DOI: 10.18372/2225-5036.31.20634

АДАПТИВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ХМАРНО-ОРІЄНТОВАНИХ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМАХ

Світлана Рзаєва[1], Юлія Костюк[1], Павло Складанний[1], Вадим Абрамов[1], Володимир Кравченко[2]

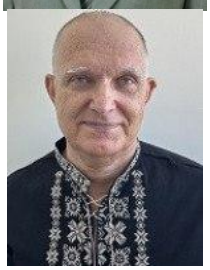
[1]Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
[2]Київський національний економічний університет імені Вадима Гетьмана

РЗАЄВА Світлана Леонідівна, кандидат технічних наук, доцент.
Рік та місце народження: 1968 рік, м. Київ, Україна.
Освіта: Севастопольський приладобудівний інститут.
Посада: доцент кафедри комп'ютерних наук.
Наукові інтереси: адміністрування і захист баз даних та сховищ даних, моделювання програмного забезпечення та його аналіз, інформаційні технології та системи.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: s.rzaieva@kubg.edu.ua
Orcid: 0000-0002-7589-2045

СКЛАДАННИЙ Павло Миколайович, кандидат технічних наук, доцент.
Рік та місце народження: 1992 рік, м. Київ, Україна.
Освіта: Державний університет телекомунікацій.
Посада: завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.
Наукові інтереси: кібербезпека, криптографія, криптоаналіз, математичне моделювання.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: p.skladannyi@kubg.edu.ua
Orcid: 0000-0002-7775-6039

КОСТЮК Юлія Володимирівна, Phd in Computer Science.
Рік та місце народження: 1980 рік, м. Київ, Україна.
Освіта: Державний торговельно-економічний університет.
Посада: доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.
Наукові інтереси: захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи, нейронні мережі.
Публікації: більше 30 наукових публікацій, серед яких монографії, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: y.kostiuk@kubg.edu.ua
Orcid: 0000-0001-5423-0985

АБРАМОВ Вадим Олексійович, кандидат технічних наук, доцент.
Рік та місце народження: 1952 рік, м. Київ, Україна.
Освіта: Київський політехнічний інститут.
Посада: доцент кафедри комп'ютерних наук.
Наукові інтереси: бази даних, захист інформації, комп'ютерні мережі, інформаційно-комунікаційні системи, інформаційно-інтелектуальні системи.
Публікації: більше 20 наукових публікацій, серед яких монографії, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: v.abramov@kubg.edu.ua
Orcid: 0000-0002-8026-1475



КРАВЧЕНКО Володимир Георгійович, кандидат економічних наук, доцент.
Рік та місце народження: 1952 рік, м. Київ, Україна.
Освіта: Київський інститут народного господарства імені Д.С.Коротченка
Посада: доцент кафедри інформатики та системології.
Наукові інтереси: бізнес-інформатика, Business Intelligence, Data Science, прикладне програмування, системи штучного інтелекту.
Публікації: більше 20 наукових публікацій, серед яких монографії, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: kvg1953@kneu.edu.ua
Orcid: 0000-0003-0113-7933:

Анотація. *У статті здійснено дослідження теоретичних та прикладних аспектів адаптивного управління інформаційною безпекою в хмарно-орієнтованих інтелектуальних транспортних системах (ІТС). Проаналізовано архітектурні особливості середовища типу «Cloud–Edge–Vehicle», визначено основні вектори кіберзагроз та обґрунтовано недоліки традиційних підходів до забезпечення безпеки, зокрема статичних політик доступу, централізованих PKI-рішень*

та класичних IDS/IPS у мультидоменних, динамічних транспортних екосистемах. Розроблено математичну та алгоритмічну модель адаптивного управління, яка розглядає ІТС як дискретну динамічну систему, стан якої визначається у часі під впливом зовнішніх загрозових факторів та адаптивних заходів безпеки. Управління формалізовано як задачу мінімізації комбінованого функціоналу ризиків та витрат, що забезпечує баланс між рівнем захищеності та продуктивністю системи. У межах запропонованого підходу інтегровано механізми збору й аналізу телеметричних і мережевих даних, методи оцінювання ризиків, алгоритми оптимізаційного вибору політик безпеки та механізми зворотного зв'язку між архітектурними рівнями в єдину замкнену систему адаптивного управління. Для виявлення аномалій у потокових даних застосовано алгоритми машинного навчання (зокрема LSTM/GRU та автоенкодери), а для забезпечення узгодженості моделей між рівнями архітектури без централізації даних – методи розподіленого навчання (Federated Learning). Розглянуто методи протидії adversarial-атакам як на етапах тренування, так і під час експлуатації ML-компонентів. Отримані результати створюють наукове підґрунтя для побудови масштабованих, стійких до загроз та ресурсно-ефективних механізмів захисту хмарно-орієнтованих ІТС. Запропонована модель може бути використана для підвищення рівня безпеки транспортних мереж, забезпечення когерентності політик між архітектурними рівнями та автоматизації процесів реагування на кіберзагрози в реальному часі.

Ключові слова: *адаптивне управління безпекою, інтелектуальні транспортні системи, хмарно-орієнтована архітектура, оцінювання ризиків, потокові дані, розподілене навчання, adversarial-атаки, машинне навчання, інформаційна безпека.*

Вступ

Інтенсивна цифрова трансформація транспортної галузі супроводжується зростанням обсягів даних, масштабуванням мережевих інфраструктур та впровадженням технологій машинного навчання в критичні контури керування рухом. У таких умовах інтелектуальні транспортні системи (ІТС) стають складними гібридними екосистемами, які інтегрують транспортні засоби, периферійні обчислювальні вузли та хмарні платформи в єдине розподілене середовище. Хмарно-орієнтовані архітектури забезпечують масштабоване зберігання та обробку потокових даних, аналітику в реальному часі та централізоване управління політиками, що є важливими для ефективності та безпеки транспортних мереж.

Разом з тим, така архітектурна відкритість і динамічність породжує новий клас загроз, які охоплюють як традиційні протокол-орієнтовані атаки на TCP/IP-стек (IP spoofing, ARP poisoning, session hijacking тощо), так і складні багатовекторні сценарії, що поєднують компрометацію бортових вузлів, маніпуляції телеметрією та цілеспрямовані атаки на ML-компоненти. Особливої актуальності набувають adversarial-впливи на моделі машинного навчання, які можуть призводити до викривлення аналітичних висновків та прийняття хибних рішень у реальному часі.

Традиційні механізми забезпечення інформаційної безпеки, орієнтовані на статичні політики доступу (RBAC), централізовані PKI та IDS/IPS, виявляються недостатньо ефективними в умовах мультидоменних і динамічних хмарно-орієнтованих середовищ. Вони не враховують зміну топології в реальному часі, не забезпечують низьку латентність реагування та не охоплюють захист ML-компонентів від adversarial-атак.

Адаптивне управління інформаційною безпекою постає як концептуально новий підхід, що базується на безперервному моніторингу стану системи, оцінюванні ризиків у реальному часі та динамічному переналаштуванні політик безпеки залежно від поточного контексту функціонування системи. Його математична та алгоритмічна формалізація забезпечує інтеграцію механізмів детекції інцидентів, оцінки загроз і прийняття рішень у єдиний ітераційний цикл зворотного зв'язку, що дозволяє автоматизувати реагування на події та оптимізувати використання ресурсів між транспортними, периферійними та хмарними рівнями.

Наукова новизна дослідження полягає в розробленні формалізованої архітектурно-функціональної та алгоритмічної моделі адаптивного управління інформаційною безпекою для хмарно-орієнтованих ІТС, яка враховує багаторівневу структуру системи, потокову природу даних, вразливості ML-компонентів і потребу в когерентності політик між усіма рівнями архітектури.

Метою статті є **розроблення математичної та алгоритмічної моделі адаптивного управління інформаційною безпекою** в хмарно-орієнтованих інтелектуальних транспортних системах, яка забезпечує динамічне коригування політик безпеки залежно від поточного стану системи та актуальної ситуації у сфері загроз, підтримує когерентність рішень між архітектурними рівнями та підвищує стійкість до складних кіберзагроз, зокрема adversarial-впливів на ML-компоненти.

Постановка проблеми. У сучасних інтелектуальних транспортних системах спостерігається стійка тенденція до глибшої інтеграції хмарних та периферійних обчислювальних платформ з локальними та бортовими підсистемами автомобілів, дорожньої інфраструктури та центрів управління. Хмарні сервіси забезпечують масштабоване зберігання й аналіз потокових даних, централізовану координацію сервісів прогнозування та планування маршрутів, а також підтримують реалізацію mobility-digital-twin та інших аналітичних функцій, критичних для ефективності міських транспортних мереж. Такий перехід до хмарно-орієнтованих (cloud-and-edge) архітектур підвищує функціональні можливості ІТС, водночас породжуючи нові системні вимоги до безпеки та надійності [2].

Хмарно-орієнтована архітектура ІТС має мультидоменний і багаторівневий характер: у ній

співіснують бортові агенти транспортних засобів, периферійні (edge / MEC) вузли, регіональні оркестратори **транспортних сервісів** (наприклад, центри керування дорожнім рухом, транспортні диспетчерські хаби або локальні control planes мультихмарної інфраструктури) та глобальні хмарні сервіси, які забезпечують централізовану аналітику, маршрутизацію та управління політиками безпеки. Така розподіленість значно збільшує «поверхню» потенційних кіберзагроз: поряд зі звичними протокол-орієнтованими атаками (спуфінг, replay, Sybil) виникають комплексні багатовекторні сценарії, що поєднують компрометацію бортових вузлів, маніпуляції телеметрією, мережеві відмови та атаки на хмарні аналітичні сервіси. Огляди останніх років демонструють, що багато існуючих механізмів захисту V2X/ITS не враховують одночасно цих мультидоменних векторів загроз у контексті хмарних обчислень [1].

Традиційні підходи щодо забезпечення інформаційної безпеки, такі як статичні політики доступу (наприклад RBAC), централізовані PKI-схеми для аутентифікації V2X та класичні IDS/IPS, виявляють суттєві обмеження в умовах динамічної хмарно-орієнтованої екосистеми. По-перше, централізовані механізми часто спричиняють критичні затримки, що робить їх непридатними для транспортних сервісів із жорсткими вимогами до латентності. По-друге, статичні політики доступу не забезпечують оперативного реагування на зміни топології та умов функціонування системи (зокрема, під час переміщення вузлів між зонами хмарного розміщення). По-третє, традиційні рішення, як правило, не враховують специфіку атак на компоненти машинного навчання та оркестратори політик у мультихмарних середовищах. У сукупності ці обмеження зумовлюють потребу у нових підходах, які поєднують адаптивне керування політиками безпеки, розподілені моделі довіри та низьколатентні механізми захисту на мережної периферії [2].

Окремо стоїть проблема своєчасного виявлення аномалій у потокових телеметричних даних та мережевих потоках у розподіленої хмарно-периферійної архітектури. Сучасні методи на базі машинного навчання (LSTM/GRU, автоенкодери, VAE тощо) демонструють високу ефективність у найкращих публікаціях, але їх застосування в реальному часі в мультиагентних ІТС ускладнюється вимогами до узгодженості моделей між локальними вузлами і глобальними сервісами, а також вразливістю моделей до adversarial-атак. Недавні дослідження виявляють потребу в методах, що поєднують stream-адаптацію моделей, розподіленого навчання (наприклад, Federated Learning) та захист від атак на ML-компоненти [4].

Питання довіри та координації між рівнями інтегрованої хмарно-периферійної архітектури також має ключове значення: компрометація окремих елементів або розбіжності у локальних оцінках загроз можуть викликати протилежні рішення, що загрожують цілісності й безпеці транспортних сервісів. Сучасні підходи зосереджуються на інтеграції динамічних моделей довіри, TRiSM-фреймворках (Trust–Risk–Security Management) та механізмах адаптивної оркестрації політик для забезпечення узгодженості й відновлюваності системи в умовах атак або відмов [6]. У даному контексті під оркестрацією розуміється автоматизоване та скоординоване керування взаємодією, розгортанням і роботою різних компонентів системи **(**сервісів, додатків, політик, мережевих елементів тощо**) у** розподіленому або хмарному середовищі**.**

Отже, науково-практична проблема полягає у відсутності комплексної, формалізованої та реалізованої моделі адаптивного управління інформаційною безпекою, інтегрованої в хмарно-орієнтовану архітектуру ІТС, яка одночасно забезпечувала б:

- контекстно-залежну оцінку загроз у реальному часі;
- динамічне переналаштування політик безпеки з урахуванням зміни топології та розміщення навантаження в мультихмарному середовищі;
- когерентність рішень між бортовими; периферійними та хмарними рівнями;
- стійке розпізнавання аномалій у потокових даних;
- захист ML-компонентів від adversarial-маніпуляцій без значного погіршення продуктивності сервісів.

Заповнення цього наукового розриву вимагає міждисциплінарного підходу: поєднання хмарно-орієнтованих архітектур, мультиагентного моделювання, адаптивного менеджменту політик та сучасних методів виявлення загроз на основі ML [2].

Аналіз останніх досліджень і публікацій.

Першочергову роль у формуванні наукового контексту відіграють дослідження, присвячені систематизації ландшафту загроз та механізмів захисту в середовищі V2X та інтелектуальних транспортних систем. Результати останніх років засвідчують, що перехід до розподілених хмарно-периферійних (cloud-edge) архітектур змінив структуру та динаміку кіберзагроз**,** розширивши їхній спектр і складність. Поряд із традиційними атаками на комунікаційні протоколи (spoofing, replay, Sybil, DoS) спостерігається зростання кількості багатовекторних атак**,** спрямованих на компрометацію довірчих відносин між агентами, а також цілеспрямованих маніпуляцій телеметричними даними**,** що використовуються в аналітичних та керуючих підсистемах. Також наявні значні прогалини у практиках захисту, зокрема нестача підходів, що одночасно враховують розподіленість, часові обмеження та мультихмарну оркестрацію [1].

Питання архітектурного інжинірингу для інтеграції хмарних і периферійних обчислень (cloud-edge) у контексті CAV/ITS активно досліджуються як науковцями, так і практиками. У науковій літературі з'явилися ґрунтовні огляди, які систематизують шаблони розгортання сервісів, сценарії offload-у обчислень та архітектурні патерни, спрямовані на зниження латентності. Ці праці демонструють, що хмарно-периферійна оркестрація (автоматичне розміщення завдань між edge і cloud) може підвищувати продуктивність і безпеку, якщо одночасно вводити механізми політик безпеки та контролю довіри на регіональному рівні. Водночас автори застерігають про нові ризики, зокрема про те, що оркестратори самі стають привабливою ціллю для атак [2].

У напрямі виявлення аномалій (anomaly detection) для потокових телеметричних даних та поведінки CAV спостерігається інтенсивний прогрес: систематичні огляди останніх років виділяють LSTM/GRU, автоенкодери, VAE і трансформерні архітектури як основні рішення, при цьому практична реалізація повинна вирішувати проблеми латентності, адаптації до зміни розподілу даних та інтерпретованості результатів. Багато останніх експериментів демонструють високу детекційну здатність ML-методів у статичних бенчмарках, але підкреслюють необхідність інкрементальних online-схем і заходів щодо забезпечення стійкості моделей до adversarial-вливів, тобто стійкості до навмисних, ворожих або шкідливих впливів на систему, які спрямовані на її дезактивацію, обман або порушення нормальної роботи [4].

Окремим і дуже активним напрямом є розподілене навчання для побудови детекторів аномалій без централізації сирих персональних даних. Дослідження останніх років показують, що такі підходи дозволяють зменшувати ризики витоку даних, підвищувати приватність і забезпечувати узгоджене навчання між бортовими системами, edge-обчисленнями та хмарною інфраструктурою. Водночас залишаються відкритими питання агрегації, синхронізації, стійкості до зіпсованих локальних оновлень та масштабованості в мультихмарних середовищах. У контексті V2X застосування розподілених методів для виявлення аномальної поведінки транспортних засобів продовжує залишатися одним із перспективних напрямів досліджень.

Протягом 2023–2025 років у наукових дослідженнях значно зросла увага до adversarial machine learning та методів захисту компонентів машинного навчання у критичних застосуваннях ІТС. Аналіз оглядових і мета-аналітичних публікацій показує, що моделі, які виконують детекцію або прийняття рішень, залишаються вразливими до атак, таких як створення шкідливих прикладів, отруєння даних або маніпуляції функціями ознак, а отже потребує впровадження як превентивних заходів, таких як robust training та сертифікованих методів захисту, так і контролю під час виконання алгоритмів, включно з shielding та моніторингом через системи типу model-watchdogs. У контексті хмарно-периферійної інфраструктури заходи з безпеки ML-компонентів мають впроваджуватися на всіх рівнях системи: локально на пристроях, регіонально на edge-серверах та централізовано у хмарі із забезпеченням узгодженості політик захисту та моніторингу між рівнями.

Дослідження дозволяють виділити кілька ключових висновків щодо адаптивного управління безпекою в хмарно-орієнтованих ІТС. По-перше, необхідно впроваджувати архітектурні патерни, які забезпечують інтеграцію хмарно-периферійної оркестрації з адаптивними політиками безпеки, що дозволяє оперативно реагувати на інциденти і змінювати правила доступу та поведінку компонентів системи у реальному часі. По-друге, для побудови детекторів аномалій необхідно застосовувати розподілені підходи до навчання, які враховують приватність даних, дозволяючи тренувати моделі на локальних даних без їх централізації та зберігаючи конфіденційність інформації про користувачів і транспортні події. По-третє, захист від adversarial-атак повинен бути інтегрований у всі рівні системи та перевірятися в мультиагентних сценаріях, де моделі взаємодіють і приймають узгоджені рішення, що дозволяє виявляти і протидіяти ворожим впливам у реальному часі. Нарешті, для практичної реалізації рішень критично важливими є: забезпечення довіри між компонентами системи, гарантування узгодженості рішень у мультиагентних сценаріях та здатність системи продовжувати безпечну роботу навіть у разі компрометації окремих вузлів або модулів (т. зв. graceful degradation). Ці висновки стали основою для нещодавніх експериментальних досліджень.

Результати дослідження

Хмарно-орієнтована архітектура інтелектуальних транспортних систем (ІТС) має багаторівневу та мультидоменну структуру, що поєднує обчислювальні та комунікаційні ресурси різних типів у єдине кероване середовище. Основними компонентами архітектури виступають: транспортні засоби з вбудованими комунікаційними модулями (CAV – Connected and Autonomous Vehicles), периферійна інфраструктура (Edge / MEC), регіональні рівні управління транспортними сервісами та глобальні хмарні платформи. Така організація дозволяє поєднати низьку латентність обробки на периферії з масштабованістю та аналітичними можливостями хмари. Кожен рівень виконує специфічні функції, спрямовані на забезпечення безпечного та ефективного функціонування транспортної екосистеми. У таблиці 1 подано структурований опис архітектурних рівнів, їхніх ключових компонентів та функціональних призначень.

Таблиця 1

Архітектурні рівні хмарно-орієнтованої ІТС

Архітектурний рівень	***Основні компоненти***	***Ключові функції***
Транспортний рівень	OBU (On-Board Unit), сенсорні системи (LiDAR, камери, радар, GPS), локальні ML-агенти, V2X-модуль, кеш моделей та телеметрії	- Збір та попередня обробка телеметрії. - Обмін даними через V2X-канали. - Локальний інтерфейс для критичних сценаріїв у реальному часі. - Тимчасове збереження даних і моделей для offline-роботи.
Периферійний рівень (Edge / MEC)	RSU/MEC сервери, Edge ML Hub, регіональні брокери повідомлень, локальні оркестратори, кеш даних	- Агрегація даних від кількох транспортних засобів. - Низьколатентна аналітика та попереднє виявлення аномалій. - Offloading обчислень від бортових вузлів. - Синхронізація моделей та політик із регіональними й хмарними рівнями.
Регіональний рівень	Центри керування дорожнім рухом, диспетчерські хаби, регіональні control planes, репозиторії моделей, компоненти довіри та ризик-менеджменту	- Координація транспортних сервісів у межах регіону. - Розподіл задач між периферійними вузлами. - Узгодження політик безпеки та управління подіями. - Збереження агрегованих даних і моделей для регіонального аналізу
Хмарний рівень	Глобальні оркестратори, Policy Manager, ML-сервіси для тренування та валідації моделей, Data Lake / DWH, сервіси OTA-оновлень, аналітичні та форенсик-платформи	- Централізоване управління політиками та оновленнями. - Глобальна аналітика та кореляція інцидентів. - Навчання та перевірка моделей у масштабі системи. - Довготривале збереження даних і підтримка мультидоменних сценаріїв
Крос-рівневі компоненти	Комунікаційна інфраструктура (V2X, 4G/5G, оптичні канали), механізми розподіленого навчання, аудит і моніторинг	- Забезпечення захищених каналів між усіма рівнями. - Передача оновлень моделей і політик без централізації сирих даних. - Формування єдиного простору довіри та спостереження

На рівні транспортних засобів розміщуються агенти взаємодії з мережею V2X, локальні модулі збору телеметрії та базові функції безпеки (наприклад, перевірка цілісності отриманих повідомлень або первинна обробка сенсорних даних). Вони виступають джерелами даних для наступних рівнів архітектури та ініціаторами транспортних подій.

Периферійний рівень (Edge / MEC) представлений дорожньою інфраструктурою з обчислювальними ресурсами (наприклад, придорожніми одиницями (RSU), базовими станціями 5G з MEC-серверами, локальними обчислювальними кластерами на рівні транспортних вузлів. Ці компоненти виконують агрегування телеметрії від транспортних засобів, локальний inference моделей машинного навчання для виявлення аномалій та підтримку сервісів з критичними вимогами до затримки (наприклад, динамічне управління світлофорами або кооперативне маневрування).

Регіональний рівень відповідає за координацію та оркестрацію транспортних сервісів у межах певної території. До нього належать центри управління дорожнім рухом, диспетчерські хаби громадського транспорту та control planes мультихмарної інфраструктури. На цьому рівні реалізуються механізми балансування навантаження між периферійними вузлами, узгодження політик безпеки та забезпечення стійкості роботи системи в разі локальних відмов.

Глобальний хмарний рівень забезпечує централізовану аналітику, управління політиками доступу та безпеки, довгострокове зберігання даних, навчання моделей та розповсюдження оновлень. Хмарні сервіси виступають вищим рівнем прийняття рішень, підтримують механізми міжрегіональної координації та забезпечують інтеграцію з зовнішніми платформами (наприклад, національними центрами безпеки чи транспортними дата-хабами). Хмарно-орієнтовану архітектуру інтелектуальних транспортних систем представлено на рис. 1.

Між усіма рівнями архітектури функціонує комунікаційна інфраструктура, що включає канали V2X, мобільний зв'язок 4G/5G, оптоволоконні з'єднання між регіональними центрами та захищені тунелі до хмарних дата-центрів. Кожен рівень виконує чітко визначені функції, але разом вони формують єдине адаптивне середовище для реалізації інтелектуальних транспортних сервісів.

Зростання ролі інтелектуальних транспортних систем та взаємодіючих транспортних засобів супроводжується активною інтеграцією компонентів машинного навчання (ML) у критичні контури прийняття рішень. Детектори аномалій, прогностичні моделі та механізми автономного управління дедалі частіше розміщуються у розподіленому середовищі, яке охоплює бортові пристрої, регіональні периферійні вузли (edge) та централізовану хмарну інфраструктуру. Така архітектура дає змогу досягати високої продуктивності та масштабованості, але водночас створює новий клас загроз, пов'язаний з уразливістю ML-моделей і складністю забезпечення їхньої узгодженої роботи в мультиагентних середовищах.

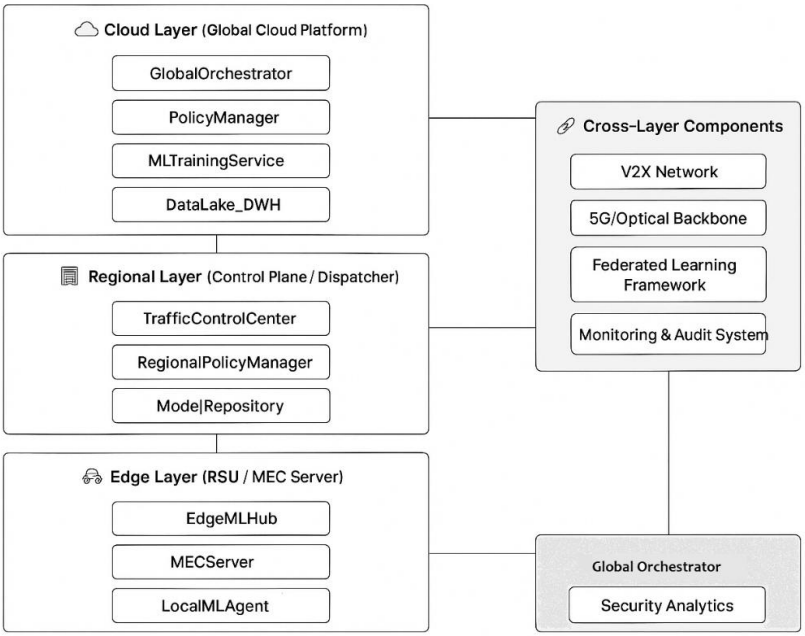


Рис. 1. Хмарно-орієнтована архітектура інтелектуальних транспортних систем

Традиційні механізми безпеки мереж та протоколів не враховують специфіку ML-компонентів, які можуть бути ціллю adversarial-впливів, атак отруєння даних, або дестабілізовані некоректними локальними оновленнями у розподіленому навчанні. Крім того, потоковий характер даних у ІТС вимагає інкрементальних і ресурсно-ефективних алгоритмів, здатних адаптуватися до змін середовища без втрати точності та надійності.

Отже, безпечна інтеграція ML у хмарно-периферійну архітектуру ІТС вимагає комплексного підходу, який включає:

- стійкі методи обробки потокових даних та виявлення аномалій у реальному часі;
- розподілене навчання моделей із гарантіями приватності та захистом від зіпсованих оновлень;
- засоби виявлення та нейтралізації adversarial-впливів як на етапі тренування, так і під час роботи системи;
- координацію політик безпеки між усіма рівнями архітектури (on-board, edge, cloud).

Далі наведено детальніший аналіз основних складових комплексного підходу до інтеграції ML у хмарно-периферійну архітектуру ІТС.

Детекція аномалій у потокових даних (схему роботи детектора аномалій у потокових даних представлено на рис. 2**)**

Потокові дані, які надходять від транспортних засобів, дорожньої інфраструктури або IoT-сенсорів, мають кілька характерних особливостей: дані генеруються постійно, у реальному часі, що ускладнює їхнє зберігання та обробку повністю; невизначена та змінювана динаміка, тобто поведінка транспортних потоків може різко змінюватися через погодні умови, аварії, зміни трафіку; наявність аномалій, вихідні дані можуть містити різні аномальні події, такі як ДТП, збої сенсорів або відхилення у рухові транспортних засобів.

У цьому контексті детекція аномалій стає інструментом для забезпечення безпеки та ефективності транспортної системи, оскільки дозволяє оперативно виявляти події, що відрізняються від нормальної поведінки.

Завдання детекції аномалій у потокових даних можна представити математично наступним чином:

$$\hat{y}^t = f_0(X_t), \qquad X_t \in R^{n \times d}, \quad \hat{y}^t \in \{0,1\},$$

де: X_t – матриця телеметричних або сенсорних даних у момент часу t, розмірності n×d; n – кількість спостережень у потоці; d – кількість ознак (наприклад, швидкість, прискорення, GPS-координати, дані камер або LIDAR); f_0 – модель машинного навчання з параметрами θ; $\hat{y}^t$ – бінарна класифікація: 0 – нормальна подія, 1 – аномальна.

Для аналізу потокових даних найчастіше застосовують рекурентні нейронні мережі, зокрема LSTM (Long Short-Term Memory) та GRU (Gated Recurrent Unit). Моделі типу LSTM здатні враховувати довгострокові залежності у часових рядах, що дозволяє ефективно прогнозувати динамічні процеси у транспортних потоках. Архітектура GRU забезпечують нижчі обчислювальні витрати при збереженні високої точності прогнозів. Такі моделі навчаються на нормальних даних і прогнозують наступні значення ознак, а значні відхилення фактичних даних від прогнозованих інтерпретуються як потенційні аномалії.

Принцип роботи:

1.Мережа навчається кодувати вхідні дані X_t у латентний простір та відновлювати їх $\hat{X}_t$.

2.На нормальних даних відновлення близьке до оригіналу.

3.Аномалії викликають високі помилки реконструкції.

Критерій аномалії: $\text{Reconstruction Error} = \|X_t - \hat{X}_t\|_2$,

Аномалія детектується, якщо *Reconstruction Error* > ϵ, де ϵ – порогове значення.

Потокові алгоритми оновлення

В умовах безперервного надходження даних у реальному часі моделі повинні оновлювати свої параметри інкрементально, без повного перенавчання. Такий підхід базується на поступовому оновленні ваг моделі за правилом:

$$\theta_{t+1} = \theta_t - \eta \nabla_\theta L(f_\theta(X_t), y_t),$$

де: η – швидкість навчання; L – функція втрат (наприклад, MSE для автоенкодерів); y_t – наявна мітка події (якщо є) або опорна нормальна поведінка.

Інкрементальні оновлення дозволяють адаптувати модель до нових умов без повного перенавчання.

Під час обробки даних у реальному часі ключовим є забезпечення низької затримки, адже виявлення аномалій має відбуватися миттєво для оперативного реагування на події. Важливою властивістю моделей є їхня адаптивність до сезонних і довгострокових змін транспортних потоків. Оскільки периферійні пристрої часто мають обмежені обчислювальні ресурси, перевага надається компактним моделям або технологіям дистиляції знань. Додатковою проблемою є наявність шуму та нестача міток у даних, що вимагає застосування методів безнаглядного навчання (unsupervised learning), здатних ідентифікувати аномалії без попередньо розмічених прикладів.

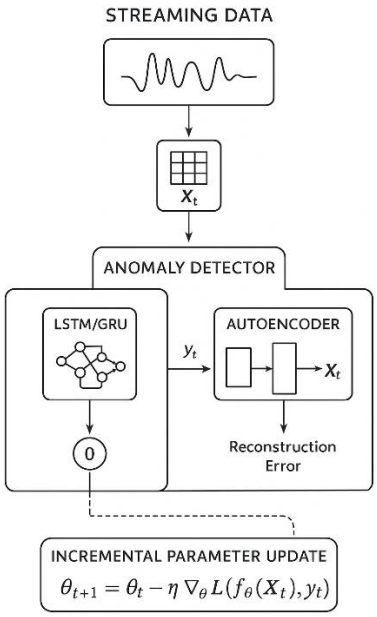


Рис. 2. Схема роботи детектора аномалій у потокових даних

Методи детекції аномалій використовуються для виявлення дорожньо-транспортних пригод або різких гальмувань за даними телеметрії транспортних засобів, для моніторингу стану дорожньої інфраструктури за допомогою сенсорів та камер, для фіксації збоїв сенсорів або некоректних показників у мережі IoT. Крім того, такі підходи сприяють оптимізації маршрутів шляхом раннього виявлення аномальних заторів чи перевантажень транспортних вузлів.

Розподілене навчання та приватність

У мультиагентних хмарно-орієнтованих інтелектуальних транспортних системах дані генеруються та зберігаються на різних рівнях, а саме у бортових системах транспортних засобів, на периферійних серверах (edge) та у хмарних центрах обробки даних. Централізоване збирання всіх сирих даних у хмарі створює ризики витоку приватної інформації та надмірні затримки при обробці, тому для забезпечення конфіденційності дедалі частіше застосовується розподілене навчання (Federated Learning). Його принцип полягає у тому, що кожен вузол системи виконує локальне навчання на власних даних, а з хмарою синхронізуються лише оновлені параметри моделі, без передавання сирих даних.

Нехай у системі функціонує *K* вузлів, кожен із власним набором даних D_k. На кожному вузлі *k* локальна модель f_θ оновлюється за формулою:

$$\theta_k^{(t+1)} = \theta_k^{(t)} - \eta \nabla_\theta L(f_\theta(D_k), y_k),$$

де η – швидкість навчання, а *L* – функція втрат, що визначає різницю між прогнозом моделі та реальними значеннями. Після завершення локального етапу навчання параметри з усіх вузлів об'єднуються у хмарному середовищі для формування глобальної моделі θ_Gза принципом середньозваженого оновлення:

$$\theta_G^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{\sum_{j=1}^{K} n_j} \theta_k^{(t+1)},$$

де $n_k = |D_k|$ – кількість прикладів у локальному наборі даних вузла *k*. Такий підхід забезпечує узгодженість параметрів між усіма рівнями архітектури бортовим, периферійним та хмарним і дозволяє масштабувати систему на мультихмарні середовища без централізації чутливої інформації.

Перевагами розподіленого навчання є збереження конфіденційності даних, узгодженість моделей у розподіленій екосистемі та масштабованість для великих гібридних середовищ. Водночас низка технічних викликів залишається відкритою. Серед них необхідність ефективної синхронізації оновлень між численними вузлами, стійкість системи до зіпсованих або шкідливих локальних оновлень, а також забезпечення низької латентності навчання і прийняття рішень у реальному часі.

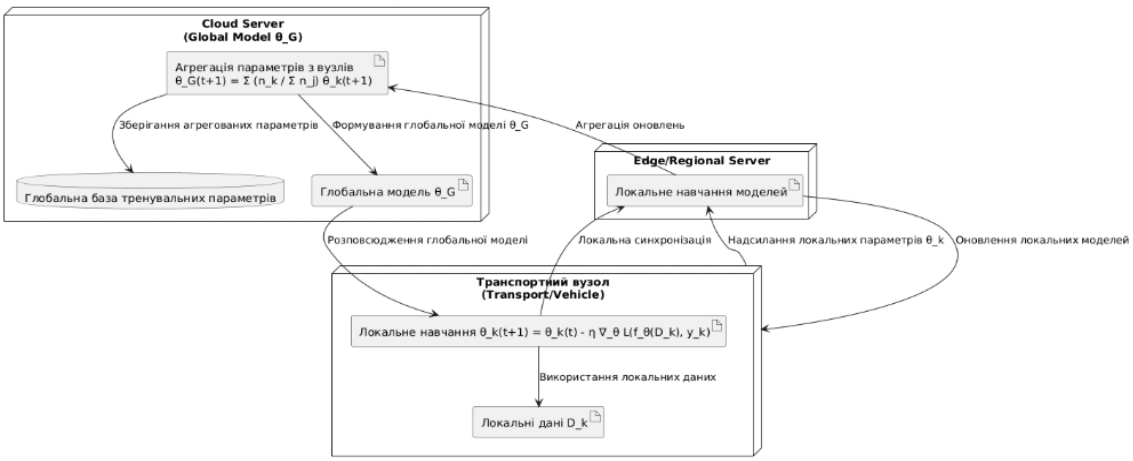


Рис. 3. Схема моделі розподіленого навчання

Розподілене навчання моделей має широке практичне застосування в інтелектуальних транспортних системах. Зокрема, воно використовується для побудови детекторів аномальної поведінки транспортних засобів без обміну персональними даними між вузлами, для спільного навчання моделей прогнозування дорожньої ситуації між edge-серверами у різних регіонах, а також для оновлення моделей штучного інтелекту у транспортних засобах через хмарну інфраструктуру без порушення приватності користувачів. Крім того, розподілені підходи дозволяють об'єднувати знання, отримані в різних містах або зонах транспортної мережі, формуючи узгоджене середовище аналітики без централізації потоків даних.

Adversarial-атаки та методи протидії

ML-компоненти у ІТС вразливі до adversarial-впливів, які можуть маніпулювати результатами детекції. Формально, adversarial-приклад X_t' створюється шляхом додавання обмеженого за нормою шуму δ до оригінального вхідного сигналу X_t так, щоб модель f_θ класифікувала модифікований вхід неправильно:

$$X_t' = X_t + \delta, \quad f_\theta(X_t') \neq f_\theta(X_t), \qquad \|\delta\|_\infty \leq \epsilon$$

Тобто δ змінює класифікацію, залишаючись при цьому невеликим за амплітудою, що робить його непомітним для людини, але достатнім для обману моделі.

Для протидії adversarial-атакам застосовуються різні методи:

1. Robust Training передбачає навчання моделі на модифікованих даних, які включають adversarial-приклади, що формалізується як:

$$\theta^* = \arg\min_\theta E_{(X,y)\sim D}\left[\max_{\|\delta\|\leq\epsilon} L(f_\theta(X+\delta), y)\right].$$

2. Certified defenses – сертифіковані методи, що гарантують обмеження похибки під атакою.

3. Runtime shielding та model-watchdogs – моніторинг поведінки моделей під час виконання, наприклад, перевірка відхилень у прогнозах або аномалій у вхідних даних.

В хмарно-периферійних ІТС ці методи застосовуються на всіх рівнях: локально, у бортових системах, регіонально – на edge/MEC-серверах та централізовано – у хмарних сервісах.

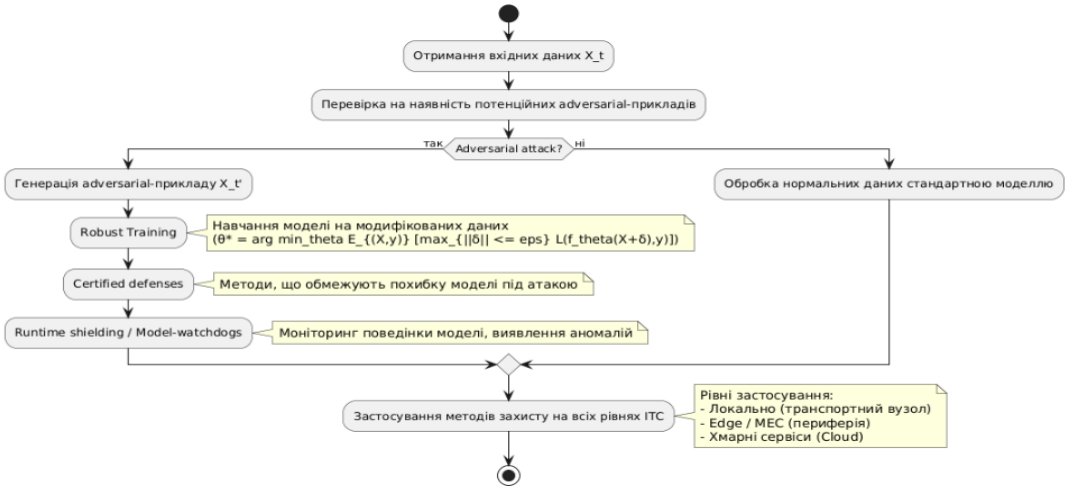


Рис. 4. Процес протидії adversarial-атакам у хмарно-орієнтованих інтелектуальних транспортних системах

Архітектурно-функціональна модель адаптивного управління безпекою ІТС

У хмарно-орієнтованих інтелектуальних транспортних системах безпека не може гарантуватися виключно за допомогою статичних політик та централізованих механізмів контролю. На відміну від традиційних корпоративних або відомчих інформаційних систем, ІТС функціонують у відкритому, багатодоменному та високодинамічному середовищі, де мережеві топології, ролі агентів і загрозова ситуація змінюються в реальному часі. Прикладом є сценарії переміщення транспортних засобів між зонами дії різних edge-провайдерів або мультихмарних сегментів, коли правила доступу, довірчі відносини й контури захисту мають оновлюватися без затримок, щоб зберегти цілісність системи.

Адаптивне управління безпекою забезпечує динамічне коригування політик, конфігурацій і механізмів контролю відповідно до поточного контексту функціонування системи, рівня загроз та стану окремих компонентів. На відміну від статичних моделей доступу (наприклад, RBAC), які задають незмінні правила, адаптивний підхід передбачає використання аналітики потокових даних, оцінювання ризиків і телеметричних сигналів для прийняття рішень у режимі реального часу. Це особливо важливо в мультиагентних сценаріях, де порушення в одному сегменті (наприклад, компрометація edge-вузла або підробка телеметрії) може каскадно впливати на глобальну систему керування транспортними потоками.

Ключова роль адаптивного управління полягає у забезпеченні когерентності політик безпеки між усіма рівнями архітектури (бортовим, периферійним, регіональним та хмарним) при збереженні працездатності системи, навіть у разі виникнення інцидентів. Для цього адаптивні механізми повинні: безперервно збирати та аналізувати інформацію про стан мережі, поведінку агентів і контекст загроз; здійснювати оцінювання ризиків у реальному часі з урахуванням локальних і глобальних факторів; узгоджувати зміни політик між розподіленими елементами системи, забезпечуючи відсутність суперечностей; застосовувати контрзаходи, які мінімізують вплив атаки без порушення критичних транспортних сервісів (graceful degradation).

Отже, адаптивне управління виступає не окремим модулем, а координуючим механізмом, який охоплює всі рівні хмарно-орієнтованої архітектури ІТС від локальних компонентів транспортних засобів і периферійних вузлів до регіональних оркестраторів і глобальних хмарних сервісів, забезпечуючи динамічну взаємодію між ключовими компонентами системи безпеки, такими як засоби аутентифікації та авторизації, детектори аномалій, системи моніторингу довіри, політикові рушії (policy engines) та контури оркестрації. Адаптивне управління інтегрується з аналітичними модулями, які виконують оцінку ризиків і контекстну обробку телеметрії, та з засобами реагування, спрямованими на нейтралізацію або локалізацію інцидентів безпеки, шляхом динамічної зміни політик доступу, переміщення обчислювальних завдань або ізоляції скомпрометованих вузлів. Завдяки цьому адаптивне управління створює основу для побудови масштабованих, стійких до загроз і функціонально безперервних транспортних інфраструктур, які здатні підтримувати безпечну роботу навіть за умов змін топології, зростання навантаження або цілеспрямованих атак на окремі компоненти системи.

Функціональна модель ІТС описує організацію процесів обробки даних та управління безпекою на всіх рівнях архітектури від бортових агентів транспортних засобів до глобальних хмарних сервісів та визначає ключові блоки системи, їхні функції та взаємозв'язки, а також потоки даних, які забезпечують обмін інформацією між компонентами. Для формалізації цих взаємодій застосовується DFD-модель, яка відображає процеси, сховища даних та напрямки потоків, тим самим забезпечуючи наочно-структурне представлення функціональної моделі.

На транспортному рівні автомобільні засоби оснащені агентами збору телеметрії та сенсорних даних, що виконують локальну детекцію аномалій і первинну обробку інформації. Ці процеси відповідають елементам DFD, які можна позначити як «Збір телеметрії та локальна детекція аномалій». Локальні сховища даних включають буфери телеметрії та журнали подій. Потоки даних від бортових агентів до периферійного рівня у DFD відображаються як вертикальні інформаційні канали, що забезпечують передачу агрегованих сенсорних даних для подальшого аналізу (на рис. 5. представлено DFD-модель хмарно-орієнтованої інтелектуальної транспортної системи).

Периферійний рівень (Edge/MEC) реалізує процеси потокової обробки телеметрії, локальної детекції аномалій з використанням моделей машинного навчання (LSTM/GRU), прогнозування дорожньої ситуації та підтримки сервісів з критичною затримкою. У DFD-моделі ці функції формалізовані як процес «Локальна аналітика та управління транспортними сервісами», а проміжні сховища даних відображаються як кешовані ML-моделі та буфери телеметрії. Потоки даних у DFD забезпечують вертикальну інтеграцію: агреговані результати аналітики від edge-вузлів надходять на регіональний рівень для координації та узгодження політик безпеки.

На регіональному рівні функціональна модель забезпечує координацію між edge-вузлами, балансування навантаження та узгодження політик безпеки, у DFD-моделі відображається процесом «Регіональна оркестрація та узгодження політик», а сховища включають бази даних стану вузлів і журнали подій. Потоки даних між регіональним та

глобальним рівнем у DFD-моделі формалізують передачу агрегованих результатів аналітики та оновлених політик безпеки, що забезпечує когерентність системи в реальному часі.

Глобальний хмарний рівень виконує централізовану аналітику, навчання та оновлення моделей машинного навчання, а також управління політиками доступу і безпеки, в DFD-моделі представлено процесом «Глобальна аналітика, навчання та управління політиками», сховища даних включають бази історичних подій та тренувальні набори моделей ML. Потоки даних забезпечують передачу оновлень моделей і політик на регіональні та периферійні рівні, завершуючи замкнутий цикл обробки даних.

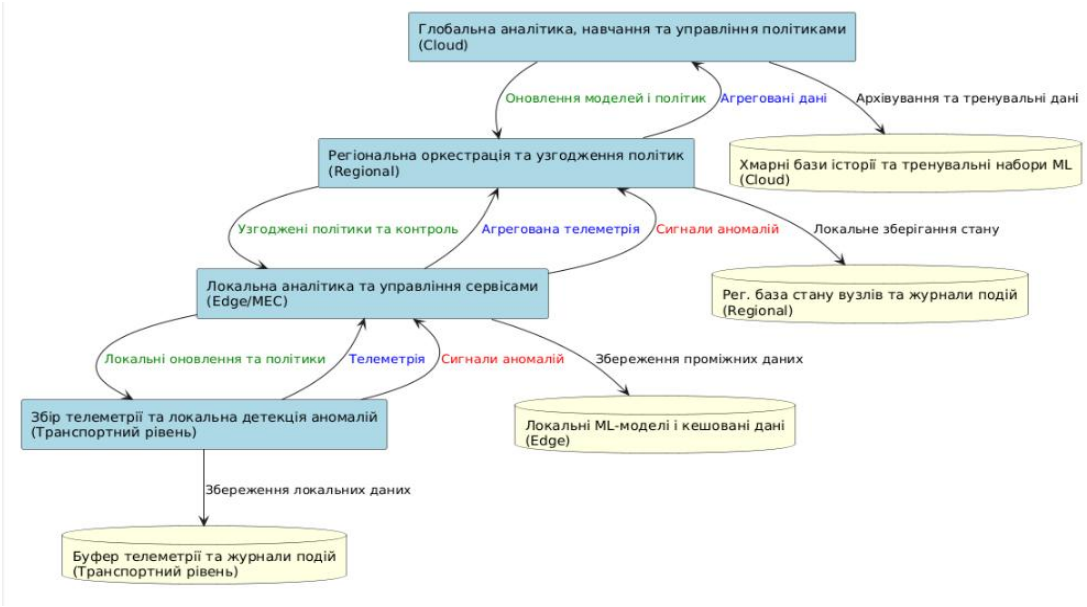


Рис. 5. DFD-модель хмарно-орієнтованої інтелектуальної транспортної системи

DFD дозволяє наочно показати, як інформація переміщується від бортових агентів транспортних засобів через периферійні та регіональні рівні до глобальних хмарних сервісів, а також як вона обробляється на кожному рівні для підтримки адаптивного управління безпекою.

Адаптивне управління інформаційною безпекою у хмарно-орієнтованих інтелектуальних транспортних системах передбачає динамічне коригування захисних заходів залежно від поточних характеристик середовища, стану мережної інфраструктури та поведінкових показників користувачів і транспортних об'єктів. Математична формалізація даного процесу дозволяє поєднати детекцію інцидентів, оцінку ризиків і прийняття рішень в єдину ітеративну процедуру зворотного зв'язку, що забезпечує автоматизацію реагування та ефективне розподілення обчислювальних і мережних ресурсів між різними рівнями системи.

Хмарно-орієнтована ІТС розглядається як дискретна динамічна система, стан якої в момент часу t позначається вектором $S(t)$ Еволюція стану описується функцією переходу

$$S(t+1) = f(S(t), A(t), E(t)),$$

де $A(t)$ – вектор адаптивних заходів безпеки (політики доступу, налаштування IDS/IPS, параметри шифрування, обмеження QoS тощо), $E(t)$ – вектор зовнішніх впливів (індикатори загроз, інтенсивність атак, мережеве навантаження), а f – функція переходу, що відображає динаміку системи під впливом заходів і загроз.

Загрози моделюються як стохастичний процес $R(t)$ що характеризується набором можливих інцидентів i з ймовірностями виникнення $p_i(t)$ і відповідними очікуваними втратами $L_i(t)$. Очікуваний ризик у момент часу t визначається інтегральною метрикою

$$R(t) = \sum_i p_i(t) L_i(t),$$

яка служить базовим показником для прийняття рішень щодо витрат на захист.

Адаптивне управління формулюється як задача мінімізації комбінованого функціоналу, що має такий запис:

$$J(S(t), A(t), E(t)) = a\,R(t) + \beta\,C(A(t)),$$

де $C(A(t))$ – функція витрат, що агрегує ресурси (обчислювальні потужності, пропускну здатність), часові затримки і непрямі операційні витрати; а a, β – вагові коефіцієнти, що визначають компроміс між рівнем захищеності та продуктивністю системи.

Для розв'язання задачі адаптивного управління застосовується набір алгоритмічних підходів, що доповнюють один одного: методи динамічного програмування для послідовного прийняття рішень у часі; стохастичні алгоритми для врахування невизначеності параметрів загроз; підходи підкріпленого навчання (*Reinforcement*

Learning, *RL*), де агент навчається політиці π шляхом максимізації довгострокової винагороди. У RL-контексті можна визначити миттєву винагороду як:

$$r(t) = -R(t) - \lambda\, C(A(t)),$$

де λ – коефіцієнт, що нормалізує вклад витрат.

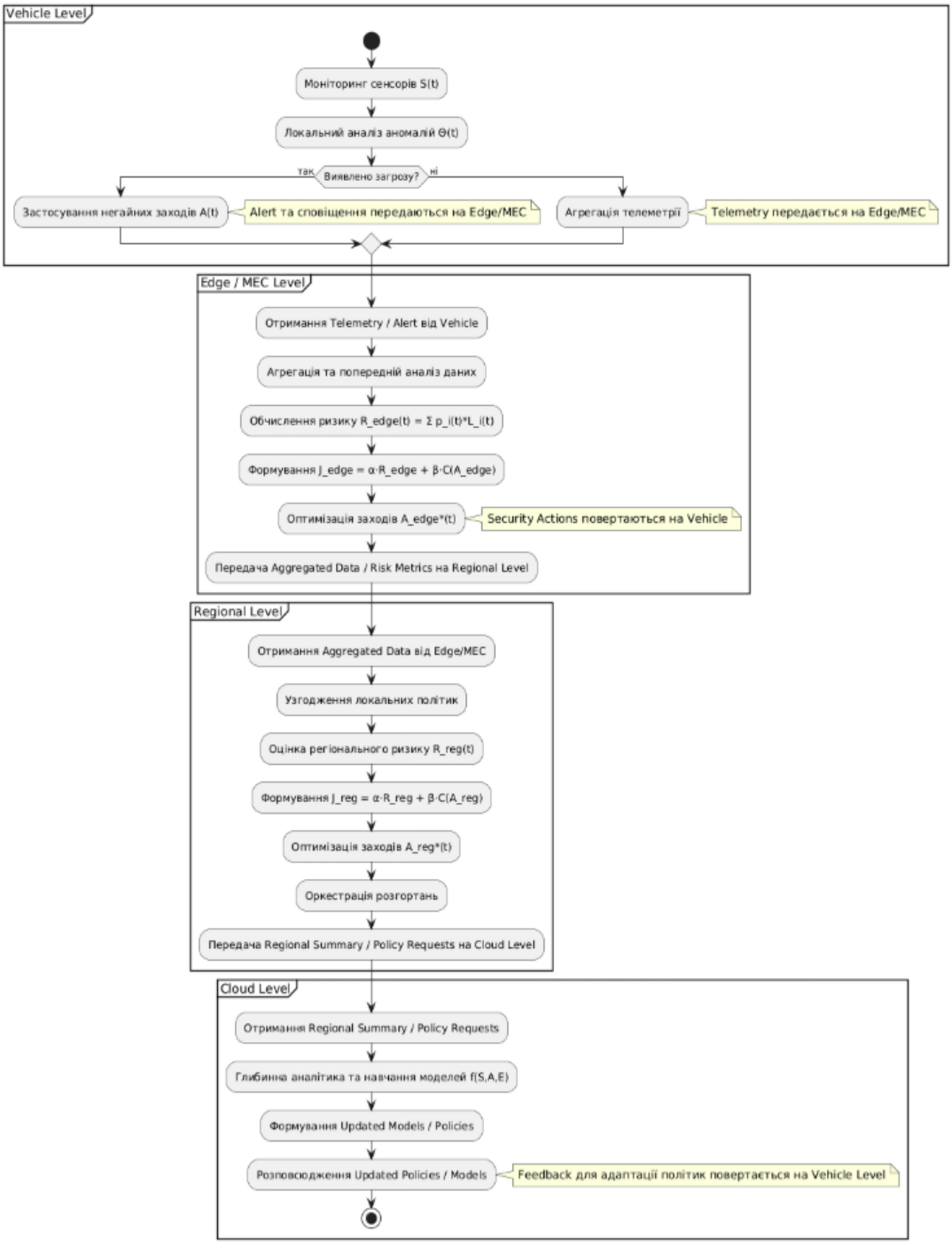


Рис. 6. Архітектура адаптивного управління інформаційною безпекою в хмарно-орієнтованих інтелектуальних транспортних системах

Додатково використовуються евристичні та оптимізаційно-орієнтовані методи (наприклад, багаторівневе евристичне планування), які дозволяють зберегти прийнятну обчислювальну складність при обмежених ресурсах.

Процес адаптації реалізується циклічно:

- моніторинг телеметрії, логів безпеки та мережевого трафіку;
- оцінка зовнішніх впливів $E(t)$ та обчислення ймовірностей $p_i(t)$;
- розрахунок ризику $R(t)$ та формування цільової функції J;
- обчислення $A^*(t)$ за допомогою комбінованих алгоритмів оптимізації;
- реалізація заходів і збір спостережень для оновлення моделі f і параметрів системи.

Механізм зворотного зв'язку передбачає регулярну корекцію моделей загроз і параметрів політик на основі аналітики ефективності заходів.

Особливості багаторівневого «Хмара–Периферія–Транспортні засоби» (*Cloud–Edge–Vehicle*) розгортання

Архітектура системи адаптивного управління інформаційною безпекою в хмарно-орієнтованих ІТС складається з чотирьох функціональних рівнів діяльності: рівень транспортних засобів, периферійний рівень (Edge / MEC), регіональний рівень, глобальний хмарний рівень (рис. 6).

Рівень транспортних засобів відповідає за збір телеметрії, локальний моніторинг стану безпеки, виявлення потенційних загроз та виконання негайних захисних дій. На цьому рівні формуються повідомлення *Alert* або агрегована телеметрія, які надсилаються на периферійний рівень для подальшої обробки та оцінки ризиків.

Периферійний рівень (Edge / MEC) забезпечує агрегацію даних від транспортних засобів і виконання попереднього аналізу загроз. Тут розраховується локальний ризик $R_{edge}(t)$ та формується функціонал оптимізації $J_{edge} = \alpha \cdot R_{edge}(t) + \beta \cdot C(A_{edge}(t))$, який дозволяє визначати оптимальні заходи безпеки. На цьому рівні застосовуються методи динамічного програмування, стохастичного управління, підкріпленого навчання (*Reinforcement Learning*) та евристичні алгоритми, що забезпечують адаптивне реагування на змінні умови загрозового середовища. Після обробки *Edge* рівень передає оновлені заходи безпеки до транспортних засобів та узагальнені дані на регіональний рівень.

Регіональний рівень виконує узагальнення результатів з кількох *Edge*-вузлів та координує політики безпеки між ними. На цьому рівні оцінюється регіональний ризик $R_{reg}(t)$та формується функціонал оптимізації J_{reg}, що дозволяє узгоджувати дії на всіх підпорядкованих вузлах. Регіональний рівень також здійснює оркестрацію розгортання політик і передає аналітичні дані та запити щодо політик на глобальний хмарний рівень.

Глобальний хмарний рівень забезпечує централізовану аналітику, навчання комплексних моделей *f(S, A, E)* та формування оновлених політик безпеки *Updated Policies* і моделей *Updated Models*, які розповсюджуються на регіональний та периферійний рівні. Даний рівень дозволяє підтримувати глобальний контроль, оцінку ефективності заходів безпеки та інтегрувати механізми зворотного зв'язку для адаптації політик у режимі реального часу.

Особливості хмарно-орієнтованих ІТС полягають у багаторівневій структурі прийняття рішень: частина функцій виконується на периферії (edge/MEC-серверах), розташованих близько до джерел даних, а решта – у центральних хмарних сервісах. Така розподілена архітектура потребує багаторівневого моделювання станів і ризиків. Адаптивне управління в цьому контексті забезпечує реактивну безпеку, дозволяючи оперативно реагувати на DDoS-атаки, маніпуляції сенсорними потоками та adversarial-атаки на ML-моделі. Додатково алгоритми управління враховують обмеження пропускної здатності мережі, часові затримки та наявні обчислювальні ресурси, що забезпечує ефективне функціонування системи в умовах реального часу.

Висновки та перспективи подальших досліджень

У роботі здійснено системний аналіз архітектурних особливостей хмарно-орієнтованих інтелектуальних транспортних систем та обґрунтовано підходи до математичної й алгоритмічної формалізації адаптивного управління інформаційною безпекою. Розроблена модель розглядає ІТС як дискретну динамічну систему з функцією переходу станів, яка описує еволюцію системи під впливом адаптивних заходів безпеки та факторів зовнішніх загроз. Процес управління формалізовано у вигляді задачі оптимізації комбінованого критерію, який інтегрує показники ризику та ресурсних витрат, що забезпечує оптимальне співвідношення між рівнем захисту та ефективністю функціонування системи.

Запропонований підхід передбачає інтеграцію механізмів збору та аналітичної обробки телеметричних і мережевих даних, методів оцінювання рівня загроз і ризиків, алгоритмів оптимізаційного вибору заходів та політик інформаційної безпеки, а також механізмів зворотного зв'язку між архітектурними рівнями системи (транспортним, периферійним, регіональним і хмарним) в єдину замкнену систему адаптивного управління. У статті використано алгоритми машинного навчання для виявлення аномалій у потокових телеметричних даних та застосовано методи розподіленого навчання (Federated Learning) з метою забезпечення узгодженості моделей між архітектурними рівнями без централізації даних. Також проаналізовано методи протидії adversarial-атакам, які охоплюють як етапи тренування, так і експлуатації моделей.

Практична цінність отриманих результатів полягає у можливості побудови масштабованих, стійких до загроз та ресурсно-ефективних систем захисту для сучасних мультиагентних хмарно-орієнтованих транспортних середовищ. Представлена модель може бути використана під час проектування національних транспортних дата-хабів, систем управління міською мобільністю та платформ для взаємодії підключених і автономних транспортних засобів.

Подальші дослідження доцільно зосередити на: розробленні прототипів агентів адаптивного управління для периферійного рівня з урахуванням

обмежень обчислювальних ресурсів; інтеграції методів підкріпленого навчання з алгоритмами стохастичного управління для підвищення ефективності прийняття рішень в умовах невизначеності; стандартизації механізмів узгодження політик безпеки між мультихмарними сегментами та транспортними доменами; розробленні формальних методів оцінювання ефективності адаптивного управління в реальних міських транспортних сценаріях.

Література

[1] Sedar R., Kalalas C., Vázquez-Gallego F., Alonso L., Alonso-Zárate J. A comprehensive survey of V2X cybersecurity mechanisms and future research paths (2023). *IEEE Open Journal of the Communications Society*, №4, 325–391. Piscataway, NJ: IEEE. DOI: 10.1109/OJCOMS.2023.3239115.

[2] Zhu Q., Yu B., Wang Z., Tang J., Chen Q. A., Li Z., Liu X., Luo Y., Tu L. Cloud and Edge Computing for Connected and Automated Vehicles (2023). *Foundations and Trends® in Electronic Design Automation*, Vol. 14, No. 1-2, pp. 1–170. Hanover, MA: Now Publishers Inc. DOI: 10.1561/1000000058.

[3] Solaas J. R. V., Tuptuk N., Mariconti E. Systematic Literature Review: Anomaly Detection in Connected and Autonomous Vehicles (2024). *IEEE Transactions on Intelligent Transportation Systems*, 26(1), 43–58. Piscataway, NJ: IEEE. DOI: 10.1109/TITS.2024.3495031.

[4] Wang B., Li W., Khattak Z. H. Anomaly Detection in Connected and Autonomous Vehicle Trajectories Using LSTM Autoencoder and Gaussian Mixture Model (2024). *Electronics*, 13(7), 1251. Basel: MDPI. DOI: 10.3390/electronics13071251.

[5] Gebrezgiher Y. T., Jeremiah S. R., Gritzalis S., Park J. H. VAE-Based Real-Time Anomaly Detection Approach for Enhanced V2X Communication Security (2025). *Applied Sciences*, 15(12), 6739. Basel: MDPI. DOI: 10.3390/app15126739.

[6] Raza S., Sapkota R., Karkee M., Emmanouilidis C. TRiSM for Agentic AI: A Review of Trust, Risk, and Security Management in LLM-based Agentic Multi-Agent Systems (2025). *arXiv preprint* arXiv:2506.04133. DOI: 10.48550/arXiv.2506.04133.

[7] Marek Pawlicki, Aleksandra Pawlicka, Rafał Kozik, Michał Choraś. A meta-survey of adversarial attacks against artificial intelligence algorithms, including diffusion models (2025). *Neurocomputing* Volume 653, 7 November 2025. DOI: https://doi.org/10.1016/j.neucom.2025.131231

[8] Mashkina, Iryna, Rzaieva Svitlana, Kostiuk Yuliia, Mazur, Nataliia, Brzhevska Zoreslava (2025) Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). с. 1-13. ISSN 1613-0073.

[9] Rzaieva Svitlana, Rzaiev Dmytro, Mykytenko Nelya, Dreis Yurii, Grechaninov Viktor (2025) Methods of Personal Data Protection in Retail: Practical Solutions. *Cybersecurity Providing in Information and Telecommunication Systems 2025* (3991). с. 492-506. ISSN 1613-0073. https://ceur-ws.org/Vol-3991/

[10] Rzaieva, S., Rzaiev, D., Kostyuk, Y., Hulak, H., Shcheblanin, O. Methods of Modeling Database System Security. *CEUR Workshop Proceedings*, 2024, 3654, pp. 384–390. *https://ceur-ws.org/Vol-3654/*

[11] Костюк Ю. В., Бебешко Б. Т., Гулак Г.М., Складанний П. М., Рзаєва С. Л., Хорольська К. В. Забезпечення кібербезпеки та швидкодії передачі даних у безпровідних мережах. //Безпека інформації, Том 30 №3 (2024). С. 365-375. DOI: 10.18372/2225-5036.30.20357

[12] Складанний П. М., Машкіна І.В., Рзаєва С. Л., Костюк Ю. В. Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз // Телекомунікаційні та інформаційні технології. № 2 (2025). С. 59-76. DOI: 10.31673/2412-4338.2025.027860

[13] Складанний П. М., Костюк Ю. В., Рзаєва С. Л., Самойленко Ю. О., Савченко Т. В. Розробка модульних нейронних мереж для виявлення різних класів мережевих атак // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», Том 3 №27 (2025). С. 534-548. DOI: https://doi.org/10.28925/2663-4023.2025.27.772

[14] Костюк Ю. В., Бебешко Б. Т., Складанний П. М., Рзаєва С. Л., Хорольська К. В. Оптимізація буфера та пріоритетів для забезпечення безпеки у Bluetooth-мережах // Безпека інформаційних систем і технологій, Том 2 №8 (2024). С. 5-16. DOI: https://doi.org/10.17721/ISTS.2024.8

УДК 004.056.5:004.7:656.1

Rzaeva S., Skladannyi P., Kostiuk Y., Abramov V., Kravchenko V. Adaptive Information Security Management in Cloud-Oriented Intelligent Transportation Systems

Abstract. *The paper investigates theoretical and applied aspects of adaptive information security management in cloud-oriented Intelligent Transportation Systems (ITS). We analyze architectural features of the "Cloud–Edge–Vehicle" environment, identify key cyber-threat vectors, and substantiate the shortcomings of traditional security approaches – specifically static access policies, centralized PKI solutions, and classical IDS/IPS – in multi-domain, dynamic transportation ecosystems. We develop a mathematical and algorithmic model of adaptive management that treats an ITS as a discrete dynamical system whose state evolves over time under the influence of external threat factors and adaptive security measures. The control problem is formalized as minimization of a combined risk-and-cost functional, ensuring a balance between the level of protection and system performance. Within the proposed approach, mechanisms for collecting and analyzing telemetry and network data, risk assessment methods, algorithms for optimal selection of security policies, and feedback loops across architectural layers are integrated into a single closed-loop adaptive management system. For anomaly detection in streaming data, we apply machine-learning algorithms (in particular, LSTM/GRU and autoencoders), while model consistency across layers without data centralization is achieved via Federated Learning. We consider methods to counter adversarial attacks both during training and at inference time for ML components. The obtained results provide a scientific foundation for building scalable, threat-resilient, and resource-efficient protection mechanisms for cloud-oriented ITS. The proposed model can be used to enhance the security of transportation networks, ensure policy coherence across architectural layers, and automate real-time cyber-threat response.*

Keywords: *adaptive security management; intelligent transportation systems; cloud-oriented architecture; risk assessment; streaming data; federated learning; adversarial attacks; machine learning; information security.*

Рзаєва Світлана Леонідівна, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка.
Rzaeva Svitlana, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science Borys Grinchenko Kyiv Metropolitan University.

Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Skladannyi Pavlo, PhD, Associate Professor, Head of the Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

Костюк Юлія Володимирівна, PhD, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Kostiuk Yuliia, PhD, Associate Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Абрамов Вадим Олексійович, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка.
Abramov Vadym, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Science Borys Grinchenko Kyiv Metropolitan University.

Кравченко Володимир Георгійович, кандидат технічних наук, доцент, доцент кафедри інформатики та системології Київського національного економічного університету імені Вадима Гетьмана.
Kravchenko Volodymyr, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Informatics and Systemology, Kyiv National Economic University named after Vadym Hetman.