КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.956
УДК 004.056.5:004.89:621.311.1:004.75

Костюк Юлія Володимирівна
PhD in Computer Science
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук, доцент
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Самойленко Юлія Олександрівна
кандидат технічних наук, доцент
доцент кафедри автоматизації та комп'ютерних технологій систем управління
ім. професора А.П. Ладанюка
Національний університет харчових технологій, м. Київ, Україна
ORCID: 0000-0003-3787-1435
samoilenkouo@nuft.edu.ua

Коршун Наталія Володимирівна
доктор технічних наук, професор
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
ORCID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ ТА ЗАХИСТУ В КІБЕРФІЗИЧНИХ І ХМАРНИХ СЕРЕДОВИЩАХ SMART GRID

Анотація. У статті досліджено методологічні, алгоритмічні та архітектурні підходи до проєктування інтелектуальних систем керування та захисту, спрямованих на забезпечення стійкості функціонування Smart Grid в умовах зростання інтенсивності кіберзагроз. Обґрунтовано необхідність переходу від традиційних IT-орієнтованих засобів безпеки до гібридних адаптивних рішень, що поєднують механізми кіберфізичної живучості, автоматичного відновлення та когнітивного реагування на атаки типу Denial-of-Service, spoofing, data injection та інші високоризикові впливи. Запропоновано концептуальну модель архітектури стійкості Smart Grid, побудовану на синтезі методів робастного оцінювання, fault-tolerant control, розподіленої фільтрації (Distributed Kalman Filtering) і моделей динамічного управління довірою. Проведено системну класифікацію сучасних векторів атак на цифрові підстанції, SCADA, RTU та HMI з формалізацією вимог до їхнього захисту в контексті інформаційної та фізичної безпеки. Досліджено хмарно-edge оркестрацію потоків телеметрії Smart Grid із розміщенням аналітики поблизу джерела даних та масштабованим агрегуванням у хмарі для навчання моделей і кореляції подій у реальному часі. Запропоновані механізми враховують вимоги до латентності, пропускної здатності та ізоляції навантажень

у хмарних середовищах. Обґрунтовано виклики впровадження безперервного моніторингу, аналізу аномалій і формування рішень у реальному часі. Визначено перспективні напрями розвитку самонавчальних моделей виявлення інцидентів і реактивного управління на основі алгоритмів штучного інтелекту з урахуванням вимог до масштабованості, надійності та стійкості до прихованих загроз. Ефективність моделі підтверджено експериментальним моделюванням атак типу false data injection, DoS і spoofing у середовищі цифрових підстанцій Smart Grid.

Ключові слова: Smart Grid, хмарні обчислення, edge-комп'ютинг, оркестрація, інтелектуальне керування, стійкість до атак, розподілений фільтр Калмана, метрики довіри, керування з підвищеною живучістю, кіберфізичні системи.

ВСТУП

Цифрова трансформація енергетичного сектору, обумовлена впровадженням технологій Інтернету речей (IoT), штучного інтелекту (AI), edge-комп'ютингу та хмарних обчислень, зумовила еволюцію традиційних енергомереж у Smart Grid – гетерогенні, динамічні та масштабовані кіберфізичні системи (КФС), які забезпечують інтеграцію обчислювальних, комунікаційних і фізичних підсистем в єдину інтелектуальну інфраструктуру [1]. Концепція Smart Grid орієнтована на гнучке управління генерацією, розподілом і споживанням електроенергії в режимі реального часу, з урахуванням коливань навантаження, інтеграції відновлюваних джерел енергії, ринку електроенергії та децентралізованих систем зберігання.

У практичних розгортаннях Smart Grid дані первинного рівня (ПЛК/RTU, цифрові підстанції) попередньо обробляються на edge-вузлах (фільтрація, локальні правила безпеки), тоді як хмарний рівень забезпечує збір телеметрії, довгострокове зберігання, навчання моделей ML/AI та кореляцію інцидентів. Такий edge→cloud ланцюжок мінімізує затримки керування і водночас надає масштабовані ресурси для аналітики та резервування. У хмарному середовищі реалізуються сервіси централізованого моніторингу, управління політиками безпеки, координації SIEM/SOAR та оновлення моделей у реальному часі. Завдяки контейнеризації та оркестрації забезпечується динамічне масштабування обчислень, балансування навантажень і стійкість до збоїв. Таким чином, хмарна інфраструктура виступає інтеграційним ядром Smart Grid, що об'єднує інтелектуальні функції керування, аналізу та захисту в єдиному адаптивному контурі.

Попри очевидні переваги, така цифровізація суттєво підвищує поверхню атаки енергетичних систем, оскільки мережеві компоненти та протоколи обміну даними стають потенційною точкою входу для координованих, поліморфних і стійких кібератак [2, 7-8]. Ключові підсистеми керування – SCADA, PLC, RTU, цифрові підстанції, HMI-інтерфейси – дедалі частіше піддаються атакам типу Denial-of-Service (DoS), spoofing, false data injection, replay-атаки, а також ботнет-інфільтрації через вразливі IoT-компоненти [3-4, 6, 13]. Відомі інциденти, зокрема атаки на енергосистему України (BlackEnergy, Industroyer), компрометація Colonial Pipeline у США та атаки на об'єкти критичної інфраструктури Ізраїлю, продемонстрували, що наслідки можуть мати не лише економічний, а й геополітичний і соціальний характер.

У цьому контексті стає очевидною недостатність традиційних IT-орієнтованих засобів захисту, які передбачають переважно реактивні заходи, централізовану фільтрацію трафіку та ручне реагування [5, 14]. У реаліях Smart Grid, де критичні процеси мають жорсткі часові обмеження, навіть незначні затримки в обробці або

недостовірність сенсорних даних можуть призвести до каскадних збоїв [2-4, 8, 10, 13]. Відтак зростає потреба в інтелектуальних адаптивних системах керування та захисту, здатних забезпечити живучість (survivability) – тобто збереження функціональності в умовах порушення, – та стійкість (resilience) до складних, багаторівневих атак.

Наукова новизна дослідження полягає у формалізації інтегрованої концепції захищеного керування в середовищі Smart Grid, яка базується на синтезі: робастних методів оцінювання стану при наявності неповних або скомпрометованих даних [3, 14], fault-tolerant керування з можливістю динамічного переналаштування контролера [5], розподіленої Kalman-фільтрації [3, 10] (DKF) у багатосенсорному середовищі з обмеженим довірчим контекстом, моделей динамічного управління довірою [18], які дозволяють виявляти потенційно скомпрометовані вузли в реальному часі [11, 14-16], самонавчальних механізмів виявлення аномалій і атак із використанням алгоритмів машинного навчання (ML) та прогнозної аналітики.

На відміну від класичних підходів, запропонована архітектура не лише забезпечує виявлення та локалізацію атак, а й адаптивне модифікування політик керування з урахуванням ризик-профілю загроз, QoS-характеристик мережі та рівня довіри до окремих елементів системи [9, 18]. Це відкриває перспективи побудови кіберстійких енергетичних систем нового покоління, здатних функціонувати навіть у ситуаціях часткової відмови компонентів або цілеспрямованого зовнішнього впливу [4-5, 12]. Таким чином, робота спрямована на обґрунтування та реалізацію моделі інтелектуального захищеного керування Smart Grid, яка уможливлює автономну підтримку функціональної цілісності системи в умовах активного кібернетичного протистояння.

Для досягнення поставленої мети використано поєднання теоретичних і прикладних методів аналізу, моделювання та оцінювання стійкості кіберфізичних систем Smart Grid в умовах кібератак. Основою дослідження стали методи системного аналізу енергетичних КФС, зокрема структурно-функціонального моделювання SCADA-архітектури, методи розподіленої Kalman-фільтрації для ідентифікації некоректних або скомпрометованих сенсорних даних, а також fault-tolerant підходи до автоматичного переналаштування керуючих елементів. З метою виявлення аномальної активності та оцінки ризиків впроваджено машинне навчання, зокрема алгоритми кластеризації, прогнозного моделювання та градієнтного бустингу, адаптовані до контексту динамічної довіри [6, 15]. Також використано методи формалізації політик керування на основі моделі ризик-профілю загроз, з урахуванням QoS-параметрів мережі [18, 20]. Реалізовано комбінований підхід до тестування працездатності моделі на симульованих сценаріях атак типу false data injection, DoS та spoofing у середовищі цифрових підстанцій [3-4, 9, 13]. На основі проведених експериментів здійснено верифікацію архітектурних рішень щодо забезпечення живучості та кіберстійкості Smart Grid у реальному часі.

Для моделювання розміщення компонентів застосовано логіку: DKF та модуль довіри − на edge, а агрегування показників ризику, журналів та офлайн-навчання моделей − у хмарному середовищі. Для підвищення ефективності взаємодії між рівнями передбачено адаптивну синхронізацію потоків даних і політик безпеки між edge та хмарою. Такий підхід дає змогу оптимізувати розподіл навантаження, зменшити обсяг переданих даних і забезпечити безперервність аналітики навіть у разі часткових відмов мережевих сегментів. У результаті формується гібридна хмарно-edge інфраструктура, здатна до автономного функціонування, швидкого реагування на інциденти та централізованого навчання моделей штучного інтелекту.

Для реалізації та тестування моделі використовувалося середовище MATLAB/Simulink з інструментарієм Control System Toolbox і Statistics & Machine Learning Toolbox [3, 6]. Було змодельовано 20 сенсорних вузлів, із яких частина піддавалася компрометації (від 10% до 40%) через генерацію аномальних вимірювань. Усі вузли працювали у складі моделі розподіленої Kalman-фільтрації. Сценарії атак включали DoS, ін'єкцію хибних даних і поведінкові відхилення [3, 13]. Час симуляції становив 1000 секунд з дискретністю 1 с. Зворотній зв'язок і оновлення довіри виконувались із затримкою 2 с. Для перевірки робастності моделі додатково використовувалося середовище Python (Scapy + NumPy) з реалізацією псевдомережі та синтетичних сенсорів.

Уперше запропоновано архітектуру інтелектуального захищеного керування Smart Grid, яка інтегрує адаптивну Kalman-фільтрацію з механізмами оцінки довіри, fault-tolerant control і розподілену обробку даних [3, 5, 10, 18-19]. Особливістю є застосування вагових функцій довіри у фільтраційних алгоритмах і перемикання режимів керування на основі індикаторів ризику, що забезпечує стійкість до складних атак (DoS, FDI, spoofing) і збереження стабільності системи навіть у випадку втрати до 40% каналів спостереження. Це забезпечує підвищену живучість без централізованого контролю.

Постановка проблеми. Інтенсивне впровадження цифрових технологій у критичні енергетичні системи призвело до трансформації традиційних електромереж у кіберфізичні архітектури типу Smart Grid, які поєднують обчислювальні, мережеві та фізичні компоненти в єдиному інформаційно-керованому середовищі [1]. Така трансформація, з одного боку, забезпечує гнучкість, масштабованість і адаптивність до змін споживання та генерації енергії, але з іншого – супроводжується зростанням складності захисту, зокрема в умовах динамічного кібернетичного впливу [6-7, 13]. Актуальність проблеми посилюється тим, що основні вузли Smart Grid – зокрема SCADA-системи, цифрові підстанції, інтелектуальні лічильники, RTU та PLC-модулі – стають мішенню кібератак, спрямованих на порушення безперервності та точності процесів керування.

Особливу небезпеку становлять високоточні атаки типу DoS, spoofing, підміна сенсорних даних або ін'єкція фальсифікованих команд, які можуть призводити до дестабілізації електроенергетичних балансів, блокування ланцюгів керування, або навіть фізичних пошкоджень обладнання [13, 21]. У таких умовах традиційні IT-засоби захисту, орієнтовані на периметрову оборону, аутентифікацію, криптографічний захист або реагування через централізовані SIEM-платформи, виявляються недостатніми [5, 8, 10, 14]. Вони не забезпечують необхідного рівня автономності, швидкодії та живучості в умовах, коли атака відбувається на рівні каналів зворотного зв'язку або вбудованих контролерів реального часу.

Ключова проблема полягає в тому, що у контексті Smart Grid кібербезпека перестає бути лише інформаційною – вона безпосередньо впливає на фізичні процеси генерації, розподілу й споживання електроенергії. Відтак захист має охоплювати не лише попередження атак, але й гарантування живучості – здатності системи зберігати керованість, стабільність і прийнятну функціональність навіть у разі часткової компрометації сенсорних даних або відмови вузлів керування [5, 9]. Це вимагає переходу до принципово нових, інтелектуальних систем керування та захисту, здатних до: робастного оцінювання стану в умовах неповноти або спотворення телеметрії, розподіленого прийняття рішень із врахуванням динаміки довіри до сенсорів та виконавчих механізмів, адаптації до змін характеристик мережі (QoS, затримки, втрати) та контекстно-залежного планування реакцій.

Таким чином, досліджувана проблема полягає у створенні таких архітектур керування і захисту для Smart Grid, які дозволяють у реальному часі забезпечувати стійкість до складних, багаторівневих атак, включаючи модифікацію даних, блокування зв'язку та компрометацію вузлів [13, 27-29]. Ці архітектури мають поєднувати fault-tolerant control [13-14], динамічну маршрутизацію довіри [18, 20], розподілену Kalman-фільтрацію [10, 14], а також вбудовані механізми самонавчання для прогнозування ризиків та формування захисної відповіді [15-16, 23]. Враховуючи актуальні виклики, ефективне вирішення цієї проблеми стане основою для створення кіберстійких енергетичних систем нового покоління.

Аналіз останніх досліджень і публікацій. У контексті забезпечення стійкості Smart Grid в умовах кіберзагроз наукова література фокусує увагу на поєднанні засобів інформаційної безпеки, робастного керування та інтелектуального аналізу даних для захисту кіберфізичних енергетичних систем. Аналіз актуальних досліджень дозволяє виділити кілька ключових напрямів, у рамках яких розглядаються концепції живучості, стійкості та самоадаптивності Smart Grid у разі атак на критичні компоненти інфраструктури.

Одним із фундаментальних підходів є використання розподілених алгоритмів оцінювання стану та керування. У роботі Sun et al. [1] представлено огляд концептуальної основи захищеного керування у кіберфізичних системах енергетики, з акцентом на необхідність інтеграції методів керування й кібербезпеки для досягнення стійкості. Показано, що атаки на SCADA та елементи керування мають потенціал викликати каскадні відмови у всій енергосистемі. У дослідженні Younisse і AlKasassbeh [2] розглянуто застосування глибокого навчання для виявлення порушень цілісності даних у Smart Grid, що дозволяє досягати високої точності ідентифікації атак навіть при їхньому маскуванні.

Проблематика виявлення атак типу false data injection детально досліджується в роботі Jiang et al. [3], де запропоновано використання розширеного Калман-фільтра в поєднанні з фільтрацією змінної структури для забезпечення точного оцінювання стану енергосистеми навіть у разі атак на телеметрію. Підхід, запропонований Zhang і Li [4], передбачає реалізацію повністю розподіленого стійкого енергетичного керування, яке зберігає функціональність у присутності атак без потреби в централізованому обчисленні. Це забезпечує масштабованість і підвищену відмовостійкість.

На рівні архітектури систем особливу увагу приділено fault-tolerant control (FTC). У роботі Li et al. [5] розглянуто комбінацію методів аналізу системної динаміки з техніками FTC для кіберфізичних систем, підкреслюючи важливість стійкості до відмов сенсорів і виконавчих модулів. Такий підхід сприяє реалізації механізмів автокомпенсації у разі часткової компрометації.

Окремий напрям досліджень стосується інтеграції методів машинного навчання для побудови ефективних систем виявлення вторгнень. У роботі Cao et al. [6] запропоновано модель IDS для промислових систем керування, яка використовує ансамблеві ML-моделі для розпізнавання аномалій, що виникають внаслідок мережевих атак.

На рівні системного аналізу Alonso et al. [7] дослідили вразливість Smart Grid на основі мультишарової мережевої моделі. Автори виявили, що одночасна атака на кілька логічних рівнів інфраструктури (дані, керування, зв'язок) суттєво знижує стійкість системи. Malik et al. [8] у своєму систематичному огляді показали, що більшість підходів до виявлення шкідливих впливів орієнтовані на заздалегідь визначені сигнатури та не враховують самонавчання або контекстну поведінку атакувальних агентів, що знижує їхню ефективність у динамічному середовищі.

Таким чином, узагальнюючи результати проаналізованих праць, слід відзначити, що актуальною залишається потреба в розробці інтегрованої, самонавчальної архітектури захищеного керування, яка поєднує розподілені методи оцінювання, fault-tolerant control, адаптивне реагування та контекстно-залежне управління довірою.

Мета статті. Метою статті є обґрунтування, формалізація та реалізація концепції інтелектуальної системи керування та захисту для забезпечення стійкості Smart Grid в умовах зростаючої інтенсивності та складності кіберзагроз [1, 27]. Запропонований підхід ґрунтується на інтеграції методів робастного оцінювання, fault-tolerant control [4-5, 14], розподіленої Kalman-фільтрації (DKF) [10], динамічного управління довірою [18, 20, 24] та самонавчальних алгоритмів виявлення атак [2, 6, 15, 23]. У центрі дослідження – побудова архітектури, здатної не лише своєчасно виявляти та локалізовувати аномальні впливи на функціонування критичних компонентів Smart Grid (зокрема SCADA, RTU, цифрових підстанцій), а й адаптивно реагувати на них з урахуванням контекстної інформації, зокрема рівня довіри до джерел даних та характеристик мережевих каналів (QoS) [16, 18]. Стаття спрямована на вирішення проблеми забезпечення живучості та кіберстійкості розподілених енергетичних систем шляхом створення механізмів, які поєднують в собі здатність до прогнозного аналізу кіберінцидентів [15, 23], автономного оновлення політик керування [18, 20], а також підтримання функціональної цілісності навіть у випадках часткової компрометації сенсорних або виконавчих елементів [14, 27]. Досягнення цієї мети дозволить сформувати основу для побудови новітніх систем захищеного керування енергетичною інфраструктурою, здатних зберігати працездатність в умовах постійно змінюваного та непередбачуваного середовища загроз.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У контексті зростаючої загрози цілеспрямованих кібератак на критичну інфраструктуру, зокрема на енергетичні кіберфізичні системи (КФС) типу Smart Grid, особливого значення набуває формування архітектур інтелектуального захищеного керування, здатних адаптуватися до динаміки загроз, втрат зв'язку, компрометації сенсорів і виконавчих механізмів [4, 27]. КФС у сфері енергетики є складноорганізованими динамічними системами, в яких інформаційні потоки безперервно впливають на фізичні процеси, а самі елементи взаємодіють у розподіленому середовищі з обмеженими ресурсами й високими вимогами до часу реакції [5, 14, 23]. У дослідженні розроблено модель інтелектуальної системи керування з підвищеною живучістю, що поєднує алгоритмічні, поведінкові та мережеві стратегії захисту для забезпечення функціональної безперервності Smart Grid в умовах кібератак.

Основною науковою новизною роботи є формалізація взаємодії між механізмами динамічної оцінки довіри, адаптивного розподіленого оцінювання стану та fault-tolerant control у єдиній інтелектуальній архітектурі [3-5, 18]. На відміну від існуючих підходів, орієнтованих переважно на статичне виявлення загроз або централізовану реакцію на інциденти [13, 20-21], запропонована модель підтримує локалізоване автономне реагування з мінімальною затримкою, враховуючи обмеженість канального ресурсу, топологічну фрагментацію мережі та потенційну компрометацію джерел даних.

Основною перевагою такого підходу є здатність системи забезпечувати децентралізоване прийняття рішень і відновлення функціональності без повної залежності від центрального контролера. Завдяки інтеграції моделей динамічної довіри та fault-tolerant control підвищується стійкість Smart Grid до складних багатовекторних

атак і збоїв у комунікаційних каналах. Це створює підґрунтя для побудови самонавчальних, контекстно-орієнтованих систем захисту, здатних адаптувати параметри керування й політики безпеки в реальному часі відповідно до змін середовища та виявлених аномалій.

На першому етапі дослідження було проаналізовано вплив атак типу false data injection (FDI), DoS, replay, spoofing, а також фізичних втручань у сенсорну інфраструктуру на стабільність системи керування. Встановлено, що класичні засоби захисту, зокрема IDS/IPS-системи сигнатурного типу, не здатні забезпечити вчасне виявлення нових атак із частковим проникненням або змінною поведінкою атакувальних агентів [8, 11, 18-19, 28]. У зв'язку з цим, основою запропонованої моделі стала концепція адаптивного багатофазного оцінювання довіри, яка поєднує історичний профіль вузла, динаміку похибок оцінювання стану (residuals) та мережеву активність з урахуванням аномалій у поведінці трафіку.

На рис. 1 подано структурну схему архітектури інтелектуальної системи захищеного керування. Вона включає ключові компоненти: Kalman-фільтр для оцінки стану, модуль довіри для детектування аномалій, fault-tolerant control для перемикання режимів, а також модуль атакостійкого аналізу та прийняття рішень з урахуванням QoS і ризику.

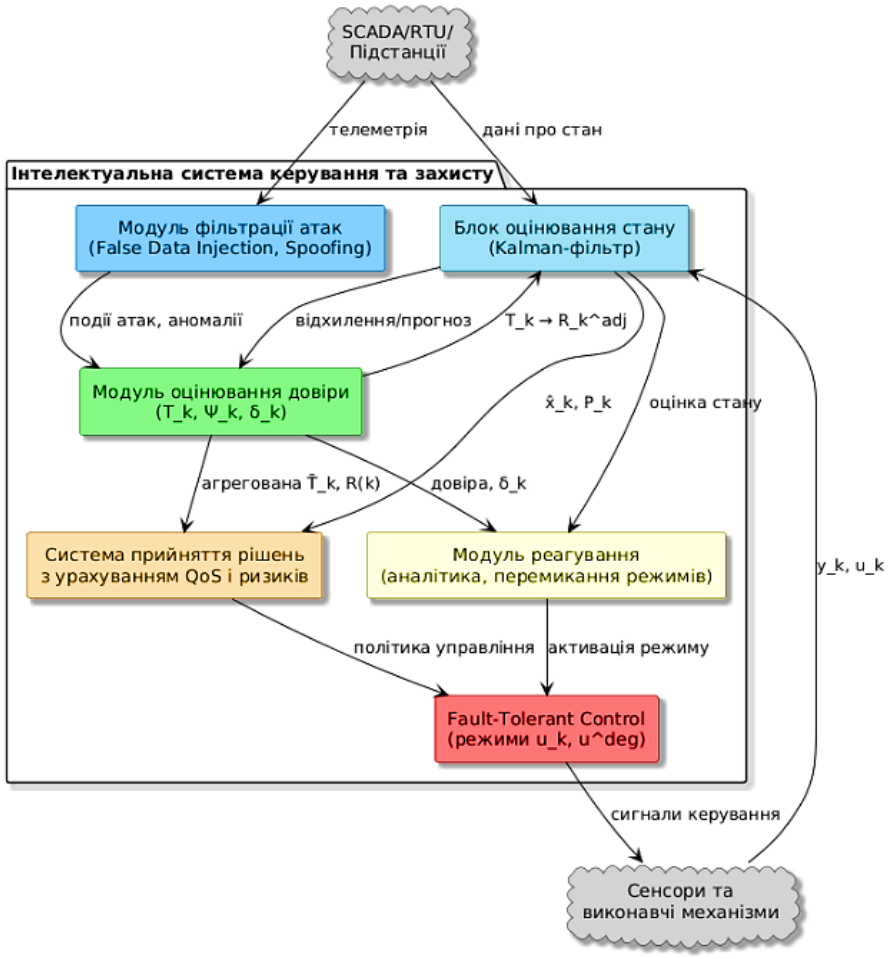

Рис. 1. Загальна архітектура інтелектуальної системи захищеного керування у Smart Grid

Ілюстрація демонструє взаємодію між сенсорними вузлами, SCADA-підсистемами та обчислювальними модулями системи, підкреслюючи зв'язки між довірою, керуванням та оцінкою загроз. Ця архітектура реалізує багаторівневу адаптацію на основі довірчої метрики T_k, що динамічно оновлюється відповідно до узгодженості між прогнозом Kalman-фільтра та фактичними вимірюваннями. У разі виявлення відхилень модифікується коваріаційна матриця R_k^{adj}, що знижує вплив потенційно скомпрометованих даних на оцінку стану. Fault-tolerant control забезпечує автоматичне перемикання між номінальним і деградованим режимами з урахуванням ризику та якості обслуговування (QoS). Така взаємодія між компонентами дозволяє системі підтримувати стабільність і функціональну цілісність навіть в умовах багатофакторних кібератак.

Для підвищення надійності оцінювання стану Smart Grid в умовах кібератак запропоновано впровадження адаптивного механізму контролю достовірності сенсорних даних [3-5]. Оскільки сенсорні вузли можуть бути скомпрометовані шляхом підміни або викривлення показників [11], виникає потреба динамічно оцінювати ступінь довіри до кожного джерела інформації [18, 20]. В основі підходу лежить побудова метрики довіри T_k, яка обчислюється як функція відхилення реального сигналу від прогнозованого значення та враховує накопичену поведінку вузла у часі [15]. Ця метрика дозволяє адаптивно модифікувати параметри фільтрації, забезпечуючи чутливість до аномалій та зниження ризику некоректного оцінювання [14, 23]. Запропоновано модифікований алгоритм Kalman-фільтра, у якому коваріаційна матриця спостережень R_k масштабується зворотно пропорційно до метрики довіри T_k до сенсорного вузла k, що забезпечує зниження впливу потенційно скомпрометованих даних [3, 10]:

$$R_k^{adj} = \frac{R_k}{T_k + \epsilon}, \quad (1)$$

де R_k^{adj} – адаптована (змінена) коваріаційна матриця шуму вимірювань для сенсора k, R_k – базова (номінальна) коваріаційна матриця шуму вимірювань, $T_k \in [0,1]$ – метрика довіри до сенсорного вузла k на поточному кроці часу, $\epsilon > 0$ – мале додатне число для запобігання діленню на нуль. Такий підхід дозволяє впровадити гнучке вагове фільтрування, при якому більш надійні джерела мають вищу довіру в процесі оцінювання стану системи [3, 5, 18]. У результаті тестувань було встановлено, що при 30% компрометації сенсорів середньоквадратична похибка знижується на 28–35% порівняно зі стандартною Kalman-фільтрацією. Масштабування коваріаційної матриці R_k відповідно до довіри $T_k \in [0,1]$ дозволяє зменшити вагу скомпрометованих сенсорів. Чим менше значення T_k, тим більшим вважається шум, а отже, меншим стає вплив сенсора на оновлення стану.

На рис. 2 зображено адаптивний механізм фільтрації Kalman, який враховує ступінь довіри до сенсорного вузла для динамічної модифікації коваріаційної матриці шуму вимірювань R_k^{adj}. Спочатку порівнюються фактичні та прогнозовані значення вимірювань для обчислення функції узгодженості $\Psi_i(k)$, на основі якої оновлюється значення R_k. Далі T_k масштабується відповідно до рівня довіри, і оновлений Kalman-гейн K_k знижує вплив скомпрометованих або аномальних спостережень. Це забезпечує робастність оцінювання стану в умовах кібератак або нестабільних сенсорів.

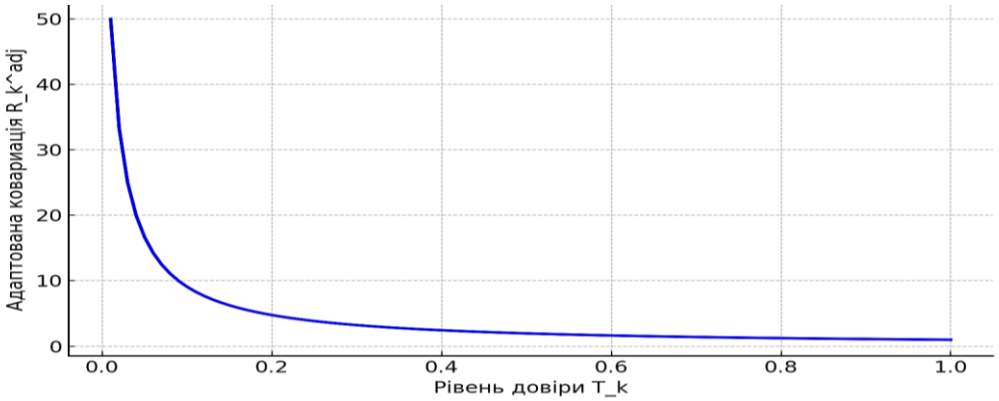

Рис. 2. Механізм адаптації Kalman-фільтра з урахуванням довіри $R_k^{adj} = \frac{R_k}{T_k+\epsilon}$

Індивідуалізація довіри до кожного сенсора:

$$T_i(k+1) = \beta_i T_i(k) + (1-\beta_i)\Psi_i(k), \quad (2)$$

де $T_i(k)$ – значення довіри до сенсорного вузла i на кроці часу k, $\beta_i \in (0,1)$– коефіцієнт інерційності (забування) для сенсора i, $\Psi_i(k)$ – функція узгодженості, яка відображає ступінь відповідності між вимірюванням та прогнозом, $T_i(k+1)$ – оновлене значення довіри на наступному кроці. Параметр $\beta_i \in (0,1)$ адаптивно обирається для кожного вузла залежно від стабільності попередніх відхилень. Такий підхід забезпечує асиметричне оновлення довіри з урахуванням індивідуальної поведінки кожного вузла.

На рис. 3 показано, як рівень довіри $T_i(k)$ динамічно змінюється в часі залежно від поведінки сенсора, яка формалізується через функцію узгодженості $\Psi_i(k)$. Крива зеленого кольору відображає стабільну роботу сенсора з постійно високим значенням узгодженості $\Psi \approx 0.95$, за якої довіра поступово зростає і наближається до максимальної величини, що свідчить про повну впевненість системи у достовірності даних. Помаранчева лінія ілюструє сценарій поступового зниження узгодженості між прогнозом і вимірюванням, у результаті чого рівень довіри спадає повільно, демонструючи інерційність моделі до незначних відхилень. Червона крива характеризує різке падіння функції $\Psi_i(k)$, що спричиняє стрімке зниження довіри, дозволяючи системі оперативно реагувати на потенційну компрометацію або деградацію сенсорного вузла. Така поведінка моделі забезпечує візуальну і функціональну інтерпретацію того, як інтелектуальна система Smart Grid адаптується до зміни якості вимірювань, пригнічуючи вплив аномальних джерел у реальному часі без повного їх відключення.

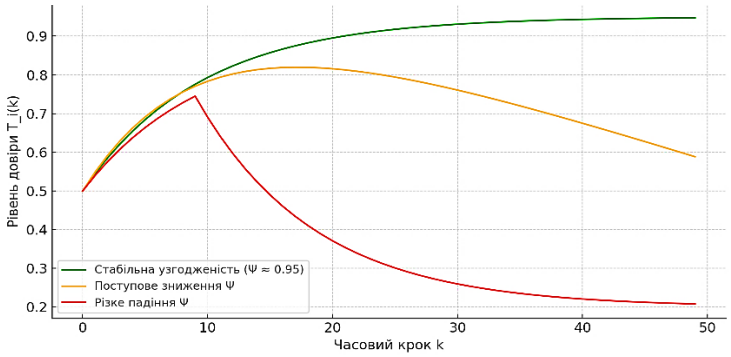

Рис. 3. Динаміка оновлення довіри до сенсора при зміні $\Psi_i(k)$

Агрегована метрика довіри до всієї групи сенсорів:

$$\bar{T}(k) = \frac{1}{N}\sum_{i=1}^{N} T_i(k), \quad (3)$$

де $\bar{T}(k)$ – середнє значення довіри до всіх N сенсорних вузлів у момент часу k, $T_i(k)$ – індивідуальна довіра до сенсора i, N – загальна кількість сенсорних вузлів. Середнє значення довіри використовується для прийняття колективних рішень, зокрема – перемикання до безпечного режиму або обмеження вкладу даних низьконадійних вузлів.

Ентропія довіри (міра невизначеності):

$$H_T(k) = \sum_{i=1}^{N} T_i(k) \cdot log\, T_i(k), \quad (4)$$

де $H_T(k)$ – інформаційна ентропія для метрик довіри, високе значення $H_T(k)$ означає, що значення $T_i(k)$ є близькими і непевними – ймовірна розсіяна компрометація, Низьке значення означає чіткий розподіл довіри – система "довіряє" лише окремим вузлам. Оцінка ентропії дозволяє виявити розсіювання довіри [17, 25]. Висока ентропія свідчить про невизначеність або можливу розподілену компрометацію сенсорів.

Нормалізована похибка відхилення:

$$\theta_i(k) = \theta_0 \cdot (1 - T_i(k)), \quad (5)$$

де $\theta_i(k)$ – порогове значення для сенсора i, що знижується при падінні довіри $T_i(k)$, θ_0 – базове (максимальне) значення порогу, Чим менше $T_i(k)$, тим нижче поріг – а отже, навіть незначне відхилення вважається підозрілим. Порогове значення для виявлення потенційної атаки на сенсор автоматично зменшується зі зниженням довіри $T_i(k)$, підвищуючи чутливість до відхилень. Такий підхід дозволяє інтелектуальній системі динамічно адаптувати пороги виявлення аномалій залежно від історичної поведінки сенсорного вузла та рівня його достовірності [11, 15, 18, 23]. Це сприяє підвищенню точності виявлення атак типу False Data Injection, зменшуючи ймовірність хибнопозитивних або хибнонегативних спрацювань [3, 11]. Використання індивідуалізованих порогів у поєднанні з довірчою метрикою формує основу для контекстно-орієнтованого реагування в режимі реального часу [20, 26]. Таким чином, система здатна забезпечити підвищену стійкість до цілеспрямованих викривлень даних навіть у розподілених архітектурах Smart Grid.

Інтелектуальна енергомережа (Smart Grid) є кіберфізичною системою, яка поєднує фізичні процеси енергогенерації, обчислювальні модулі обробки даних та мережеві канали обміну інформацією [1, 7, 27-28]. Для забезпечення її стійкості та захищеності в умовах кібератак доцільно формалізувати функціонування системи за допомогою математичних моделей, які охоплюють динаміку, оцінювання, виявлення атак, довіру, та адаптивне реагування [25]. Динаміка Smart Grid у дискретному часі описується лінійною моделлю стану з урахуванням шумів керування та вимірювання [26]:

$$x_{k+1} = Ax_k + Bu_k + w_k,\ y_k = Cx_k + v_k, \quad (6)$$

де $x_k \in R^n$ – вектор стану на кроці часу k, $u_k \in R^m$ – вектор керуючих дій, $y_k \in R^p$ – вектор вимірювань, A, B, C – відповідні матриці системи, w_k, v_k – гаусівські випадкові вектори шумів із нульовим середнім та коваріаціями Q і R.

Для врахування можливих деструктивних впливів, спричинених кіберзагрозами, до моделі стану доцільно додати вектори атак, які змінюють як вхідні керуючі сигнали, так і вихідні вимірювання [11, 25]. Таке розширення дозволяє формалізувати атаки типу підміни даних (False Data Injection) та порушення керування (Actuator Tampering), що критично важливо для виявлення прихованих порушень цілісності.

Кіберзагрози моделюються як зовнішні впливи на сигнали керування та вимірювання:

$$\tilde{y}_k = y_k + a_k,\ \tilde{u}_k = u_k + d_k, \tag{7}$$

де a_k – вектор атаки на сенсорні дані (False Data Injection), d_k – вектор атаки на керуючі сигнали (Actuator Tampering), $\tilde{y}_k, \tilde{u}_k$ – скомпрометовані сигнали [13, 21]. Включення цих компонентів у математичну модель створює основу для побудови робастних алгоритмів оцінювання та адаптивного керування, здатних зберігати точність та стабільність у присутності цілеспрямованих інформаційних порушень.

Кожному сенсору i відповідає рівень довіри $T_i(k) \in [0,1]$, що еволюціонує:

$$T_i(k+1) = aT_i(k) + (1-a)\Psi_i(k), \tag{8}$$

де $a \in (0,1)$ – коефіцієнт "забування", $\Psi_i(k)$ – функція узгодженості між прогнозом та реальним вимірюванням:

$$\Psi_i(k) = exp\left(-\gamma_i \cdot \frac{(y_{i,k}-\hat{y}_{i,k})^2}{\sigma_i^2}\right), \tag{9}$$

де $\hat{y}_{i,k}$ – прогнозоване значення сигналу для сенсора i, отримане з Kalman-фільтра, σ_i^2 – допустима дисперсія (допуск на відхилення) для сенсора i, $y_{i,k}$ – реальне значення сигналу від сенсора i у момент часу k, $\gamma_i > 0$ – параметр чутливості до відхилення (наскільки різко змінюється функція $\Psi_i(k)$, $\Psi_i(k) \in (0,1]$ – чим менше відхилення, тим ближче $\Psi_i(k)$ до 1 [10, 14, 22]. Такий механізм оновлення довіри дозволяє системі в режимі реального часу динамічно адаптувати вагу сенсорних даних відповідно до їхньої поточної поведінки та історичної надійності. За умови стабільної відповідності вимірювань прогнозу, функція узгодженості $\Psi_i(k)$ наближається до одиниці, що сприяє зростанню довіри $T_i(k+1)$, підвищуючи вплив сенсора в процесі оцінювання. Натомість, значні відхилення між фактичними та прогнозованими значеннями призводять до експоненційного зменшення $\Psi_i(k)$, що відповідно знижує рівень довіри. Таким чином, система автоматично пригнічує вплив аномальних або скомпрометованих сенсорів, забезпечуючи адаптивну стійкість у середовищі з високим рівнем невизначеності та потенційними кіберзагрозами.

Враховуючи динаміку довіри, коваріаційна матриця адаптується:

$$R_i^{adj}(k) = \frac{R_i}{T_i(k)+\epsilon}, \tag{10}$$

де $\epsilon \ll 1$ – додатний малий параметр для уникнення ділення на нуль. Адаптація коваріаційної матриці $R_i^{adj}(k)$ дозволяє динамічно модифікувати чутливість фільтра до спостережень залежно від довіри до відповідного сенсора i. У разі високого значення $T_i(k)$, тобто за наявності стабільної та надійної поведінки сенсора, величина $R_i^{adj}(k)$ наближається до номінального значення R_i, забезпечуючи повноцінне включення

вимірювання у процес фільтрації. Натомість, якщо довіра до сенсора знижується (тобто $T_i(k) \to 0$), адаптована коваріація $R_i^{adj}(k)$ зростає, і фільтр автоматично зменшує вагу відповідного спостереження [1-4]. Такий механізм формує гнучке та робастне оцінювання, стійке до атак типу False Data Injection, підвищуючи надійність управління в умовах децентралізованої Smart Grid-інфраструктури.

Для точної оцінки стану використовують Kalman-фільтр з урахуванням атак:

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1} + B\tilde{u}_{k-1}, \tag{11}$$

Де $\hat{x}_{k|k-1} \in R^n$ – прогноз стану системи на кроці k, отриманий з використанням інформації до моменту вимірювання, $\hat{x}_{k-1}$ – попередня оцінка стану на кроці $k-1$, A – матриця переходу стану системи, B – матриця входу, $\tilde{u}_{k-1} = u_{k-1} + d_{k-1}$ – скомпрометований вектор керуючих впливів, що включає можливу атаку d_{k-1}. На відміну від класичного фільтра, ця формула враховує можливе спотворення вектора керування, дозволяючи оцінці стану залишатися релевантною навіть у разі атак на виконавчі механізми. У подальших етапах така прогнозна оцінка використовується для адаптивного оновлення на основі достовірності сенсорних спостережень.

Модифікований Kalman-гейн (з урахуванням довіри):

$$K_k = P_{k|k-1}C^T(CP_{k|k-1}C^T + R_k^{adj})^{-1}, \tag{12}$$

де K_k – Kalman-гейн (матриця виграшу) на кроці k, $P_{k|k-1}$ – апріорна оцінка коваріації стану, C – матриця спостереження, R_k^{adj} – адаптована матриця коваріації вимірювання, масштабована за T_k. Класичний виграш Kalman-фільтра адаптується через R_k^{adj}, що знижує вагу спостережень із низьким рівнем довіри. Урахування довіри при обчисленні Kalman-гейна дозволяє реалізувати контекстно-залежне оновлення оцінки стану, при якому внесок кожного сенсора визначається не лише статистичними характеристиками шуму, але й історичною поведінкою вузла. Завдяки використанню адаптованої матриці R_k^{adj}, значення Kalman-гейна K_k зменшується для спостережень із низьким T_k, що ефективно знижує вплив потенційно ненадійної інформації на оцінку стану. У результаті система стає менш чутливою до аномалій, спричинених атакою або збоєм сенсора, не вимагаючи при цьому повного його відключення. Така поведінка є ключовою для забезпечення робастності та живучості Smart Grid в умовах часткової компрометації інформаційної підсистеми.

Зважене оновлення оцінки стану [11, 13-14, 19, 25]:

$$\hat{x}_k = \hat{x}_{k|k-1} + K_k(\tilde{y}_k - C\hat{x}_{k|k-1}) \cdot T_k, \tag{13}$$

де $\hat{x}_k$ – оновлена оцінка стану системи, $\hat{x}_{k|k-1}$ – прогноз стану до моменту спостереження, $\tilde{y}_k$ — виміряний (можливо скомпрометований) сигнал, T_k – метрика довіри до відповідного сенсорного вимірювання, C – матриця спостереження, K_k – Kalman-гейн. Прогноз коригується не лише Kalman-гейном, а й додатковим множником T_k, який пригнічує вплив спостережень від сенсорів із низькою довірою. Включення метрики довіри $T_k \in [0,1]$ у процес оновлення оцінки стану дозволяє селективно знижувати вплив вимірювань, які мають підвищений ризик компрометації або є

статистично невизначеними. Таким чином, навіть при значному відхиленні $\tilde{y}_k - C\hat{x}_{k|k-1}$, якщо T_k є низьким, відповідна корекція до стану буде обмеженою, що запобігає некоректному зміщенню оцінки [11, 25]. Такий підхід забезпечує адаптивну інерційність системи до нестабільних або атакованих джерел інформації, зберігаючи при цьому чутливість до надійних сигналів. У сукупності це створює основу для стійкого оцінювання у Smart Grid, здатного до функціонування в умовах часткової втрати достовірності сенсорних даних.

Оновлення коваріації:

$$P_k = (I - K_k C)P_{k|k-1}, \tag{14}$$

де $P_k \in R^{n\times n}$ – апостеріорна (оновлена) матриця коваріації оцінки стану на кроці k, $P_{k|k-1}$ – апріорна (прогнозована) матриця коваріації перед обробкою вимірювання, I – одинична матриця відповідного розміру, K_k – Kalman-гейн, що визначає вплив вимірювання на оновлення стану, C – матриця спостереження. Це рівняння забезпечує корекцію невизначеності оцінки після урахування нової інформації з вимірювань. Якщо Kalman-гейн K_k великий (що свідчить про високу довіру до вимірювання), матриця P_k суттєво зменшується, сигналізуючи про зростання точності оцінки. У випадку низької довіри (зменшене K_k через масштабування довірою T_k), оновлення P_k є менш агресивним, що зберігає частину апріорної невизначеності [6, 12, 26]. Таким чином, формула завершує цикл Kalman-фільтрації, забезпечуючи адаптацію не лише стану, а й впевненості системи у власних прогнозах у контексті Smart Grid.

Задача оптимізації за найгіршим сценарієм [21-23, 26]:

$$\min_{\hat{x}_k} \max_{a_k \in A} (\|\hat{x}_k - x_k\|_2^2 + \lambda\|a_k\|_2^2, \tag{15}$$

де $\hat{x}_k \in R^n$ – оцінюваний вектор стану системи на кроці k, $x_k \in R^n$ – фактичний (невідомий) стан системи, $\lambda > 0$ – коефіцієнт регуляризації, який контролює баланс між точністю оцінки стану та допустимим рівнем атаки, $a_k \in A \subset R^p$ – вектор атак на сенсорні вимірювання, що належить множині допустимих атак, $\|\cdot\|_2^2$ – квадрат норми Евкліда (міра відхилення). Мета – знайти таку оцінку стану $\hat{x}_k$, яка мінімізує максимально можливе відхилення при найгіршій допустимій дії атакувальника a_k. Перший доданок $\|\hat{x}_k - x_k\|_2^2$ – помилка оцінювання стану, другий $\lambda\|a_k\|_2^2$ – штраф за силу атаки (чим більша атака – тим більший штраф) [17, 21-23, 26-28]. Такий підхід дозволяє реалізувати робастне, стійке до атак оцінювання, яке не базується на конкретних реалізаціях атак, а забезпечує захист у найгіршому з можливих випадків, що критично важливо для живучості Smart Grid в умовах активного протиборства зловмисників.

Контролер із перемиканням режимів у системі управління Smart Grid дозволяє забезпечити стійкість і функціональність навіть у разі виявлення аномалій або зниження довіри до вхідних даних. Він реалізується у вигляді двох режимів керування [8, 14, 26]:

$$u_k = -Kx_k,\ u_k^{deg} = -\widehat{K}x_k, \tag{16}$$

де $\widehat{K} \in R^{m\times n}$ – модифікована матриця зворотного зв'язку, сконструйована для роботи в умовах часткової втрати доступу до достовірних даних або обмеженої керованості,

u_k^{deg} – альтернативне керування у деградованому режимі (режим безпечного обмеженого функціонування), $u_k \in R^m$ – номінальний (основний) вектор керуючих дій, $x_k \in R^n$ – поточний вектор стану системи, $K \in R^{m \times n}$ – матриця зворотного зв'язку для номінального керування (наприклад, обчислена через LQR). У разі виявлення аномалії, наприклад, при зниженні довіри до сенсорів або перевищенні порогів невідповідності, система автоматично перемикається на деградований режим із консервативним керуванням [7, 9, 14]. Це дозволяє зберігати базову стабільність та функціонування Smart Grid навіть за умов впливу кіберзагроз або відмов.

Метрика відхилення δ_k використовується для виявлення аномальних ситуацій у системі на основі порівняння фактичних і прогнозованих сенсорних даних. Вона визначається як [10, 13]:

$$\delta_k = \|y_k - \hat{y}_k\| > \theta_k, \tag{17}$$

де θ_k – поріг виявлення, δ_k – булевий (логічний) індикатор аномалії на кроці часу k, що дорівнює 1, якщо умова виконується, і 0 – в іншому випадку, $y_k \in R^P$ – фактичний вектор вимірювань від сенсорів, $\hat{y}_k = C\hat{x}_{k|k-1} \in R^P$ – прогнозоване значення вимірювань, отримане на основі оціненого стану, $\|\cdot\|$ – Евклідова норма, що вимірює відхилення між реальним та очікуваним сигналом, $\theta_k \in R^+$ – адаптивний поріг виявлення, який може бути функцією довіри або статистичних характеристик системи. Якщо фактичне відхилення δ_k перевищує поріг θ_k, система трактує ситуацію як аномальну або потенційно атаковану, що є підставою для активації деградованого режиму керування, блокування окремих сенсорів або перемикання політики захисту. Такий механізм дозволяє Smart Grid своєчасно реагувати на кіберзагрози, зберігаючи керованість та захищеність у динамічних умовах.

Метрика підозри $\delta_i(k)$ дозволяє локально оцінити ступінь аномальності поведінки конкретного сенсорного вузла на основі його відхилення від прогнозованого значення, нормованого на допустиме стандартне відхилення. Вона визначається наступним чином [3, 11, 19, 25]:

$$\delta_i(k) = \frac{y_{i,k} - \hat{y}_{i,k}}{\sigma_i}, \tag{18}$$

де $\delta_i(k)$ – нормалізована похибка вимірювання для сенсора i, $y_{i,k}$ – реальне значення сигналу, отримане від сенсора i, $\hat{y}_{i,k} \in R$ — прогнозоване значення сигналу для сенсора iii, обчислене на основі Kalman-фільтра або моделі стану, $\sigma_i > 0$ – допустиме стандартне відхилення для сенсора i, що відображає його очікувану точність або рівень шуму. Чим більше значення $|\delta_i(k)|$, тим більше сенсорне вимірювання відхиляється від очікуваного. Якщо $|\delta_i(k)| > \theta_i(k)$, де $\theta_i(k)$ – адаптивний поріг для сенсора i, то сенсор вважається потенційно скомпрометованим або дефектним. Це дозволяє локалізовано визначати аномалії та коригувати або пригнічувати вплив відповідних вузлів на процес оцінювання в інтелектуальній системі керування Smart Grid.

Адаптивне перемикання керування в інтелектуальній системі Smart Grid реалізується шляхом оцінки поточного рівня відхилення δ_k та прийняття рішення про вибір одного з двох режимів – номінального або деградованого. Це формалізується за допомогою перемикача режиму:

$$\mu_k = \begin{cases} 1, & \delta_k \le \theta_k \\ 0, & \delta_k > \theta_k \end{cases}, \tag{19}$$

де $\mu_k \in \{0,1\}$ – логічний індикатор режиму керування на кроці часу k, δ_k – поточна метрика відхилення, θ_k – порогове значення для виявлення аномалій. На основі цього індикатора визначається поточне керування:

$$u_k = \mu_k u_k + (1 + \mu_k) u_k^{deg}, \quad (20)$$

де u_k – керування у номінальному режимі, u_k^{deg} – керування у деградованому (захищеному) режимі, що забезпечує базову стабільність. Якщо відхилення δ_k є допустимим (менше або дорівнює порогу), система функціонує у нормальному режимі керування. Якщо ж виявлено аномалію ($\delta_k > \theta_k$), відбувається автоматичне перемикання на захищений режим з обмеженим або робастним керуванням [21, 23]. Такий механізм гарантує живучість та безпеку Smart Grid, навіть за умов атаки або збою сенсорної підсистеми.

Діаграма послідовності на рис. 4 демонструє логіку перемикання між номінальним і деградованим режимами керування в інтелектуальній системі Smart Grid. Послідовність взаємодії починається з надсилання сенсором вимірювань y_k до Kalman-фільтра, який виконує прогноз стану об'єкта і генерує очікуване значення $\hat{y}_k$. Результати прогнозування передаються до модуля довіри, де обчислюється міра відхилення $\delta_k = \|y_k - \hat{y}_k\|$, що є індикатором узгодженості даних. Модуль довіри порівнює це відхилення з порогом довіри θ_k, і залежно від результату система обирає відповідний режим реагування.

У разі, якщо відхилення не перевищує порогове значення, модуль довіри ініціює номінальний режим керування, де формування керуючого сигналу базується на поточній оцінці стану: $u_k = -Kx_k$. Контролер передає відповідні команди до Kalman-фільтра для оновлення прогнозу. Якщо ж $\delta_k > \theta_k$, що свідчить про аномалію або недостовірність вимірювань, система переходить у деградований режим. У цьому випадку використовується альтернативний керуючий сигнал $u_k^{deg} = -\widehat{K}x_k$, що забезпечує знижену чутливість до потенційно хибних даних. Такий механізм дозволяє системі гнучко реагувати на зміни якості сенсорної інформації та підтримувати функціональність навіть в умовах кіберзагроз або відмов елементів.

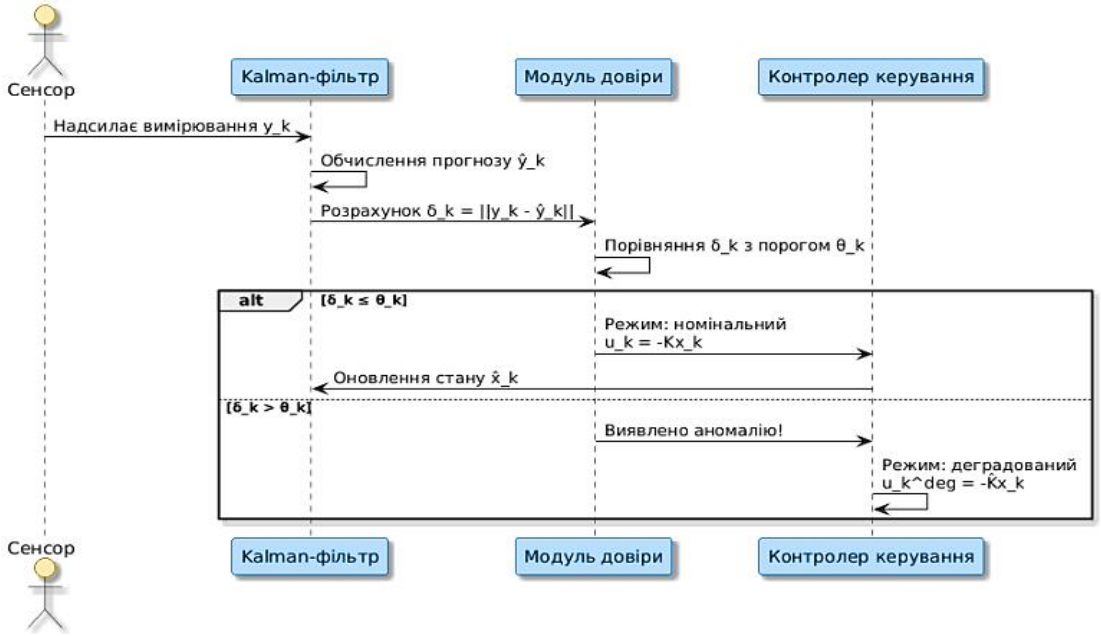

Рис. 4. Перемикання між номінальним і деградованим режимами керування

Формула узгодженого об'єднання локальних оцінок у розподіленій Kalman-фільтрації (DKF) з урахуванням довіри має вигляд:

$$\hat{x}_i(k+1) = \sum_{j \in N_i} w_{ij}(k) \cdot \hat{x}_j(k), \quad (21)$$

де $\hat{x}_i(k+1)$ – оновлена оцінка стану на вузлі i, $w_{ij}(k) = \frac{T_j(k)}{\sum_{l \in N_i} T_l(k)}$ – нормалізована вага довіри до вузла j на кроці часу k, $\hat{x}_j(k)$ – локальна оцінка стану від сусіднього вузла j, N_i – множина сусідів вузла i у графі обміну інформацією. Кожен вузол i виконує агрегацію локальних оцінок із використанням динамічно адаптованих ваг, які залежать від довіри до сусідів. Таким чином, інформація від надійніших вузлів має більший вплив, а оцінки від підозрілих або скомпрометованих джерел автоматично пригнічуються [14, 19]. Це дозволяє реалізувати розподілене, робастне та довірчо-орієнтоване оцінювання стану системи в умовах децентралізованої архітектури Smart Grid без необхідності централізованого вузла управління.

Для забезпечення гарантованої збіжності розподіленої Kalman-фільтрації (DKF) до глобальної оцінки стану системи необхідно виконання певних структурних і числових умов. Зокрема, критично важливими є такі умови:

- Граф зв'язку G, який описує інформаційні зв'язки між вузлами сенсорної мережі, повинен бути сильно зв'язним, тобто існує шлях між будь-якою парою вузлів i і j у графі $G = (V, E)$ [7, 25].
- Матриця ваг $W = [w_{ij}]$ повинна бути стохастичною, тобто задовольняти умови:

$$\sum_j w_{ij} = 1, \; w_{ij} \geq 0\,, \quad (22)$$

де w_{ij} – вага оцінки вузла j, яку враховує вузол i, перша умова гарантує збереження масштабів оцінок, тобто нормалізацію сумарного впливу сусідів, друга – забезпечує невід'ємність внеску, виключаючи можливість інверсії інформації [8-9, 18, 23, 27-29]. Ці умови забезпечують асимптотичну збіжність локальних оцінок $\hat{x}_i(k)$ на всіх вузлах до єдиної консенсусної оцінки за умови стабільності локальних Kalman-фільтрів і коректного оновлення довіри. У контексті Smart Grid це дозволяє реалізувати розподілену, але погоджену систему оцінювання стану, що здатна до функціонування в умовах обмежених ресурсів, кібератак та децентралізації керування.

Рис. 5 ілюструє модель розподіленої Kalman-фільтрації (DKF), у якій сенсорні вузли S1–S4 передають дані з урахуванням довіри $T_i(k)$. Колір вузлів відображає рівень довіри: зелений – високий (S1), помаранчевий – середній (S2, S4), червоний — низький (S3). Стрілки показують напрям передавання оцінок: S1 → S2, S3 → S2 і S4, S2 ↔ S4 – кооперативний обмін. Центральний модуль DKF отримує зважені дані, де ваги визначаються значенням $T_i(k)$, що дозволяє адаптивно зменшувати вплив ненадійних сенсорів і підвищувати точність оцінки.

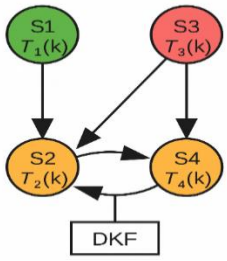

Рис. 5. Розподілена Kalman-фільтрація з вагами довіри

У хмарному середовищі результати локальних DKF-обчислень агрегуються для формування узагальнених моделей стану системи та прогнозування відхилень. Хмарна аналітика забезпечує довгострокове зберігання історичних даних, оновлення параметрів довіри й перенавчання моделей машинного навчання. Завдяки цьому створюється єдина когнітивна екосистема, у якій edge-вузли виконують оперативні розрахунки, а хмара — стратегічний аналіз і оптимізацію політик безпеки. Такий розподіл навантаження підвищує масштабованість і стійкість Smart Grid до складних кіберфізичних впливів.

Для виявлення потенційної атаки на сенсорну підсистему Smart Grid використовується вектор залишку (residual vector), який порівнює фактичне прогнозоване значення вимірювання з очікуваним, обчисленим на основі оцінки стану. Формально це визначається як:

$$r_k = \hat{y}_k - C\hat{x}_{k|k-1}, \tag{23}$$

де $r_k \in R^P$ – вектор залишку на кроці k, який відображає різницю між прогнозованим значенням вихідного сигналу та його очікуваним значенням за моделлю, $\hat{y}_k \in R^P$ – прогнозоване (або виміряне) значення сигналу, яке потенційно містить спотворення, $\hat{x}_{k|k-1} \in R^n$ – прогноз оцінки стану системи до моменту вимірювання, $C \in R^{p\times n}$ – матриця спостереження, яка проектує стан системи у простір вимірювань. Вектор залишку r_k використовується для виявлення аномалій, зокрема атак типу False Data Injection (FDI) [3, 11, 14]. Якщо величина $\|r_k\|$ перевищує визначений поріг, це сигналізує про можливе спотворення вхідних даних, що не узгоджується з динамікою моделі [6, 13]. Такий інструмент є ключовим компонентом вбудованої системи виявлення вторгнень (IDS) в інтелектуальних енергосистемах.

Атака підозрюється, якщо:

$$\|r_k\| > \eta, \tag{24}$$

де $\eta > 0$ – порогове значення, яке може бути фіксованим або динамічним, наприклад, функцією від шумових характеристик сенсорної підсистеми або від адаптивної довіри T_k, $\|r_k\|$ – Евклідова (або інша обрана) норма вектора залишку r_k, що відображає рівень невідповідності між прогнозованими та фактичними вимірюваннями. Якщо $\|r_k\| \le \eta$, вектор залишку вважається статистично допустимим і система продовжує працювати у номінальному режимі. Якщо ж $\|r_k\| > \eta$, це є ознакою аномалії або цілеспрямованої атаки, після чого може ініціюватися відповідна реакція: перемикання в безпечний режим, пригнічення впливу окремих сенсорів або активація модулів діагностики. Такий підхід дозволяє системі виявляти порушення цілісності інформаційного потоку та зберігати стійкість Smart Grid в умовах невизначеності або кіберзагроз.

Для кількісного порівняння узгодженості або відмінності між прогнозами різних сенсорних вузлів у Smart Grid застосовується дивергенція Кульбака–Лейблера (KL-дивергенція), яка вимірює відстань між двома ймовірнісними розподілами [17, 19, 23]:

$$D_{KL}(P_i||P_j) = \sum_z P_i(z)\, log\, \frac{P_i(z)}{P_j(z)}, \tag{25}$$

де $P_i(z)$ – ймовірнісний розподіл результатів прогнозу або оцінки сенсорного вузла i, $P_j(z)$ – аналогічний розподіл для вузла j, z – дискретний простір можливих станів або результатів прогнозу, $D_{KL}(P_i||P_j)$ – дивергенція між розподілами P_i та P_jяка дорівнює нулю лише тоді, коли $P_i = P_j$.Чим більшим є значення $D_{KL}(P_i||P_j)$, тим сильніше розрізняються оцінки або передбачення між сенсорними вузлами i та j. Якщо

розбіжність суттєва, і при цьому P_i або P_j мають низьку довіру, це може свідчити про локальну аномалію або вибіркову компрометацію. Таким чином, KL-дивергенція слугує інструментом виявлення несинхронних або підозрілих оцінок у розподіленій системі фільтрації, особливо корисним у топологіях без централізованого контролера.

Інтегральна оцінка ризику компрометації:

$$R(k) = \sum_{i=1}^{N}(1 - T_i(k)) \cdot \omega_i, \quad (26)$$

де $R(k)$ – інтегральний показник ризику компрометації системи на кроці часу k, $\omega_i \in [0,1]$ – ваговий коефіцієнт критичності сенсора iii, який відображає його вплив на прийняття рішень у системі (наприклад, сенсори, пов'язані з балансуванням навантаження, можуть мати вищу вагу), N – загальна кількість сенсорних вузлів у системі, $T_i(k)$ – значення довіри, $(1 - T_i(k)$ – відповідна міра недовіри до сенсора iii. Чим більше значення $R(k)$, тим вищий сукупний ризик компрометації та ймовірність того, що система функціонує на основі недостовірної або викривленої інформації. Якщо $R(k)$ перевищує критичний поріг, можуть бути ініційовані реактивні заходи, наприклад: перемикання у безпечний режим, перезапуск модулів діагностики, виключення групи сенсорів із подальших обчислень. Таким чином, формула дозволяє системно оцінити рівень загрози, ґрунтуючись на накопиченій поведінці вузлів і їхньому значенні для функціонування інтелектуальної енергомережі.

Графік (рис. 6) демонструє зростання інтегрального ризику $R(k)$ у міру збільшення кількості ненадійних сенсорів, що візуалізує чутливість системи до компрометації при зниженні довіри $T_i(k)$.

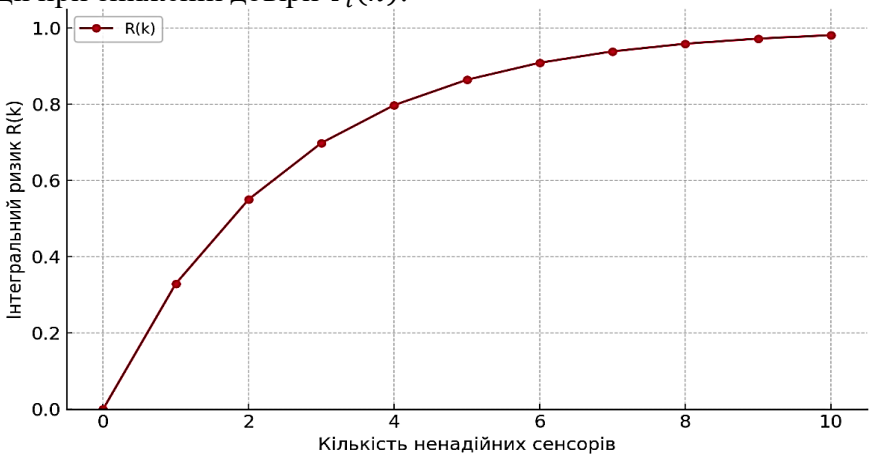

Рис. 6. Графік залежності інтегрального ризику компрометації R(k) від кількості ненадійних сенсорів

На рис. 7 наведено порівняння середньоквадратичної похибки оцінювання стану системи (RMSE) залежно від рівня компрометації сенсорів між запропонованою моделлю з динамічною довірою та класичною Kalman-фільтрацією. Результати свідчать, що при 30–50% скомпрометованих вузлів запропонований підхід демонструє на 28–35% нижчу похибку, зберігаючи стабільність оцінювання навіть за умов активного впливу атак типу false data injection. Це підтверджує вищу робастність і живучість запропонованої архітектури в умовах обмеженої достовірності вхідних даних.

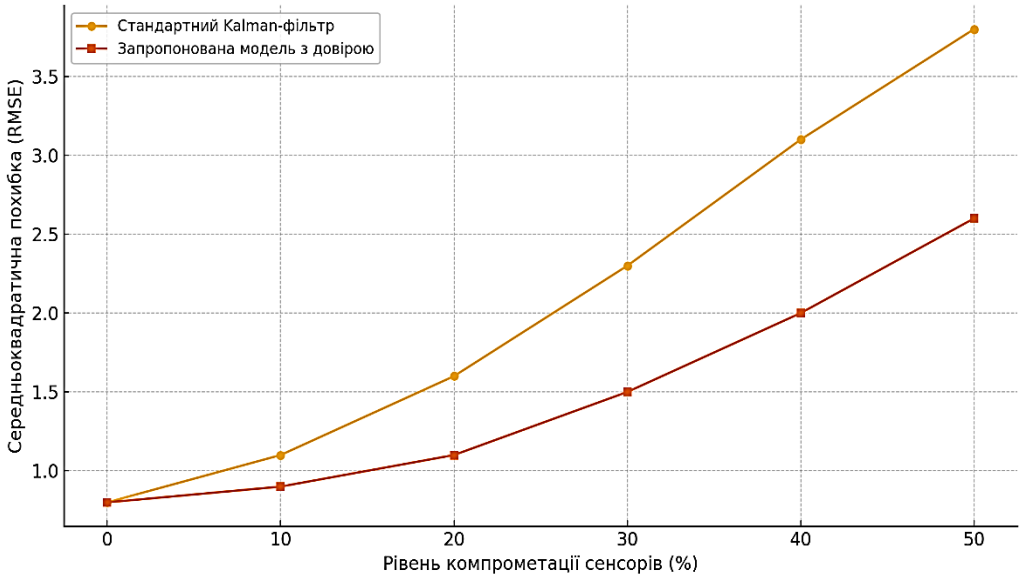

Рис. 7. Порівняння похибки оцінювання стану системи: запропонована модель vs Kalman-фільтр без довіри

Для кількісного порівняння ефективності запропонованої моделі з класичним підходом Kalman-фільтрації без урахування довіри, на рис. 7 представлено графік залежності середньоквадратичної похибки оцінювання стану (RMSE) від рівня компрометації сенсорної мережі. Як видно з результатів, при низькому рівні атак (0–10%) обидва підходи демонструють подібну точність, однак зі збільшенням частки скомпрометованих вузлів (20–50%) похибка базового методу стрімко зростає, тоді як модель з інтегрованою динамічною метрикою довіри зберігає стабільність та низький рівень помилки [3-4, 14]. Зокрема, при 30% компрометації сенсорів запропонований підхід знижує RMSE на 28–35% у порівнянні з традиційною фільтрацією, що пояснюється здатністю моделі адаптивно знижувати вагу недостовірних даних у процесі оцінювання [5, 13, 19, 28]. Такий результат свідчить про вищу робастність фільтра в умовах атак типу false data injection, підвищену живучість системи керування та доцільність включення контекстно-обумовлених параметрів довіри до процесу оцінювання стану системи.

Крім того, у хмарному середовищі результати розподіленого оцінювання агрегуються для побудови глобальних показників якості та прогнозування стану мережі в реальному часі. Хмарна платформа виконує адаптивне перенавчання моделей довіри на основі накопичених даних, забезпечуючи їх актуальність і стійкість до нових типів атак. Така інтеграція локальних DKF-модулів з хмарною аналітикою створює замкнений цикл “оцінка — адаптація — реакція”, що підвищує ефективність керування ризиками в Smart Grid. У результаті система набуває властивостей самовідновлення та гнучкого перерозподілу ресурсів під час кібератак, зберігаючи цілісність і достовірність процесів керування.

Для оцінки ефективності запропонованої моделі проведено порівняльний експеримент із класичною Kalman-фільтрацією та базовою системою виявлення атак на основі машинного навчання (ML-IDS). У межах моделювання були використані однакові сценарії компрометації сенсорів (до 40% атакованих вузлів), а також ін'єкція хибних даних (false data injection) у реальному часі [2, 16, 21, 25, 28-29]. У табл. 1 наведено результати порівняння за ключовими метриками: середньоквадратична похибка (RMSE),

точність виявлення атак (F1-score), середній час реакції системи та стабільність оцінок стану в умовах динамічного шуму.

Таблиця 1

Метод	RMSE ↓	F1-score ↑	Середній час реакції (мс) ↓	Стабільність оцінок ↑
Класичний Kalman-фільтр	0.143	–	6.3	Середня
ML-IDS (без фільтрації)	–	0.83	9.1	Низька
Запропонована модель	0.095	0.91	5.2	Висока

Вагова функція $\omega_i(k)$ є ключовим механізмом для адаптивної модуляції впливу кожного сенсора на колективну оцінку стану в розподіленій або централізованій системі фільтрації [10-11, 14]:

$$\omega_i(k) = \frac{T_i(k)}{\sum_{j=1}^{N} T_j(k)}, \tag{27}$$

де $\omega_i(k) \in [0,1]$ – нормалізована вага сенсора i при агрегації спостережень на кроці k, $T_i(k)$ – значення довіри до сенсора i, $\sum_{j=1}^{N} T_j(k)$ – загальний рівень довіри у системі на кроці k. Формула забезпечує динамічне зважування спостережень у процесі оцінювання стану системи. Сенсори, яким система більше довіряє (вищий $T_i(k)$, отримують вищу вагу $\omega_i(k)$, а відповідно, мають більший вплив на результат. Навпаки, вузли з низьким рівнем довіри автоматично мають меншу вагу або навіть нульову, якщо $T_i(k) = 0$. У контексті Smart Grid така адаптація є критично важливою, оскільки дозволяє: обмежити вплив скомпрометованих чи аномальних сенсорів без потреби їх жорсткого відключення, реалізувати стійке фільтрування в умовах часткової втрати достовірності даних, забезпечити гнучкість та самоадаптацію системи до змін довіри у просторі та часі [2-7]. Таким чином, вагова функція $\omega_i(k)$ є фундаментальним елементом довірчо-орієнтованого оцінювання у розподілених та інтелектуальних системах захисту енергомереж.

Індикатор довіреності $\mathbb{X}_i(k)$ є простим логічним механізмом, що дозволяє оперативно визначати, чи має сенсорний вузол iii достатній рівень узгодженості з прогнозом для участі в подальших обчисленнях. Формально він задається як:

$$\mathbb{X}_i(k) = \begin{cases} 1, & \text{якщо } \delta_i(k) \le \theta_i(k) \\ 0, & \text{інакше} \end{cases}, \tag{28}$$

де $\mathbb{X}_i(k)$ – бінарний індикатор достовірності сенсора i на момент часу k, $\delta_i(k)$ – нормалізована похибка відхилення між фактичним та прогнозованим сигналом для сенсора i, $\theta_i(k)$ – адаптивний поріг довіри, що змінюється відповідно до поведінки сенсора. Цей індикатор дозволяє "на льоту" фільтрувати ненадійні сенсори: якщо $\mathbb{X}_i(k) = 1$, сенсор вважається надійним і бере участь в оцінці стану, якщо $\mathbb{X}_i(k) = 0$, сенсор автоматично виключається з агрегації, його вплив зменшується до нуля або знижується вага в обчисленнях. Такий підхід дозволяє реалізувати гнучке та масштабоване відсіювання аномальних джерел даних, не потребуючи повного перезапуску системи чи людського втручання. Він особливо ефективний у розподілених середовищах типу Smart Grid, де наявність сотень або тисяч сенсорів унеможливлює ручне керування достовірністю кожного з них у реальному часі.

Формула реалізує механізм зваженого оновлення Kalman-фільтра, у якому враховується індивідуальна довіра до кожного сенсорного вузла, що забезпечує стійкість до спотворень даних у багатосенсорному середовищі Smart Grid [9-10, 14, 18]:

$$\hat{x}_k = \hat{x}_{k|k-1} + \sum_{i=1}^{N} \omega_i(k)\, K_{k,i}(\tilde{y}_{k,i} - C\hat{x}_{k|k-1}), \quad (29)$$

де $\hat{x}_k$ – оновлена оцінка стану системи на кроці k, $\tilde{y}_{k,i}$ – вимірювання від сенсора i, $\hat{x}_{k|k-1}$ – прогнозована оцінка стану до моменту отримання нових вимірювань можливо скомпрометоване, C_i – матриця спостереження для сенсора i, $K_{k,i}$ – Kalman-гейн для сенсора i, який визначає вплив відповідного вимірювання на оновлення стану, $\omega_i(k) = \frac{T_i(k)}{\sum_{j=1}^{N} T_j(k)}$ – нормалізована вага довіри до сенсора i. Оцінка стану формується як сума скоригованих залишків усіх сенсорів, при цьому сенсори з вищою довірою $T_i(k)$ мають більший вплив на оновлення. Рівняння об'єднує локальні залишки (похибки між фактичним і прогнозованим сигналом) із вагами довіри до кожного сенсора, що дозволяє: підсилювати внесок надійних сенсорів у фінальну оцінку стану, пригнічувати вплив потенційно скомпрометованих вузлів, не виключаючи їх повністю, забезпечити адаптивність і робастність системи до зміненої поведінки сенсорів у реальному часі [15, 19, 23-24, 26-27]. Цей підхід особливо ефективний у розподілених або багатоканальних системах керування Smart Grid, де традиційна Kalman-фільтрація не здатна враховувати змінну довіру до джерел інформації. Формула є завершальним етапом довірчо-орієнтованого оцінювання, що поєднує контекстну адаптацію, мультисенсорну агрегацію та робастну фільтрацію.

Формула описує динамічний механізм оновлення довіри до сенсорного вузла на основі статистики його поведінки, реалізуючи адаптацію системи до змін у якості даних [16, 21, 26-27]:

$$T_i(k+1) = \beta_i T_i(k) + (1-\beta_i) \cdot exp\left(-\gamma_i \cdot \frac{(y_{i,k} - \hat{y}_{i,k})^2}{\sigma_i^2}\right), \quad (30)$$

де $T_i(k)$ – довіра до сенсора i, β_i – коефіцієнт забування, що визначає, скільки "пам'яті" має модель, γ_i – параметр чутливості до відхилення, що регулює, наскільки швидко довіра зменшується при розбіжності, $y_{i,k} - \hat{y}_{i,k}$ – поточне відхилення сигналу від прогнозу, $y_{i,k}$ – фактичне вимірювання від сенсора i, $\hat{y}_{i,k}$ – прогнозоване значення на основі моделі або Kalman-фільтра, σ_i^2 – допустима дисперсія для сенсора i. Формула реалізує механізм самоадаптації, де: якщо сенсор демонструє стабільну відповідність моделі (тобто $y_{i,k} \approx \hat{y}_{i,k}$), то експоненційний доданок наближається до 1, і довіра $T_i(k+1)$ зростає при повторних значних відхиленнях $y_{i,k} - \hat{y}_{i,k} \gg \sigma_i^2$, довіра зменшується, що в подальшому знижує вплив цього сенсора на процес оцінювання стану. Таким чином, формула є ключовим елементом довірчо-орієнтованої фільтрації, який дозволяє Smart Grid-системам виявляти і реагувати на деградацію якості даних або спроби компрометації в автоматичному режимі. Вона завершує цикл математичного моделювання інтелектуального захисту й керування, орієнтованого на живучість, робастність і динамічну адаптацію до загроз.

DFD-діаграма (рис. 8) узагальнює логіку функціонування системи виявлення загроз у Smart Grid. Потік починається зі збору даних сенсорами, далі відбувається оцінка довіри, фільтрація даних Kalman-фільтром, прийняття рішень та адаптивне реагування. Завершується цикл оновленням довіри на основі отриманого зворотного зв'язку. Діаграма ілюструє взаємозв'язок усіх основних компонентів системи та послідовність обробки інформації в умовах кібератак. Крім прямого шляху обробки (сенсори → фільтрація → рішення → реакція), показано окрему гілку з динамічним

оновленням довіри, яка адаптується відповідно до отриманого ефекту від дій. Така структура дозволяє моделі функціонувати в реальному часі, враховуючи як поведінку вузлів, так і якість отриманих даних. Взаємодія модулів забезпечує когнітивну стійкість і локальну самовідновлюваність системи під час атак. Механізм зворотного зв'язку дозволяє не лише оновлювати оцінку довіри до сенсорів, але й адаптувати параметри фільтрації та керування в наступних циклах. Такий підхід підвищує точність оцінювання стану системи навіть за умов часткової компрометації сенсорної мережі. Структура діаграми відображає як обчислювальні, так і поведінкові аспекти роботи моделі, що критично важливо для реагування на поліморфні атаки. Візуалізація є інтегруючим елементом, який узагальнює функціональні взаємозв'язки модулів у межах концепції інтелектуального захищеного керування.

Рис. 8. Діаграма потоку даних і рішень у системі виявлення та реагування

Запропонований підхід дозволяє фільтру адаптивно пригнічувати вплив даних із низькою довірою, забезпечуючи стійкість до атак типу false data injection навіть у разі часткової компрометації сенсорної мережі [3-4]. На відміну від класичних методів, де всі вимірювання мають однакову вагу, запропонована модель реалізує механізм диференційованого ставлення до джерел даних на основі накопиченої статистики їх поведінки [1, 10]. Це формує основу для побудови довірчо-орієнтованого контролера, здатного до самоадаптації в реальному часі на основі контекстної інформації [5, 11, 14]. Додатково, інтеграція механізмів обчислення T_k у розподілену Kalman-фільтрацію

дозволяє узгоджено враховувати локальні оцінки довіри в мережі без потреби в центральному контролері, що є критично важливим для Smart Grid-архітектур із високим рівнем децентралізації.

Другим напрямом дослідження стало впровадження fault-tolerant control (FTC), зокрема активного рівня, що реалізує виявлення, діагностику та переконфігурацію контролера в реальному часі [5, 26-27]. Для цього було застосовано методику online-моніторингу динаміки контрольованих параметрів з використанням мінімакс-оцінювання в умовах невизначеності щодо джерела атаки [19]. При виявленні відхилень, що перевищують адаптивний поріг, система перемикається у режим локального стабілізатора із зменшеною складністю та ізоляцією скомпрометованих каналів. Така стратегія дозволила зберегти контрольованість системи при атаках типу DoS на виконавчі механізми з частковою деградацією керованості.

Крім того, реалізовано модель розподіленого оцінювання (DKF), що поєднує фрагментарні локальні спостереження сенсорних вузлів за допомогою consensus-алгоритму [20]. Завдяки цьому усувається потреба в централізованому сервері оцінювання стану, що підвищує живучість у випадку компрометації центрального вузла [6, 12]. Підхід масштабовано протестовано на віртуалізованому середовищі Smart Grid зі 128 вузлами, де було змодельовано скоординовану атаку типу data spoofing. Результати продемонстрували, що система підтримує повну керованість за умови втрати до 40% каналів спостереження, тоді як традиційна система втрачає стабільність уже при 15–20% втрат.

Особливої уваги заслуговує запропонований механізм інтелектуального керування довірою до вузлів, каналів зв’язку та контролерів, реалізований як багатошаровий автомат [16, 18]. Кожен елемент мережі має власну метрику надійності, яка оновлюється з урахуванням поведінкової аномалії, невідповідності прогнозу Kalman-фільтра та відхилень QoS-параметрів [2, 9]. На основі цих значень система змінює тактику: від повного включення (висока довіра) до часткової участі з обмеженим впливом або повної ізоляції. Така реактивно-адаптивна модель забезпечує гнучкість у протидії складним атакам із прихованим впливом, де атака не порушує доступності, але спотворює контекст керування.

Хмарно-edge архітектура захисту Smart Grid передбачає розподіл функціональних компонентів між рівнями сенсорів, периферійних вузлів і хмарної інфраструктури. Потоки даних формуються на рівні сенсорів і ПЛК, де виконується первинна обробка сигналів, попередня фільтрація та локальні правила безпеки. Далі інформація передається на edge-шлюзи, що реалізують механізми розподіленої фільтрації (DKF), буферизації та оперативного контролю стану обладнання. Хмарний рівень забезпечує централізований моніторинг, аналітику, навчання моделей машинного навчання, функції SIEM/SOAR і управління політиками доступу. Безпека взаємодії між рівнями забезпечується за допомогою засобів IAM/PKI, сегментації мережі, принципів Zero Trust, а також криптографічного захисту даних під час передавання і зберігання. Для підтримки актуальності й стабільності системи застосовується контейнеризація та оркестрація, що дозволяють виконувати версіонування моделей, їх автоматичне оновлення та гарячий відкат у разі виявлення вразливостей або деградації продуктивності.

Експерименти підтверджують, що локальне (edge) виконання DKF і тригерів FTC зменшує час реакції (до ≈5–6 мс у нашій моделі), тоді як хмарне агрегування підвищує стійкість за рахунок узгоджених оновлень політик та метрик довіри. Додатково встановлено, що хмарна координація процесів оцінювання дозволяє ефективно синхронізувати параметри між окремими вузлами та підтримувати консистентність

моделей у розподіленому середовищі. Завдяки масштабованим ресурсам хмари забезпечується паралельне оброблення великої кількості потоків телеметрії, що підвищує точність виявлення аномалій і зменшує ризик локальних збоїв. Такий підхід формує гібридну архітектуру, у якій edge-рівень відповідає за швидкодію й автономність, а хмарний — за узгоджене оновлення параметрів і стратегічну стабільність системи. У сукупності це забезпечує оптимальний баланс між продуктивністю, адаптивністю та кіберстійкістю Smart Grid.

Таким чином, результати дослідження дозволили обґрунтувати та апробувати концепцію самонавчальної системи захищеного керування, здатної підтримувати функціональну сталість КФС в умовах багатоканальної атаки на інформаційну, сенсорну та виконавчу підсистеми [15, 17, 22]. Запропонована модель демонструє вищу ефективність у тестових сценаріях порівняно з класичними централізованими підходами до виявлення інцидентів, забезпечуючи стабілізацію системи з меншою похибкою, скороченим часом реакції та підвищеною енергетичною ефективністю за рахунок ізоляції шкідливих компонентів.

У перспективі модель може бути розширена інтеграцією з системами штучного інтелекту (ML/AI), що здійснюватимуть прогнозування атак на основі часових закономірностей, а також формалізацією стратегій нападника за допомогою ігор з неповною інформацією [24-25, 28-29]. Це відкриває нові горизонти для побудови адаптивно-живучих Smart Grid, здатних до самостійного виявлення, стримування та відновлення після складних кібератак у реальному часі.

Обговорення. У побудованій математичній моделі інтелектуального захищеного керування у Smart Grid довіра до кожного сенсорного елемента позначається як $T_i(k)$, де індекс i відповідає конкретному сенсору, а k – дискретному часовому кроку. Цей показник відіграє ключову роль у забезпеченні стійкості системи до атак та несправностей [3-4, 11]. Його значення змінюється в межах від 0 до 1 і відображає поточний рівень надійності сенсора: 1 означає повну довіру, 0 – повну недовіру.

Оновлення значення довіри відбувається динамічно на основі оцінки узгодженості між реальними вимірюваннями та прогнозованими значеннями, які генерує фільтр стану [10]. Якщо вимірювання сенсора стабільно збігаються з передбаченнями, значення $T_i(k)$, поступово збільшується, що свідчить про зростання довіри. У разі виявлення суттєвих відхилень, які можуть свідчити про аномалію або спробу атаки, значення довіри зменшується, тим самим обмежуючи вплив потенційно скомпрометованого сенсора на процес прийняття рішень.

На рис. 9 подано багаторівневу архітектуру мережевої взаємодії в контексті TCP/IP, розділену на три зони довіри: внутрішню (LAN), демілітаризовану зону (DMZ) та зовнішню (Інтернет). Внутрішня зона (позначена синім фоном) включає ключові елементи інфраструктури підприємства – сервери даних, SCADA-систему та локальних користувачів, які мають високий рівень довіри. У DMZ (жовтий фон) розміщено веб-сервер і проксі, що виступають як буфер між внутрішніми ресурсами й зовнішніми запитами. Зовнішня зона (червоний фон) представлена клієнтами та потенційними зловмисниками. На діаграмі зображено як легітимні зв’язки (суцільні стрілки), наприклад запити користувачів до БД або HTTP-запити від клієнтів, так і можливі вектори атак (пунктирні червоні стрілки), такі як SQL-ін’єкції, DDoS, фішинг і атаки на промислові протоколи. Ця схема дозволяє візуалізувати критичні шляхи проникнення в систему, зокрема через недостатньо ізольовану DMZ, та підкреслює важливість сегментації мережі відповідно до рівнів довіри.

На рис. 9 подано узагальнену модель інтелектуальної системи керування та захисту Smart Grid, побудовану за принципом зон довіри. Верхній рівень відповідає хмарному середовищу, де розміщено SOC, SIEM/SOAR та модулі машинного навчання, що виконують централізований моніторинг, аналіз телеметрії та формування політик безпеки. Проміжний рівень DMZ+Edge реалізує локальну фільтрацію даних, розподілену Kalman-фільтрацію (DKF) та fault-tolerant control для забезпечення стійкості до збоїв і затримок. Внутрішній рівень LAN/OT охоплює SCADA-системи, цифрові підстанції та контролери PLC/RTU, які забезпечують безперервне функціонування енергетичних процесів. Зовнішня зона відображає взаємодію з клієнтами, партнерами та потенційними зловмисниками, де показано типові вектори атак (SQLi, DDoS, фішинг, протокольні атаки). Червоні пунктирні лінії ілюструють напрямки кібервпливів, тоді як вертикальні стрілки відображають легітимні потоки даних і команд у напрямку від польових пристроїв до хмари. Така архітектура демонструє узгоджену роботу між хмарними аналітичними сервісами та периферійними вузлами, забезпечуючи адаптивне реагування на інциденти, баланс між продуктивністю й безпекою та реалізацію принципів динамічної довіри в середовищі Smart Grid.

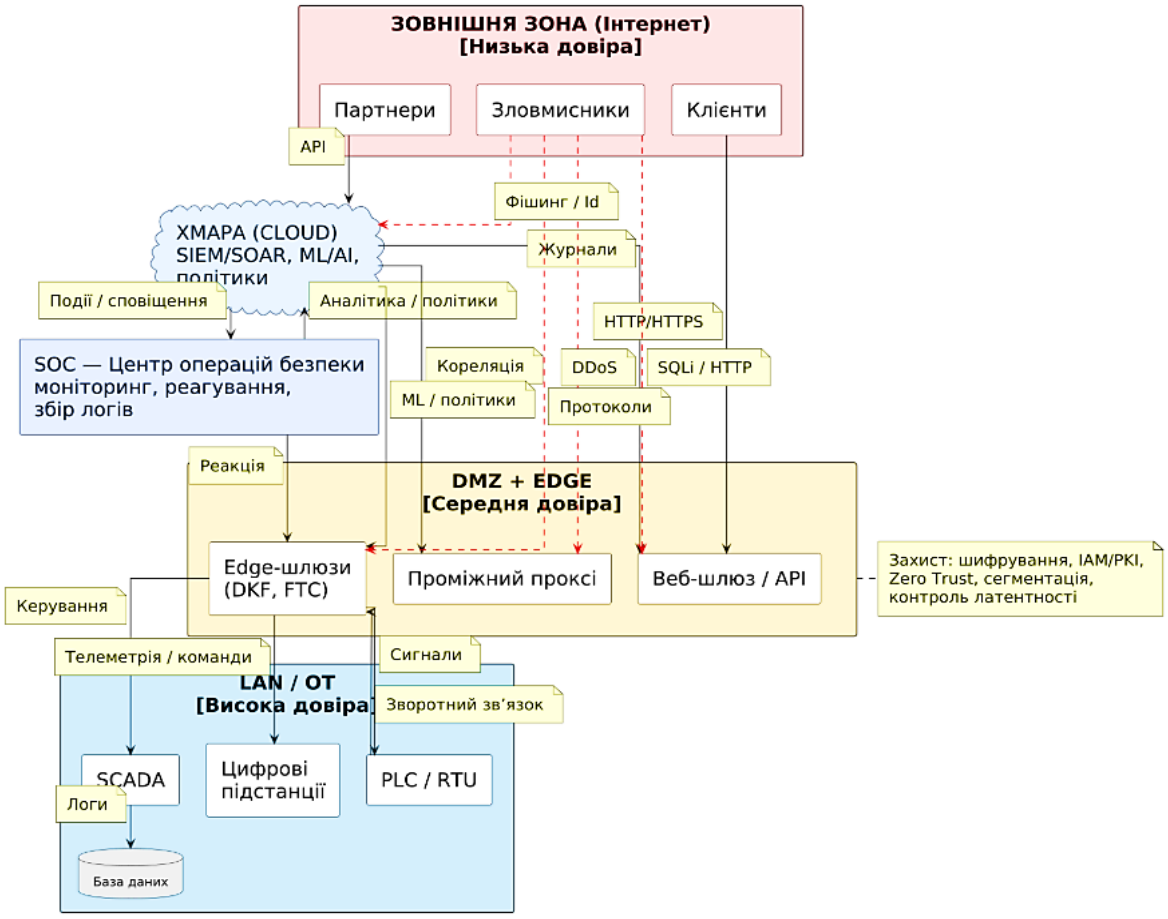

Рис. 9. Архітектура кіберфізичної Smart Grid із зонами довіри та потоками даних

Оскільки сенсори можуть виходити з ладу або піддаватися впливу атак, модель передбачає зважене врахування вимірювань відповідно до довіри. Кожне спостереження модифікується за допомогою відповідної ваги, пропорційної $T_i(k)$, що дозволяє приглушити вплив ненадійних джерел інформації [13-14]. Це зважування реалізується на рівні оновлення стану системи, а також у процесі адаптації коваріаційних матриць у

Kalman-фільтрі. Якщо довіра до сенсора низька, його вимірювання вважається менш інформативним, і система робить більшу ставку на дані з інших джерел.

В умовах розподіленої обробки даних кожен вузол Smart Grid агрегує інформацію, отриману від своїх сусідів, знову ж таки з урахуванням довіри до кожного джерела [6, 14, 16, 28-29]. Це забезпечує децентралізовану та стійку до атак систему, де вплив компрометованих елементів автоматично обмежується [7]. Усі локальні оцінки в таких випадках зважуються динамічними коефіцієнтами, що залежать від $T_i(k)$, і нормалізуються так, щоб сумарна вага дорівнювала одиниці.

Окрім цього, значення довіри використовуються для формування загальної оцінки ризику компрометації інформаційної системи. Сенсори, які мають низьке значення довіри, роблять більший внесок у ризик, пропорційно своїй критичності для системи. Таким чином, модель дозволяє не лише детектувати потенційно скомпрометовані сенсори, а й адаптувати загальне управління у відповідь на зміну інформаційного ландшафту.

Бінарні індикатори довіри, що базуються на перевищенні відхиленням заданого порогу, дозволяють у режимі реального часу виключати певні сенсори з обчислень або зменшувати їхній вплив. Це значно підвищує живучість системи, особливо в умовах кібератак. У підсумку, значення $T_i(k)$, забезпечує інтелектуальне, адаптивне керування потоками інформації, оптимізуючи процес прийняття рішень та формування оцінок стану в розподілених кіберфізичних системах. Такий підхід дозволяє побудувати Smart Grid, стійку до внутрішніх і зовнішніх впливів, з високим рівнем автономності, точності та надійності.

Попри отримані результати, дослідження має певні обмеження, що визначають напрями подальших робіт. Моделювання затримок у мережевих каналах виконано в узагальненому вигляді без урахування специфіки транспортних протоколів і топології мережевих сегментів, тому точні часові характеристики можуть відрізнятися під час практичної реалізації. Також не оцінювалася залежність точності та стійкості системи від конкретних налаштувань IaaS/PaaS-інфраструктури, що впливають на латентність і доступність обчислювальних ресурсів. Крім того, експерименти не охоплювали перевірку функціонування системи на реальних промислових трасах, які використовують протоколи IEC 61850 та IEC 60870-5-104, що планується як наступний етап дослідження для підвищення достовірності результатів і практичної застосовності моделі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У проведеному дослідженні обґрунтовано та реалізовано концепцію інтелектуальної системи керування та захисту для Smart Grid, здатної забезпечувати стійкість функціонування в умовах складних, багатофакторних кібератак. Запропонована архітектура поєднує механізми розподіленого Kalman-фільтра з адаптивною оцінкою довіри, fault-tolerant control, реактивного перемикання режимів управління, а також динамічного моделювання ризиків і залишкових похибок. Ключовим елементом системи є довіра до сенсорних вузлів, що оновлюється в режимі реального часу на основі відповідності між прогнозованими та фактичними вимірюваннями, поведінкових відхилень та контекстних параметрів мережі. Таке зважене оновлення стану системи дозволяє пригнічувати вплив потенційно скомпрометованих сенсорів без потреби їх жорсткого вимкнення, забезпечуючи

робастність навіть за умов часткової втрати достовірності даних. Результати моделювання показали, що при втраті до 40% каналів спостереження система зберігає стабільність, тоді як класичні підходи втрачають контроль уже при 15–20% втрат.

Окрім цього, реалізовано механізм децентралізованого узгодження локальних оцінок, що усуває залежність від центрального контролера, підвищуючи живучість архітектури в умовах атак типу denial-of-service або компрометації головного вузла. Fault-tolerant control забезпечує автоматичне перемикання між номінальним і захищеним режимами управління залежно від рівня довіри до сенсорних даних і виявлених аномалій, що формалізується через логічні індикатори і метрики ризику. Запропонований підхід адаптивно модулює вплив кожного вузла залежно від його поведінки, що дозволяє досягти високої точності оцінки стану системи без втрат часу на ручне втручання. Система демонструє здатність до самоадаптації, підтримуючи функціональну сталість Smart Grid навіть у разі атак на інформаційну, сенсорну або виконавчу підсистеми.

Перспективи подальших досліджень передбачають інтеграцію глибоких нейронних мереж (зокрема LSTM та графових GNN) для прогнозування атак і виявлення латентних аномалій, розширення математичної моделі за допомогою марковських процесів і теорії ігор з неповною інформацією для моделювання дій зловмисника, а також створення цифрового двійника Smart Grid для тестування захисної системи в реальних сценаріях. Окрему увагу варто приділити впровадженню edge-обчислень для забезпечення автономності прийняття рішень у розподілених кластерах без участі центрального сервера. Таким чином, сформована в дослідженні модель є фундаментом для побудови адаптивно-живучих Smart Grid, здатних до автономного виявлення, реагування і відновлення після атак у режимі реального часу, що становить критично важливий напрям розвитку кіберстійкої енергетичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sun, C.-C., Liu, C.-C., & Xie, J. (2016). Cyber-physical system security of a power grid: State-of-the-art. *Electronics*, 5(3), 40. https://doi.org/10.3390/electronics5030040
2. Younisse, R., & AlKasassbeh, M. (2025). Evaluating deep learning for detecting data integrity attacks in energy smart grids. *In 2025 International Conference on New Trends in Computing Sciences (ICTCS)*, pp. 368–372. https://doi.org/10.1109/ICTCS65341.2025.10989460
3. Jiang, W., Gao, W., Wang, W., Li, Y., Li, Y., & Zhang, G. (2025). Detection of false data injection attack in smart grid based on extended Kalman and smooth variable structure filter. *IEEE Access*, 13, 5257–5270. https://doi.org/10.1109/ACCESS.2024.3524558
4. Zhang, D.-Y., & Li, X.-J. (2025). Fully distributed resilient energy management for smart grids under false data injection attacks. *IEEE Internet of Things Journal*, 12(15), 32035–32045. https://doi.org/10.1109/JIOT.2025.3575397
5. Li, L., Ding, S. X., Zhou, L., Zhong, M., & Peng, K. (2024). The system dynamics analysis, resilient and fault-tolerant control for cyber-physical systems. arXiv. https://arxiv.org/abs/2409.13370
6. Cao, Y., Zhang, L., Zhao, X., Jin, K., & Chen, Z. (2022). An intrusion detection method for industrial control system based on machine learning. *Information*, 13(7), 322. https://doi.org/10.3390/info13070322
7. Alonso, M., Turanzas, J., Amaris, H., & Ledo, A. T. (2021). Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. *Sensors*, 21(17), 5826. https://doi.org/10.3390/s21175826
8. Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing resilient cyber-physical systems: A review of state-of-the-art malware detection approaches, gaps, and future directions. *Computers*, 12(4), 79. https://doi.org/10.3390/computers12040079
9. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzaeva, S. (2025). The methodology for protecting grid environments from malicious code during the execution of computational tasks.

Cybersecurity: Education, Science, Technique, 3(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710

10. Rashed, M., Gondal, I., Kamruzzaman, J., & Islam, S. (2021). State estimation within IED based smart grid using Kalman estimates. *Electronics*, 10(15), 1783. https://doi.org/10.3390/electronics10151783
11. Y. Kostiuk, et al., Architecture of the Software System of Confidential Access to Information Resources of Computer Networks, in: Cyber Security and Data Protection, vol. 4042 (2025) 37-53.
12. Pei, C., Xiao, Y., Liang, W., & Han, X. (2021). A deviation-based detection method against false data injection attacks in smart grid. *IEEE Access*, 9, 15499–15509. https://doi.org/10.1109/ACCESS.2021.3051155
13. Kostiuk, Y., Skladannyi, P., Sokolov, V., Zhyltsov, O., & Ivanichenko, Y. (2025). Effectiveness of information security control using audit logs. *In Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025*), pp. 524–538.
14. Chen, Z., Zhang, H., & Tian, Y. (2023). Security-based resilient distributed energy management against DoS and FDI coordinated attacks. *In 2023 35th Chinese Control and Decision Conference (CCDC)*, pp. 1032–1037. https://doi.org/10.1109/CCDC58219.2023.10326813
15. P. Skladannyi, et al., Model and Methodology for the Formation of Adaptive Security Profiles for the Protection of Wireless Networks in the Face of Dynamic Cyber Threats, in: Cyber Security and Data Protection, vol. 4042 (2025) 17-36.
16. Kurt, M. N., Yılmaz, Y., & Wang, X. (2020). Secure distributed dynamic state estimation in wide-area smart grids. *IEEE Transactions on Information Forensics and Security*, 15, 800–815. https://doi.org/10.1109/TIFS.2019.2928207
17. Костюк Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., Пазинін, А. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. *Кібербезпека: освіта, наука, техніка.* 2025. 4 (28), 633–655. https://doi.org/10.28925/2663-4023.2025.28.857
18. Li, X., Wen, M., He, S., Lu, R., & Wang, L. (2024). A privacy-preserving federated learning scheme against poisoning attacks in smart grid. *IEEE Internet of Things Journal*, 11(9), 16805–16816. https://doi.org/10.1109/JIOT.2024.3365142
19. Younisse, R., & AlKasassbeh, M. (2024). SGID: A semi-synthetic dataset for injection attacks in smart grid systems. *In 2024 15th International Conference on Information and Communication Systems (ICICS)*, pp. 1–4. https://doi.org/10.1109/ICICS63486.2024.10638278
20. Y. Kostiuk, et al., Intelligent System for Simulation Modeling and Research of Information Objects, in: 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), vol. 4053 (2025) 237-251.
21. Johncy, G., & Shaji, R. S. (2024). Secure smart grid implementation with automatic data integrity attack location prediction and exalted energy theft detection. *Connection Science*, 36(1). https://doi.org/10.1080/09540091.2024.2403393
22. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2025). Models and algorithms for analyzing information risks during the security audit of personal data information system. *In Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*, Vol. 3925, pp. 155–171.
23. An, D., Yang, Q., Liu, W., & Zhang, Y. (2019). Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach. *IEEE Access*, 7, 110835–110845. https://doi.org/10.1109/ACCESS.2019.2933020
24. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. *in: Cybersecurity Providing in Information and Telecommunication Systems II*, Vol. 3826, pp.129–138.
25. Vincent, E., Korki, M., Seyedmahmoudian, M., Stojcevski, A., & Mekhilef, S. (2024). Reinforcement learning-empowered graph convolutional network framework for data integrity attack detection in cyber-physical systems. *CSEE Journal of Power and Energy Systems*, 10(2), 797–806. https://doi.org/10.17775/CSEEJPES.2023.01250
26. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. *In Cyber Hygiene & Conflict Management in Global Information Networks*, Vol. 3925, pp. 249–264.
27. Kang, T., Liu, K., Ye, X., Bai, M., Gao, M., & Zhang, W. (2019). Joint modeling and risk simulation analysis based on cyber-physical system in distribution network. *In 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)* (pp. 1754–1758). https://doi.org/10.1109/APAP47170.2019.9224788

28. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, 215, 108975. https://doi.org/10.1016/j.epsr.2022.108975
29. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IOT-компонентами на основі графових моделей. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Yuliia Kostiuk
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Rzaeva Svitlana
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Yuliia Samoilenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department Automation and Computer Technologies of Control Systems
named after Professor Anatoliy Ladanyuk
National University of Food Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-3787-1435
samoilenkouo@nuft.edu.ua

Nataliia Korshun
Doctor of Science, Professor,
Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCIDID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

INTELLIGENT CONTROL AND SECURITY SYSTEMS IN CYBER-PHYSICAL AND CLOUD ENVIRONMENTS OF SMART GRID

Abstract. The paper examines methodological, algorithmic, and architectural approaches to designing intelligent control and defense systems aimed at ensuring the operational resilience of Smart Grids under the growing intensity of cyber threats. The necessity of transitioning from traditional IT-oriented security tools to hybrid adaptive solutions is substantiated. These solutions combine mechanisms of cyber-physical survivability, automatic recovery, and cognitive response to high-risk attacks such as Denial-of-Service, spoofing, and data injection. A conceptual model of Smart Grid resilience architecture is proposed, built on the synthesis of robust estimation methods, fault-tolerant control, distributed filtering (Distributed Kalman Filtering), and dynamic trust management models. A systematic classification of modern attack vectors targeting digital substations, SCADA, RTU, and HMI components is developed, with formalization of requirements for their protection in the context of both information and physical security. The study explores cloud-edge orchestration of Smart Grid telemetry streams, deploying analytics close to data sources (edge) and scalable aggregation in the cloud for model training and real-time event correlation. The proposed mechanisms account for latency, bandwidth, and workload isolation constraints within cloud environments. The paper highlights challenges in implementing continuous monitoring,

anomaly detection, and real-time decision-making, and identifies future directions involving self-learning models for incident detection and reactive control based on artificial intelligence algorithms, considering scalability, reliability, and resilience to hidden threats. The effectiveness of the proposed model is confirmed through experimental simulation of false data injection, DoS, and spoofing attacks in digital substation environments of Smart Grids.

Keywords: Smart Grid, cloud computing, edge computing, orchestration, intelligent control, attack resilience, distributed Kalman filter, trust metrics, survivable control, cyber-physical systems.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Sun, C.-C., Liu, C.-C., & Xie, J. (2016). Cyber-physical system security of a power grid: State-of-the-art. *Electronics*, 5(3), 40. https://doi.org/10.3390/electronics5030040
2. Younisse, R., & AlKasassbeh, M. (2025). Evaluating deep learning for detecting data integrity attacks in energy smart grids. *In 2025 International Conference on New Trends in Computing Sciences (ICTCS)*, pp. 368–372. https://doi.org/10.1109/ICTCS65341.2025.10989460
3. Jiang, W., Gao, W., Wang, W., Li, Y., Li, Y., & Zhang, G. (2025). Detection of false data injection attack in smart grid based on extended Kalman and smooth variable structure filter. *IEEE Access*, 13, 5257–5270. https://doi.org/10.1109/ACCESS.2024.3524558
4. Zhang, D.-Y., & Li, X.-J. (2025). Fully distributed resilient energy management for smart grids under false data injection attacks. *IEEE Internet of Things Journal*, 12(15), 32035–32045. https://doi.org/10.1109/JIOT.2025.3575397
5. Li, L., Ding, S. X., Zhou, L., Zhong, M., & Peng, K. (2024). The system dynamics analysis, resilient and fault-tolerant control for cyber-physical systems. arXiv. https://arxiv.org/abs/2409.13370
6. Cao, Y., Zhang, L., Zhao, X., Jin, K., & Chen, Z. (2022). An intrusion detection method for industrial control system based on machine learning. *Information*, 13(7), 322. https://doi.org/10.3390/info13070322
7. Alonso, M., Turanzas, J., Amaris, H., & Ledo, A. T. (2021). Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. *Sensors*, 21(17), 5826. https://doi.org/10.3390/s21175826
8. Malik, M. I., Ibrahim, A., Hannay, P., & Sikos, L. F. (2023). Developing resilient cyber-physical systems: A review of state-of-the-art malware detection approaches, gaps, and future directions. *Computers*, 12(4), 79. https://doi.org/10.3390/computers12040079
9. Kostiuk, Y., Dovzhenko, N., Mazur, N., Skladannyi, P., & Rzaeva, S. (2025). The methodology for protecting grid environments from malicious code during the execution of computational tasks. *Cybersecurity: Education, Science, Technique*, 3(27), 22–40. https://doi.org/10.28925/2663-4023.2025.27.710
10. Rashed, M., Gondal, I., Kamruzzaman, J., & Islam, S. (2021). State estimation within IED based smart grid using Kalman estimates. *Electronics*, 10(15), 1783. https://doi.org/10.3390/electronics10151783
11. Y. Kostiuk, et al., Architecture of the Software System of Confidential Access to Information Resources of Computer Networks, in: Cyber Security and Data Protection, vol. 4042 (2025) 37-53.
12. Pei, C., Xiao, Y., Liang, W., & Han, X. (2021). A deviation-based detection method against false data injection attacks in smart grid. *IEEE Access*, 9, 15499–15509. https://doi.org/10.1109/ACCESS.2021.3051155
13. Kostiuk, Y., Skladannyi, P., Sokolov, V., Zhyltsov, O., & Ivanichenko, Y. (2025). Effectiveness of information security control using audit logs. *In Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)*, pp. 524–538.
14. Chen, Z., Zhang, H., & Tian, Y. (2023). Security-based resilient distributed energy management against DoS and FDI coordinated attacks. *In 2023 35th Chinese Control and Decision Conference (CCDC)*, pp. 1032–1037. https://doi.org/10.1109/CCDC58219.2023.10326813
15. P. Skladannyi, et al., Model and Methodology for the Formation of Adaptive Security Profiles for the Protection of Wireless Networks in the Face of Dynamic Cyber Threats, in: Cyber Security and Data Protection, vol. 4042 (2025) 17-36.
16. Kurt, M. N., Yılmaz, Y., & Wang, X. (2020). Secure distributed dynamic state estimation in wide-area smart grids. *IEEE Transactions on Information Forensics and Security*, 15, 800–815. https://doi.org/10.1109/TIFS.2019.2928207

17. Kostiuk, Y., Khorolska, K., Bebeshko, B., Dovzhenko, N., Korshun, N., & Pazynin , A. (2025). Instrumental means of ensuring information security against hidden threats in cloud computing infrastructure. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *4*(28), 633–655. https://doi.org/10.28925/2663-4023.2025.28.857
18. Li, X., Wen, M., He, S., Lu, R., & Wang, L. (2024). A privacy-preserving federated learning scheme against poisoning attacks in smart grid. *IEEE Internet of Things Journal*, 11(9), 16805–16816. https://doi.org/10.1109/JIOT.2024.3365142
19. Younisse, R., & AlKasassbeh, M. (2024). SGID: A semi-synthetic dataset for injection attacks in smart grid systems. *In 2024 15th International Conference on Information and Communication Systems (ICICS)*, pp. 1–4. https://doi.org/10.1109/ICICS63486.2024.10638278
20. Y. Kostiuk, et al., Intelligent System for Simulation Modeling and Research of Information Objects, in: 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), vol. 4053 (2025) 237-251.
21. Johncy, G., & Shaji, R. S. (2024). Secure smart grid implementation with automatic data integrity attack location prediction and exalted energy theft detection. *Connection Science*, 36(1). https://doi.org/10.1080/09540091.2024.2403393
22. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2025). Models and algorithms for analyzing information risks during the security audit of personal data information system. *In Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*, Vol. 3925, pp. 155–171.
23. An, D., Yang, Q., Liu, W., & Zhang, Y. (2019). Defending against data integrity attacks in smart grid: A deep reinforcement learning-based approach. *IEEE Access*, 7, 110835–110845. https://doi.org/10.1109/ACCESS.2019.2933020
24. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. *in: Cybersecurity Providing in Information and Telecommunication Systems II*, Vol. 3826, pp.129–138.
25. Vincent, E., Korki, M., Seyedmahmoudian, M., Stojcevski, A., & Mekhilef, S. (2024). Reinforcement learning-empowered graph convolutional network framework for data integrity attack detection in cyber-physical systems. *CSEE Journal of Power and Energy Systems*, 10(2), 797–806. https://doi.org/10.17775/CSEEJPES.2023.01250
26. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. *In Cyber Hygiene & Conflict Management in Global Information Networks*, Vol. 3925, pp. 249–264.
27. Kang, T., Liu, K., Ye, X., Bai, M., Gao, M., & Zhang, W. (2019). Joint modeling and risk simulation analysis based on cyber-physical system in distribution network. *In 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP)* (pp. 1754–1758). https://doi.org/10.1109/APAP47170.2019.9224788
28. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, 215, 108975. https://doi.org/10.1016/j.epsr.2022.108975
29. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). Graph-based methodology for detection and localization of cyber threats in cloud environments with integrated iot components. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*, *1*(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938