co-designed enforcement architecture consisting of two mechanisms: an application-pipeline gate and an ORM row filter, which are implemented at three check points (L1/L2/L3) and kept in agreement by a published per-request scope.

2. A single "active tenant" design: every request resolves access for exactly one active tenant, which keeps the gate a plain allow-check, the row filter a single rule, and structure "access denied" and "not found" responses properly.

3. A cross-tenant sharing model of action-matched, server side grants (per-resource and tenant-wide) that take effect only in the owning tenant's

workspace, bounded by issuance rules, plus account-less revocable capability tokens whose validity is a single row lookup.

4. A supporting performance result: effective-access resolution by a batch chain-walk costing O(chain depth) database round trips independent of the number of grants, validated by an exact analytic model and measurement.

The Proposed Authorization Engine

System and threat model. A principal is the identity a request runs as: a user (a real account with a legacy role and a home tenant) or a share capability (no account). Each principal has a home tenant and, at any moment, acts in exactly one **active tenant**. Acting tenant is the home tenant by default, or a foreign tenant it holds a grant on. Every request is resolved for that single active tenant. The rows the principal may reach are the active tenant's rows it is scoped to, and to act in another tenant the principal switches workspace, never seeing two tenants at once.

Decision to make a currently active tenant was made after examining alternatives**.** An alternative design lets one token carry a merged view, which is the union of the principal's home tenant and every tenant it has been granted access to. A user then sees all of them at once. We deliberately reject that design for two reasons. First, user confusion (a design hypothesis we do not test empirically). When rows from several tenants appear together it is ambiguous which tenant a create or edit affects and where a shared item really lives, which invites mistakes on exactly the cross-tenant data that most needs care. Making the active tenant explicit removes that ambiguity, and the user picks one workspace. Second, backend simplification. Resolving for one tenant replaces three sources of complexity with simpler counterparts: the parallel home and granted channels collapse to a single flat statement set; the disjunction over those channels collapses to a single row-filter rule (a row is visible only when it belongs to the active tenant and lies within the principal's scope); and the tenant-aware gate becomes a plain allow-check, with the deny-vs-hide outcome following structurally. Fewer moving parts that must agree mean a smaller surface for the leak-prone bugs this engine exists to prevent.

We assume the application authenticates the principal (e.g., via an identity provider) and that the database is trusted. The adversary is a logged-in principal, possibly a guest or a share-link holder, attempting to exceed its authority: to read or write resources outside its scope, to discover whether a resource exists, to keep using a revoked share, or to assert an ownership or active-tenant value the backend would trust. Accordingly, two values are never taken from the caller: the resource's owning tenant and the active tenant. Both are derived server-side.

Because access-kit is an in-process engine, its trusted computing base is the entire application process: the gate and the row filter are advisory to

code that chooses to call them. The L3 row filter in particular is an ORM convenience and can be bypassed: by *IgnoreQueryFilters*, by raw SQL or a micro-ORM, by a second or misconfigured *DbContext*, or by a projection that reads columns off a type that does not carry a resource marker. This is the defining trade-off against out-of-process policy-decision points such as Zanzibar [7], OPA, or Cedar, which isolate the decision in a separate service or sandbox, gaining a hard trust boundary at the cost of a network or IPC hop on every check. access-kit deliberately takes the in-process side of that trade-off. The mitigations are to centralize data access on one configured context, to forbid *IgnoreQueryFilters* outside the authorization store (enforceable by a Roslyn analyzer or an architecture test), and, where a hostile in-process actor must be assumed, to carry the same tenant-scoped predicate at the database with row-level security [17] as defense in depth.

Authorization model. The model vocabulary displayed in Table 1.

An action is an "area:verb" string. Matching supports two wildcards: "*" matches everything and "area:*" matches any verb in an area. A resource selector is either global (every resource, bounded in practice by the tenant row filter) or an explicit set of root-aggregate ids. A statement is an "Allow" or "Deny" of an action over a selector. A policy is a named set of statements with an optional parent policy. A principal's statements along a policy chain are the union over the chain. A grant (*PrincipalPolicy*) binds a principal to a policy, optionally narrowed by a resource constraint, and records the owner tenant (*ResourceTenantId*) of the resources it reaches.

The resource hierarchy is expressed through three marker interfaces the host's entities implement, so the engine never references concrete domain types:

• *IRootResource*: a root aggregate (e.g., a Project) carrying its own *Id* and *TenantId*;

Table 1. **Core concepts**

Concept	Type	Meaning
Action	area:verb string	unit of authorization, e.g., document: update; supports "*" and "area:*"
Statement	*Allow* / *Deny* over a resource selector	a single authorization clause
Resource selector	*global* or an explicit id set	what a statement applies to
Policy	named statement set + optional ParentPolicyId	reusable, inheritable permission set
Grant	principal → policy (+ optional scope-down, owner tenant)	binds a principal to a policy over resources
Share token	revocable row carrying its own statements	account-less capability
Effective access	flattened statements at a point in time	the evaluated decision object; deny wins

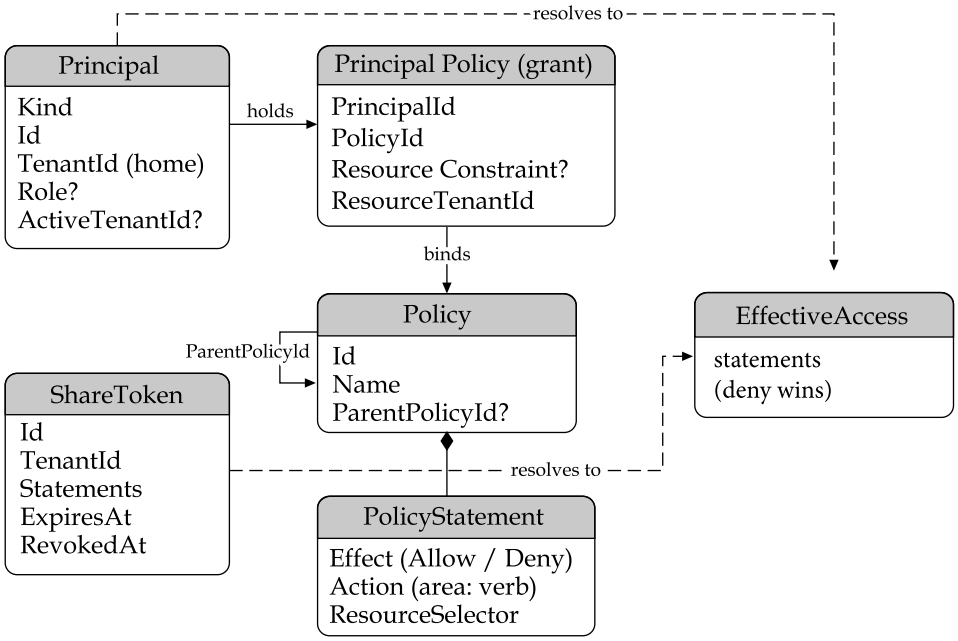


Fig. 1. Authorization data model

- *IChildResource*: homed to a root via *RootId*;
- *ITenantResource*: tenant-owned (carries a *TenantId*).

Effective access is the flattened set of statements for a principal at request time, with deny-wins precedence: an action is allowed if and only if some Allow matches and no Deny matches. An action, optionally on a specific resource, is allowed exactly when some Allow statement matches the action and either applies globally or covers that resource, and no matching Deny statement exists (deny wins). A request that names no resource asserts only the action, leaving the row filter (L3) to narrow the rows.

Figure 1 shows the data model.

A principal resolves to an EffectiveAccess either through its role and grants (walking policy inheritance) or, for a share principal, directly from a token's statements.

Enforcement checkpoints. A single authorized request passes three enforcement check points, realized by two mechanisms: a gate (check points L1 and L2) and a row filter (L3). These two mechanisms are the two points of the title, and the engine's contribution is to keep them in agreement (Fig. 2).

The gate (L1/L2) runs in the application pipeline before any data request is processed; the row filter (L3) runs inside the ORM on every query.

Throughout, we name two outcomes in transport-neutral terms: an access denied response and a not found response. In the HTTP reference adapter these correspond to 403 Forbidden and 404 Not Found, as the figures show.

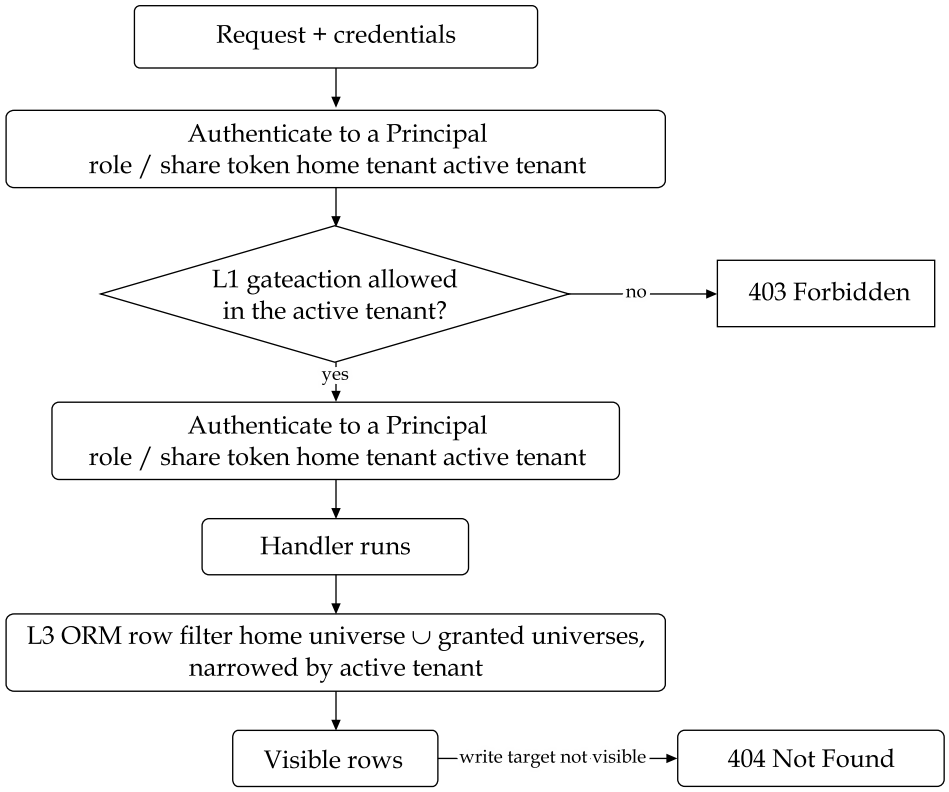


Fig. 2. Request flow

The **gate** lives in the request pipeline (in our case, a MediatR pipeline behavior). It is explicit, cheap, and the natural place to deny an action outright. But it sees only the action and (optionally) a resource id, not the set of rows a query will return. The **row filter** implemented as a global query filter in the ORM [18]. It is implicit so every query against a marked entity is scoped automatically, and a handler cannot accidentally return unscoped data. But it cannot produce an access denied response: an unauthorized row is simply absent.

Using either one alone is unsafe. A gate without a row filter relies on every query author to scope correctly (the BOLA defect [4]). A row filter without a gate cannot distinguish "forbidden" from "does not exist," and cannot deny an action before its side effects. Access-kit uses both, and the gate publishes the per-request scope that the row filter consumes. Both mechanisms then read the same EffectiveAccess, resolved for the active tenant, so the gate consults it to allow the action, and the filter to bound the rows. The actions the gate authorizes and the rows the filter exposes are therefore derived from one structure rather than two independently maintained code paths, the usual source of gate/filter divergence. We argue from this shared construction that the two stay consistent. Verifying that agreement in a given deployment is the integrating host's responsibility.

The row filter is a single rule per resource family, applied over the active tenant's rows, so a row is kept only when it belongs to the active tenant and lies within the principal's scope. The matching predicate covers a root aggregate, a tenant-aware child, a scope-only child, and an off-spine tenant row.

Denying an action versus hiding a resource. Placing an action gate (L1) in front of a row filter (L3) raises one case the filter alone cannot report correctly: a principal that may see a resource but not act on it. A guest with read-only access to a foreign tenant who issues a write must receive an "access denied" response, not a "not found" one. The latter would misreport a forbidden action as a missing resource and leak which ids exist. Because access is resolved for a single active tenant, this falls out structurally. The principal's effective access in that tenant simply contains no matching write statement, so the plain gate denies the action before any row is loaded, while the read still passes. No special tenant-aware check is needed. An access denied response does itself disclose that something exists, so where a resource must be hidden even from principals who lack read access the application returns a uniform not found response (deny read and write alike), which the row filter already produces by making the row invisible.

Multi-tenant isolation and cross-tenant sharing. Every tenant-owned row is filtered to the active tenant, so the isolation is implemented by default. Because a request acts in one tenant, a result set never contains a second tenant's data. Sharing is what lets a principal act in a tenant other than its home: a grant owned by tenant A (its *ResourceTenantId* set server-side from the granting context, never trusted from the caller) gives the grantee statements that take effect only while it is acting in A's workspace. Switching to that workspace re-mints the token with A as the active tenant. The grantee's home role does not follow it across the boundary, so in A it can do exactly what A granted and no more.

Grants come at two grains, **per-resource** (scoped to specific root-aggregate ids) and **tenant-wide** (the whole tenant), and are action-matched: a read-only grant contributes only its read statements, so a document: view grant can never satisfy a document:update request. Resolved for the active tenant, the row filter therefore needs only two inputs (Table 2).

Two issuance safeguards bound sharing. Grantable templates model the common shapes: for example, *ResourceReader/ResourceEditor* (attached

Table 2. **Inputs to the row filter (resolved for the active tenant)**

Input	Source	Meaning
active tenant	activeTenantId (server-derived)	the one tenant every row is filtered to
in-scope roots	ResourceScopeFor(area)	*global*, or the root-aggregate ids the principal is scoped to in that tenant

with a resource constraint, i.e. per-resource) and *TenantGuestReader/TenantGuestManager* (attached without one, i.e. tenant-wide). Guest grant rules bound what a tenant may grant by area, for example, read verbs in any non-protected area, write verbs only in whitelisted areas, and the policy, tenant, admin, and share areas never grantable. Wildcards are never grantable so it caps the blast radius of any share regardless of how the grant is constructed.

Account-less sharing: revocable capability tokens. A *ShareToken* is a database row carrying its own statements, an *ExpiresAt*, and a *RevokedAt*. The share link carries only a compact, URL-safe encoding of the row id (a version byte plus the 16-byte id in base64url, ~23 characters), and therefore no authority of its own. Because the row is the single source of truth for scope, tenant, expiry, and revocation, revoking a share is a single column write. There is no signed bearer token to invalidate and no cache to clear, in contrast to self-contained capabilities such as Macaroons [16]. Validity is decided by reading the row: the share is active when it has not been revoked and has not yet expired, so revocation and expiry take effect on the next request. The version byte lets the link format be changed while old links are rejected cleanly. The web adapter turns a valid link into a Principal (subject share|<id>), so the rest of the request pipeline treats a share like any other principal.

Token entropy and link hygiene. Since the link is the authority until the row is revoked, the row id must be unguessable. Access-kit mints it from a cryptographically secure RNG as a 128-bit value, leaving an attacker no better strategy than brute force over the full 128-bit space. It must not be a sequential or time-ordered identifier (for example a version-7 GUID), which would let one live link expose the range of others, nor *Guid.NewGuid()*, whose output is not contractually a CSPRNG. Because the capability transmitted in a URL, it therefore inherits URL-leakage hazards, such as browser history, the Referer header, server and proxy access logs, and shared-screen exposure. The mitigations are a short expiration timespan, instant revoke, HTTPS-only transport, treating the link as a secret, and optionally exchanging it once for a cookie-bound session so the capability does not linger in the address bar.

Active-tenant token exchange. When a user can act in several tenants, the application exchanges its identity token, once and server-side, for a short-lived application token carrying an *activeTenantId*, re-minted on every workspace switch (in the spirit of OAuth 2.0 [19] and its token-exchange extension [20]). The requested tenant is validated against the caller's home tenant together with the tenants it holds a grant on. A request outside that set is rejected. Because every re-mint re-validates against current grants, a revoked grant stops working within one token lifetime, and the active tenant is never a client-supplied value the backend trusts. Performing this exchange once on the server is the fix for the identity/access *double-exchange* flaw, in which a client is trusted to assert which tenant it is acting in (Fig. 3).

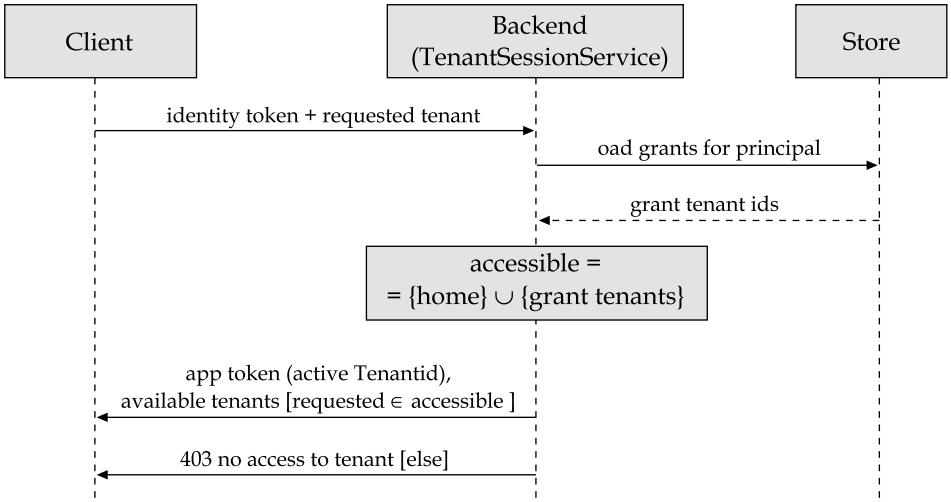


Fig. 3. Active-tenant exchange

To act in another tenant the caller exchanges its token, server-side, for one carrying that activeTenantId; the requested tenant is validated against the caller's own grants and never trusted from the client.

Effective-access resolution. Resolving a user's effective access for the active tenant starts from the role's baked-in statements only when the principal is acting in its home tenant, and adds, for each grant owned by the active tenant, the union of statements along the grant's policy-inheritance chain, intersected with the grant's optional scope-down constraint. The result is one flat statement set for that tenant. A share principal resolves directly from its token's statements.

The naive way to walk policy inheritance is one database query per policy per grant, which results in an N+1 pattern. Access-kit instead resolves inheritance by a batch chain-walk, which collects the frontier of policy ids at each hierarchy level and loads that whole level in one query, deduplicating already-loaded policies (which also guards against cycles). A principal with any number of grants therefore costs O(chain depth) queries (typically one to three), regardless of how many grants share those policies. The store reads current state on every call, so grant and revoke are immediate with no cache to invalidate. A caching decorator can wrap the store if a hot path needs it.

A database that supports recursive common table expressions (WITH RECURSIVE, e.g., PostgreSQL) can resolve the entire policy closure for a principal's grants in a single query: O(1) round trips, one fewer order than the batch walk's O(chain depth). We implement and benchmark this alternative in Section "Experimental results" and it is, as expected, the fastest. The batch walk in this case is not presented as round-trip-optimal, but as a solution which is located above the storage port. In this case, there is no need to use database-specific recursive SQL, runs unchanged on any backing store (relational, document, or in-memory), and keeps policy-

resolution logic in application code rather than pushing it into the database. Its contribution is removing the N+1, turning O(grants × depth) round trips into O(depth), while a recursive CTE trades that portability for one fewer order of round trips. Both sit far below the naive baseline. The choice is portability versus a database-native single round trip.

Results

Analytic cost model. Let G be the number of grants a principal holds, D the depth of the policy-inheritance chain they resolve through, and Q the number of database round trips spent loading policies. The naive resolver issues one policy query per level per grant, so $Q_{naive} = G \times D$ (plus one grants-load). The batch chain-walk loads one query per level and deduplicates shared policies, so $Q_{batch} = D$, independent of G. Table 3 (and the exact counts in Table 4) follow directly.

If a single round trip costs τ (network + execution), end-to-end resolution latency is $\approx Q \times \tau$. The exact counts (Table 4) give this projection directly for $\tau \in \{0.2, 1.0\}$ ms.

Experimental results. We implemented the harness as a BenchmarkDotNet project. The query-count benchmark counts logical round trips through an instrumented store. The timed benchmarks measure in-process cost, and the database-backed benchmarks run against PostgreSQL 16 in a Testcontainers container on the same host. The environment was an Apple M3 Pro, .NET 10.0.3 (Arm64 RyuJIT), under the ShortRun job.

The round-trip counts confirm the analytic model exactly (Table 4): the batch walk's count equals the chain depth and does not grow with the number of grants, while the naive count grows as $G \times D$, so the reduction factor is exactly the grant count G: linear in G, not a fixed multiplier (500× at $G = 500$, and 5000× at $G = 5000$). The point is the shape: naive scales with grants, the batch walk does not.

Because the difference is round trips, wall-clock impact scales with database latency, and on PostgreSQL the projection holds (Fig. 4). Naive resolution rises with the grant count (2.8 ms at 10 grants, 27.7 ms at 100 at depth 1, and 83.7 ms at 100 grants over a depth-3 chain), because every policy load is a separate round trip. The batch walk stays flat in the grant

Table 3. **Resolution cost (database round trips for policy loading)**

Quantity	Naive	Batch
policy round trips	$Q(G \times D)$	$Q(D)$
sensitivity to grants G	Linear	None
sensitivity to depth D	Linear	Linear

Table 4. **Measured (counted) policy round trips**

Grants	Depth	Naive	Batch	Reduction
10	3	30	3	10×
100	3	300	3	100×
500	3	1500	3	500×
500	5	2500	5	500×

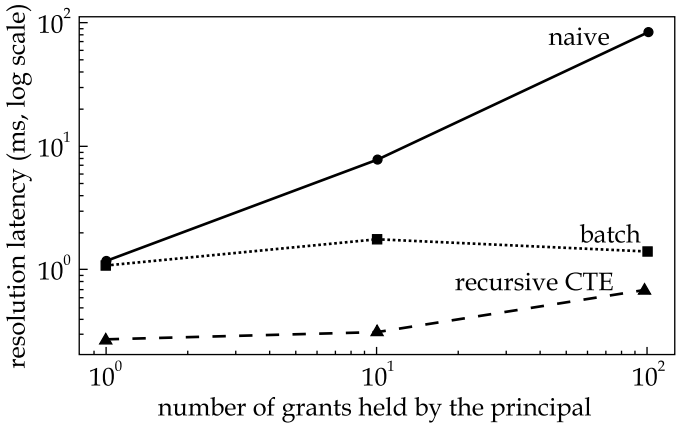


Fig. 4. Measured resolution latency on PostgreSQL (chain depth 3, log–log) naive grows with the grant count, the batch walk is flat in grants, and the recursive CTE is fastest at one round trip

count at 0.6-1.8 ms, and the recursive CTE is fastest at 0.27-0.69 ms in a single round trip. At 100 grants and depth 3 the three approaches differ by orders of magnitude (83.7 vs 1.4 vs 0.69 ms), confirming that the batch walk removes the N+1 and that, where the database offers recursive CTEs, a single database-native query is round-trip-optimal.

Resolution therefore dominates the per-request budget (one to a few round trips, ≈0.3-1.8 ms) and is the natural cache point: the caching decorator over the access store resolver serves effective access from memory, collapsing those round trips to zero on a hit. Every other cost is negligible beside it. Against a zero-latency in-memory store (the worst case for the batch walk) the batch walk is ~1.8× slower than a straight walk at a single grant (941 ns vs 532 ns) but overtakes it by ~10 grants, running ~2-2.4× faster and allocating ~40% as much at 100-500 grants, so removing the N+1 is a net win even on CPU. The in-memory gate runs in tens of nanoseconds to ~1 μs (41 ns at 5 statements, 1.14 μs at 500), and the share-link codec encodes and decodes in ~35 ns. Both are three to five orders of magnitude cheaper than one database round trip.

The L3 row filter's cost is driven by the size of the in-scope id set it must match (the IN/ANY list it emits), not the table's row count. Over a fixed pool of 5000 home rows, reading the visible set takes ≈1.4-1.8 ms for 0-10 ids, 3.0 ms at 100, 3.5 ms at 1000, and 16.2 ms at 10000 ids. Modest sharing (≤1000 shared roots) costs at most ~2× the base scan, while a 10000-id set is expensive and argues for tenant-grain sharing (a single tenant id) over enumerating thousands of roots. A by-row-count sweep on the same PostgreSQL instance confirms the predicate adds no measurable cost beyond the base scan: 2.22 ms filtered vs 2.11 ms unfiltered at 10000 rows. In this case, the id-set size, not the row count, is the cost variable.

Security: leakage scenarios addressed. Table 5 lists the information-leakage scenarios access-kit addresses against a naive role-check baseline. How it differs qualitatively from the other engines is discussed in Section 2.

Discussion: advantages and limitations. Advantages:

(i) In-process: every decision is an in-memory check with no extra network hop, unlike Zanzibar-style services [7].

(ii) Co-designed enforcement: the gate and row filter read one published scope, eliminating the most common object-level authorization defects [4] and reporting access denied versus not found consistently, an agreement we argue from the shared construction rather than prove (see Limitations):

(iii) Instant revocation: both grants and share tokens are read from current state, so revocation needs no propagation window.

(iv) Storage-agnostic: the engine depends on ports, with an Entity Framework Core adapter provided.

(v) Migration-friendly: existing roles become baked-in statements with no data migration.

(vi) Single active tenant: resolving for one tenant keeps the gate a plain allow-check and the row filter a single per-family rule and makes the deny-vs-hide outcome structural, at the cost that acting in another tenant needs an explicit workspace switch.

Limitations: (i) The gate and row filter derive from one shared EffectiveAccess, so they are designed to agree; but because access-kit is an in-process library, upholding that agreement in a given deployment rests with the host that integrates it, and a host can confirm it for its own domain entities with conformance tests on its side. (ii) Access-kit is in-process: its trusted computing base is the whole application process, and the L3 filter can be bypassed by in-process code (IgnoreQueryFilters, raw SQL, a second context), so for a hostile-code threat model it must be paired with database row-level security. (iii) The engine is .NET-specific; cross-language or centrally audited/analyzable deployments are better served by OPA [14], Cedar [13], or OpenFGA [8]. (iv) The row filter captures a per-request scope; with ORM context pooling the compiled model must be keyed per scope to avoid cross-tenant reuse. (v) "Instant" revocation is bounded by token lifetime for active-tenant claims.

Conclusions

We presented access-kit, an embeddable authorization engine for multitenant SaaS that treats partial, cross-tenant, and account-less access as first-class concerns. Its central idea is a co-designed pair of enforcement mechanisms, an application-pipeline gate and an ORM row filter that read one published per-request scope, which makes the two report errors consistently. On top of this, every request acts in a single active tenant, chosen over a merged multi-tenant view to remove user confusion and simplify the backend, so the gate stays a plain allow-check, the row filter a single per-family rule, and the deny-vs-hide outcome structural. Cross-tenant access comes from action-matched, server-derived grants that take effect only in the owning tenant's workspace, alongside account-less, instantly revocable capability tokens. Measured on PostgreSQL, effective-access

resolution by the batch chain-walk costs O(chain depth) database round trips independent of the number of grants, a reduction over the naive N+1 that is linear in the grant count, and we compare it against a single-round-trip recursive CTE. The per-request cost is dominated by this resolution, with the in-memory gate adding nanoseconds.

Future work: a machine-checked formalization of the gate and row-filter agreement invariant; a distributed caching decorator with explicit revocation propagation bounds for very hot paths; packaging and a broader empirical study against production workloads and alternative engines; and extending the resource model beyond a two-level root/child hierarchy.

DECLARATIONS

AI and automated tools usage. AI tools were used to support drafting, language editing and spellcheck. All technical claims, experimental design, measurements, and conclusions were verified by the author, who bear full responsibility for the content; no material was included without author verification.

Conflict of interest. The author(s) declare no conflict of interest.

Grant or financial support. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

1. Chong F., Carraro G., Wolter R. Multi-Tenant Data Architecture. Microsoft *Developer Network*, 2006.
2. Ferraiolo D.F., Sandhu R., Gavrila S., Kuhn D.R., Chandramouli R. Proposed NIST standard for role-based access control. ACM *Transactions on Information and System Security*, 2001, Vol. 4 (3), 224–274. https://doi.org/10.1145/501978.501980
3. Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E. Role-based access control models. *Computer*, 1996, Vol. 29 (2), 38–47. https://doi.org/10.1109/2.485845
4. OWASP Foundation. OWASP API Security Top 10 API1:2023 Broken Object Level Authorization. 2023. URL: https://owasp.org/API-Security/ [Accessed Jun. 2026]
5. Hardy N. The Confused Deputy: or why capabilities might have been invented. ACM SIGOPS *Operating Systems Review*, 1988, Vol. 22 (4), 36–38. https://doi.org/10.1145/54289.871709
6. Hu V.C., Ferraiolo D., Kuhn R., et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. *NIST Special Publication 800-162*, 2014. https://doi.org/10.6028/NIST.SP.800-162
7. Pang R., et al. Zanzibar: Google's Consistent, Global Authorization System. *USENIX Annual Technical Conference (ATC)*, 2019, 33–46.
8. OpenFGA Authors. OpenFGA: a high-performance and flexible authorization/permission engine. Cloud Native Computing Foundation, documentation, 2024. URL: https://openfga.dev [Accessed Jun. 2026]
9. Luo Y., et al. Casbin: an authorization library that supports access control models like ACL, RBAC, ABAC. Documentation, 2024. URL: https://casbin.org [Accessed Jun. 2026]
10. Oso Security. Polar: a declarative logic language for authorization. Documentation, 2024. URL: https://www.osohq.com [Accessed Jun. 2026]
11. Okta.Auth0. Auth0 Fine-Grained Authorization (FGA). Documentation, 2024. URL: https://auth0.com/fine-grained-authorization [Accessed June 2026]
12. Amazon Web Services. AWS Identity and Access Management User Guide policies and ABAC. 2024. URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/ [Accessed Jun. 2026]

13. Cutler J.W., et al. Cedar: a New Language for Expressive, Fast, Safe, and Analyzable Authorization. *ACM on Programming Languages*, 2024, Vol. 8 (OOPSLA1), 670–697. https://doi.org/10.1145/3649835
14. Open Policy Agent Authors. Open Policy Agent (OPA) and the Rego policy language. Cloud Native Computing Foundation, documentation, 2024. URL: https://www.openpolicyagent.org [Accessed Jun. 2026]
15. Dennis J.B., Van Horn E.C. Programming semantics for multiprogrammed computations. *Communications of the ACM*, 1966, Vol. 9 (3), 143–155. https://doi.org/10.1145/365230.365252
16. Birgisson A., Politz J.G., Erlingsson Ú., Taly A., Vrable M., Lentczner M. Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud. *Network and Distributed System Security Symposium (NDSS)*, 2014. https://doi.org/10.14722/ndss.2014.23212
17. PostgreSQL Global Development Group. PostgreSQL Documentation Row Security Policies. 2024. URL: https://www.postgresql.org/docs/current/ddl-rowsecurity.html [Accessed Jun. 2026]
18. Microsoft. Entity Framework Core Global Query Filters. Documentation, 2024. URL: https://learn.microsoft.com/ef/core/querying/filters [Accessed Jun. 2026]
19. Hardt D. (Ed.). RFC 6749: *The OAuth 2.0 Authorization Framework*. IETF, 2012, 75 p. https://doi.org/10.17487/RFC6749
20. Jones M., Nadalin A., Campbell B., Bradley J., Mortimore C. *RFC 8693: OAuth 2.0 Token Exchange*. IETF, 2020. https://doi.org/10.17487/RFC8693
21. Akinshin A. Pro. NET Benchmarking: The Art of Performance Measurement. Apress, Berkeley, CA, 2019.

Received 09.07.2026
Accepted 20.07.2026
Published 25.08.2026

А.В. МЕЛЬНИЧЕНКО, канд. техн. наук, асистент,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
просп. Берестейський 37, Київ, 03056,Україна
https://orcid.org/0009-0000-3588-4772
artemxl@gmail.com
О.В. ШАЛДЕНКО, канд. техн. наук, доцент,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
просп. Берестейський 37, Київ, 03056,Україна
https://orcid.org/0000-0001-6730-965X
o.shaldenko@gmail.com

ДВОТОЧКОВИЙ МЕХАНІЗМ АВТОРИЗАЦІЇ З ВІДКЛИЧНИМ СПІЛЬНИМ ДОСТУПОМ ДЛЯ СЕРЕДОВИЩ З РОЗДІЛЕННЯМ ДАНИХ ПО ОРГАНІЗАЦІЯМ

Вступ. Хмарні платформи з розділенням організацій *(multi-tenant*), що розповсюджуються за моделлю «програмне забезпечення як послуга» (*SaaS*) і зберігають спільні дані окремих організацій, дедалі частіше потребують керування доступом, яке не може забезпечити рольова модель (*RBAC*): доступу до окремих ресурсів, а не ролей; контрольованого спільного доступу в декількох організацій; а також посилань для спільного доступу, які можна відкликати в будь-який момент. Сервер під час обробки запиту водночас виконує дію та оперує набором даних, тож авторизація має два аспекти, які мусять залишатися узгодженими: чи дозволена дія в цілому та які записи запит має право бачити або змінювати. Коли ці механізми неузгоджені, система або розкриває дані,

або повертає оманливі відповіді, що належить до класу вад «порушення авторизації на рівні об'єкта».

Мета роботи. Спроєктувати, реалізувати та оцінити вбудований механізм авторизації для *SaaS*-застосунків для реалізації часткового доступу (на рівні окремого ресурсу) всередині організації, надання спільного доступу між організаціями і спільного доступу за посиланням. Застосування механізму має не допустити непомітного витоку даних, зокрема, щоб фільтри при авторизації дії та фільтри записів з бази даних не суперечили одне одному щодо одного й того самого запиту.

Методи. Запропоновано компактну явну модель (суб'єкти, дії у форматі «область:операція», твердження політик із пріоритетом заборони та успадкуванням, ієрархія ресурсів) і узгоджений механізм застосування: шлюз на рівні обробки вхідного запиту в застосунку, який відповідає за перевірку дозволу на дію, та фільтр рядків на рівні *ORM*, який відповідає за фільтрацію даних, які дозволені для поточного суб'єкта. Їхню узгодженість забезпечує контекст області видимості запиту, який забезпечує шлюз і постачається у фільтр записів, тож обидва механізми узгоджені. Кожен запит діє в межах однієї активної організації: доступ обчислюється саме для активної організації, тож на рівні шлюзу здійснюється проста перевірка дозволу, а на рівні *ORM* застосовується фільтр записів. Ефективний доступ обчислюється пакетним обходом ланцюга політик, що усуває проблему *N*+1 запитів; розглянуто також альтернативу на основі рекурсивного *CTE*. Продуктивність оцінено аналітичною моделлю вартості та вимірюваннями на *PostgreSQL* за допомогою *BenchmarkDotNet*.

Результати. Реалізований механізм дозволяє надавати частковий доступ до ресусів, доступ поза межами організації та спільний доступ за посиланням, при цьому не потребує сторонніх сервісів та працює в рамках самого додатку. Для визначення ефективного доступу використовується пакетний обхід політик доступу з наданими дозволами. Кількість звернень до бази даних при цьому дорівнює глибині ланцюга політик і не залежить від кількості надань суб'єкта; рекурсивний *CTE* розв'язує всю задачу за одне звернення. Під час проведення експериментів з використанням СКБД *PostgreSQL* було отримано наступні показники: за умови 100 наданих дозволів і глибини ланцюга що дорівнює 3, класичний підхід без пакетної обробки потребує близько 83,7 мс, пакетний обхід — близько 1,4 мс, а *CTE* — 0,69 мс. Операції на рівні шлюзу виконуються за десятки наносекунд, тобто на 3—5 порядків швидше за одне звернення до бази; вартість фільтра рядків визначається радше розміром множини наданих ідентифікаторів ресурсів, ніж кількістю рядків таблиці. Спільний доступ між організаціями виражено через дозволи (*grants*), узгоджені за дією, з визначенням власника на боці сервера, що діють лише у робочому просторі організації-власника, а безобліковий доступ — через токени з можливістю відкликання, чинність яких визначається одним зчитуванням запису з бази даних. Узгоджене повідомлення про помилки відрізняє результати «заборонено» від «не знайдено», не розкриваючи існування ресурсу.

Висновки. *access-kit* поєднує механізм ухвалення рішення про надання доступу та фільтр рядків *ORM*, які зчитують один контекст області видимості, з міжорганізаційним і безобліковим спільним доступом. Кожен запит діє в межах однієї активної організації, таким чином зменшується імовірність здійснити дію в сторонній організації, і суттєво спрощується імплементацію, а для дій в іншій організації, користувач перемикає робочий простір. Механізм імплементовано як узагальнену еталонну реалізацію з адаптерами для *Entity Framework Core*, *MediatR* та *ASP.NET Core*.

Ключові слова: *керування доступом; авторизація; обмеження за ресурсами; спільний доступ; токени доступу; захист на рівні рядків; .NET.*

AUTHOR GUIDELINES

The journal publishes the results of research in the field of computer science, information technologies and systems and their applications in various fields of activity, system analysis, intelligent control, cyber security, biological and medical cybernetics, digital economy and learning in the digital age, etc.

Target audience — scientists, engineers, graduate students and students of higher educational institutions of the relevant specialty.

Requirements for manuscripts

1. The manuscript is accepted in electronic form, if possible — on paper in one copy (language of the article — English (*in priority*) or Ukrainian, manuscript up to 30 pages). The manuscript should contain:

• information about the Authors in English and Ukrainian: Full name, Academic Degree, Academic Title, Position, Affiliations, Postal address of the organization, Direct links to author's ORCID (if necessary, Researcher ID) and E-mail, Author-correspondent and their telephone number (*for contacting the editor*);

• Short Abstract with keywords in paper language, and Extended Abstract with keywords in either Ukrainian for English-language paper or English for Ukrainian-language paper. The text of the Extended Abstract is not less than 1800 characters with spaces, by headings: *Introduction*, *The purpose of the paper*, *Methods, Results, Conclusions, Keywords* (5–8 words);

• *DECLARATIONS*: in this section the authors declare 1) *Author contributions* in accordance with CRediT Roles or another standard; 2) *AI and tools usage* in accordance with the journal policy; 3) *Conflict of interest:* existing and type of conflict or no should be disclosed; 4) *Grant or Financial Support* for the research provide information about if it necessary; 5) *Thanks, etc.*

• *REFERENCES* — a list of sources in English in the order of mention in the text. For Non-English-language sources, citation are translated, the original language is indicated in square brackets, for Ukrainian-language papers information about authors and the title in the original language is given. Examples for design of the References is given below;

• *LITERATURE* — a list of sources in Ukrainian do not use for English-language papers;

• if desired, the authors provide information about the grant or financial support of the research;

• the license agreement is signed automatically when the submission is created in the electronic editorial system.

2. The text of the article should be submitted with the following mandatory headings: *Introduction, Problem Statement / Problem Definition, Objective, Results, and clearly formulated Conclusions*.

Requirements for the text file

File format: *.doc, *.rtf. Applicable styles: Times New Roman font, 12 pt, without a hyphen for a line break, line spacing — 1.0. Paper size: A4, all sides — 2 cm.

Formulas are typed in Formula Editors (preferably Microsoft Equation Editor 3.0. and MathType 6.9b.) Formula Editor options are (10.5; 8.5; 7.5; 14; 10). **The width of formulas is up to 12 cm.**

Figures must be of high quality, they are provided in separate files of appropriate formats (*.png, *.jpg, *.tiff, etc.). **The width of the figures is up to 12 cm.**

Tables are created using a standard text editor built into the Table toolkit. **The width of the table is up to 12 cm.**

КЕРІВНИЦТВО ДЛЯ АВТОРІВ

В журналі друкуємо результати досліджень у сфері інформатики, інформаційних технологій та систем і їх застосувань у різних сферах діяльності, системного аналізу, інтелектуального керування, кібербезпеки, біологічної та медичної кібернетики, цифрової економіки та навчання в цифрову епоху тощо.

Цільова аудиторія — науковці, інженери, аспіранти та студенти вищих навчальних закладів відповідного фаху.

Вимоги до рукописів статей

1. Рукопис приймаємо в електронному виді, за можливості — на папері в одному примірнику (мова статті — англійська (*в пріоритеті*) або українська, рукопис до 30 стор.). Рукопис має містити:

• відомості про авторів англійською та українською мовами: ПІБ, науковий ступінь, вчене звання, посаду, місце роботи, поштову адресу організації, прямі посилання авторських ідентифікаторів *ORCID* (за потреби *Researcher ID*) та *E-mail*, автор-кореспондент із номером телефону (*для зв'язку з редактором*);

• коротку анотацію з ключовими словами мовою статті та розширену анотацію з ключовими словами українською для англомовної статті або ж англійською для українськомовної статті. Текст розширеної анотації не менше 1800 знаків з пробілами, за рубриками: *Introduction / Вступ, The purpose of the paper / Мета роботи, Methods/Методи, Results/Результати, Conclusions/Висновки, Keywords/Ключові слова* (5–8 слів);

• ПОВІДОМЛЕННЯ: *у цьому розділі автори заявляють про* 1) Внесок авторів *відповідно до CRediT Roles або іншого стандарту*; 2) Застосування ШІ *та інших інструментів відповідно політики журналу*; 3) Конфлікти інтересів — *тут розкривають їх наявність і вид або відсутність*; 4) Гранти або фінансова підтримка *дослідження — за потреби інформувати*; 5) Подяки, *тощо*.

• *ЛІТЕРАТУРА* — перелік джерел для українськомовних статей українською мовою оригіналу в порядку згадування в тексті, для неукраїнськомовних джерел посилання даються англійською, в квадратних дужках вказується мова оригіналу;

• *REFERENCES* — перелік джерел англійською мовою в порядку згадування в тексті. Для неангломовних джерел в квадратних дужках вказується мова оригіналу, для українськомовних після двокрапки наводиться інформація про авторів та назва джерела мовою оригіналу. Приклади оформлення переліку посилань наведено далі;

• за бажанням автори надають інформацію про грант або фінансову підтримку дослідження;

• ліцензійний договір підписується автоматично при створені подання в системі електронної редакції.

2. Текст статті подають з обов'язковими рубриками: *Вступ, Постановка завдання/Окреслення проблеми, Мета, Результати,* чітко сформульовані *Висновки*.

Вимоги до текстового файлу

Формат файлу *.doc, *.rtf. Застосовні стилі: шрифт Times New Roman, 12 пт, без переносів, міжрядковий інтервал — 1,0. Формат паперу А4, всі береги — 2 см.

Формули набирають у редакторах формул (бажано Microsoft Equation Editor 3.0. та MathType 6.9b.) Опції редактора формул — (10,5; 8,5; 7,5; 14; 10). **Ширина формул — до 12 см**.

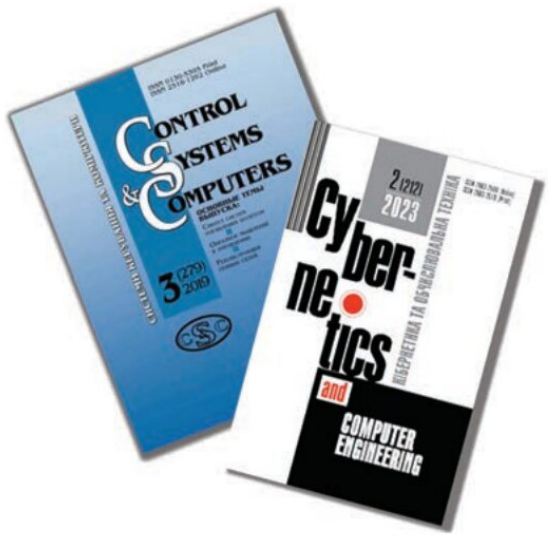
Рисунки мають бути якісними, їх надають окремими файлами відповідних форматів (*.png, *.jpg, *.tiff тощо). **Ширина рисунків — до 12 см**.

Таблиці виконують стандартним вбудованим у інструментарієм «Таблиця» текстового редактора. **Ширина таблиці — до 12 см**.

УДК 004.6/.9+519+62

Journal *"Information Technologies and Systems"* that is a merger of two academic journals with a long history — Control Systems and Computers journal ISSN (Print) 2706-8145, ISSN (Online) 2706-8153 (published since 1972) and Cybernetics and Computer Engineering journal ISSN (Print) — 2663-2578, ISSN (Online) — 2663-2586 (published since 1965). The organization responsible for publishing the journal is Institute of Information Technologies and Systems of National Academy of Sciences of Ukraine.

The journal publishes original scientific and review papers about fundamental and applied research results of informatics and information technologies, intelligent control and systems, methods and means of information technology support of knowledge, application of the mentioned technologies in various fields of life. Number of Issues is 6 per year. Currently, the journal does not charge any fees to the authors from submission to publication. The papers are an Open Access under the CC BY-NC-ND 4.0 license.



Журнал «Інформаційні технології та системи» є результатом об'єднання двох академічних журналів з багаторічною історією — журналу «Системи керування та обчислювальна техніка» ISSN (друковане видання) 2706-8145, ISSN (онлайн) 2706-8153 (видавався з 1972 року) та журналу «Кібернетика та обчислювальна техніка» ISSN (друковане видання) — 2663-2578, ISSN (онлайн) — 2663-2586 (видавався з 1965 року). Організацією, відповідальною за видання журналу, є Інститут інформаційних технологій та систем Національної академії наук України.

Журнал публікує оригінальні наукові та оглядові статті про фундаментальні та прикладні результати досліджень інформатики та інформаційних технологій, інтелектуального керування та систем, методів та засобів інформаційно-технологічної підтримки знань, застосування згаданих технологій у різних сферах життя. Кількість випусків — 6 на рік. Наразі журнал не стягує жодних гонорарів з авторів від моменту подання до публікації. Статті знаходяться у відкритому доступі за ліцензією CC BY-NC-ND 4.0.

ISSN 3083-6573 Information Technologies and Systems 2026, № 3. 1–120