DOI: 10.18372/2225-5036.31.20638

МЕТОДОЛОГІЯ ПІДТРИМКИ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ З ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ ІНФОРМАЦІЇ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ

Тетяна Смірнова, Павло Усік, Ірина Лисенко, Костянтин Буравченко, Олексій Смірнов

Центральноукраїнський національний технічний університет, Україна

СМІРНОВА Тетяна Віталіївна, к.т.н.
Рік та місце народження: 1988 рік, м. Кропивницький, Україна.
Освіта: Кіровоградський національний технічний університет, 2010 рік.
Посада: старший викладач кафедри автоматизації виробничих процесів
Наукові інтереси: кібербезпека, мережеві технології, інженерія програмного забезпечення.
Публікації: більше 100 наукових публікацій, серед яких монографії, наукові статті та патенти на винаходи.
E-mail: sm.tetyana@gmail.com
Orcid ID: 0000-0001-6896-0612

УСІК Павло Сергійович, доктор філософії (PhD).
Рік та місце народження: 1995р., м. Кропивницький, Україна
Освіта: Центральноукраїнський національний технічний університет, 2018 рік
Посада: старший викладач кафедри кібербезпеки та програмного забезпечення
Наукові інтереси: кібербезпека, розробка операційних систем, інструменти та парадигми сучасного програмування.
Публікації: 25 наукових праць, серед них: монографії, наукові статті та навчально – методичні посібники.
E-mail: usikps@kntu.kr.ua
Orcid ID: 0000-0002-3268-342X

ЛИСЕНКО Ірина Анатоліївна, к.т.н.
Рік та місце народження: 1978р., м. Нижнєвартівськ, Тюменська область, Російська федерація
Освіта: Кіровоградський державний педагогічний університет імені Володимира Винниченка
Посада: старший викладач кафедри кібербезпеки та програмного забезпечення
Наукові інтереси: кібербезпека, інформаційна безпека, інтелектуальний аналіз даних, алгоритми та методи обчислень, математичне моделювання.
Публікації: більше 40 наукових праць, серед них: монографії, наукові статті та навчально – методичні посібники.
E-mail: min_max@i.ua
Orcid ID: 0000-0003-4394-4960

БУРАВЧЕНКО Костянтин Олегович, к.т.н., доцент
Рік та місце народження: 1989 рік, м. Кропивницький, Україна.
Освіта: Кіровоградський національний технічний університет, 2011 рік.
Посада доцент кафедри кібербезпеки та програмного забезпечення
Наукові інтереси: кібербезпека, мережеві технології, інженерія програмного забезпечення.
Публікації: більше 100 наукових публікацій, серед яких монографії, наукові статті та патенти на винаходи.
E-mail: buravchenkok@gmail.com
Orcid ID: 0000-0001-6195-7533

СМІРНОВ Олексій Анатолійович, д.т.н., професор
Рік та місце народження: 1977 рік, м. Кропивницький, Україна.
Освіта: Харківський військовий університет, 1999 рік.
Посада: завідувач викладач кафедри автоматизації виробничих процесів,
Наукові інтереси: кібербезпека, мережеві технології, інженерія програмного забезпечення.
Публікації: більше 400 наукових публікацій, серед яких монографії, наукові статті та патенти на винаходи.
E-mail: dr.smirnovoa@gmail.com
Orcid ID: 0000-0001-9543-874X

Анотація. *У даній статті запропоновано методологія підтримки технологічних процесів у критичній інфраструктурі на основі хмарних технологій. Критична інфраструктура держави потребує нових підходів для забезпечення надійності, адаптивності та інформаційної безпеки технологічних процесів. При цьому, хмарні технології відкривають нові можливості для масштабованого моніторингу, аналізу та управління критичної інфраструктури в умовах гібридних загроз. Таким чином, запропонована методологія спрямована на формування інтегрованої цифрової платформи, яка базується на використанні хмарних технологій для моніторингу, аналізу та автоматизованого управління технологічними процесами в умовах високих ризиків. Метою розробленої методології є забезпечення безперервної, безпечної та стійкої роботи технологічних процесів об'єктів критичної інфраструктури держави за рахунок впровадження хмарних технологій для моніторингу, аналізу та автоматизованого управління в умовах високих ризиків. Основним завданням цієї*

методології є розробка комплексної архітектури підтримки технологічних процесів критичної інфраструктури на основі хмарних рішень, підвищення рівня технологічної готовності об'єктів критичної інфраструктури до функціонування в нестабільному середовищі шляхом впровадження адаптивних, масштабованих та захищених рішень. Запропонована у даній роботі методологія орієнтована на функціонування в умовах підвищених загроз, як техногенного, так і кібернетичного характеру з урахуванням вимог до інформаційної безпеки, надійності зв'язку, резервування критичних компонентів та гнучкості архітектури системи. Такий підхід сприяє підвищенню рівня технологічної готовності об'єктів критичної інфраструктури до роботи в умовах нестабільного середовища, знижує ймовірність збоїв та забезпечує стійкість до зовнішніх впливів.

Ключові слова: *технологічні процеси, критична інфраструктура, хмарні технології, штучний інтелект, база знань, 5G, моделювання, аналіз вразливостей, кіберзагрози, кібербезпека, Інтернет речей, CAD/CAM/ERP, CAD/SCADA, 5G, IT-інфраструктура, системи підтримки прийняття рішень, цільова функція, KPI, показники ефективності, інтелектуальне управління.*

Вступ. Розробка методології, що поєднує специфічні вимоги критичної інфраструктури оборонної галузі з перевагами хмарних платформ, потребує системного підходу. Така методологія має враховувати не лише технічні параметри продуктивності та надійності, але й нормативно-правові обмеження, стандарти кіберзахисту та особливості інтеграції з існуючими виробничими комплексами.

В даній роботі визначаються ключові принципи побудови такої методології, спрямованої на створення стійких, безпечних та адаптивних рішень для підтримки технологічних процесів критичної інфраструктури підприємств.

Отже, основними принципами побудови методології є:

– *Безперервність* – мінімізація впливу відмов на технологічні процеси.

– *Масштабованість* – здатність реагувати на зміну обсягів обробки даних.

– *Кіберстійкість* – виявлення та протидія кіберзагрозам у реальному часі.

– *Інтероперабельність* – сумісність з SCADA, IoT, ERP та іншими системами.

Для опису сукупності методів, прийомів і принципів, що використовуються у дослідженні, розроблена структурна модель методології (рис. 1), яка включає в себе різні рівні методів, що застосовуються на емпіричному, теоретичному та технологічному рівнях. Дані методи в деталях розглянуті в попередніх розділах дослідження.

Рис. 1. Структурна модель методології підтримки технологічних процесів

Опис моделі (рис. 1) наведено з аналізом ролі методів підтримки технологічних процесів критичної інфраструктури підприємств, а зокрема:

– *Ідентифікація КІ*. Метою є визначення всіх об'єктів, систем та процесів, які належать до критичної інфраструктури підприємства оборонно-промислового комплексу з класифікацією активів, визначення їх рівня критичності, встановлення пріоритетів захисту та підтримки.

– *KPI-моделювання*. Метою є формування системи ключових показників ефективності (KPI) для моніторингу стану та продуктивності технологічних процесів з визначенням метрик для оцінки безперервності, швидкодії, надійності та безпеки.

– *Хмарна архітектура*. Метою є проектування інфраструктури, яка забезпечить масштабованість, відмовостійкість і захист даних, з визначенням сервісів (IaaS, PaaS, SaaS), планування резервування.

– *Інтерпретація та реагування*. Метою є забезпечення оперативного аналізу даних і швидке прийняття рішень у разі відхилень або виникнення інцидентів з впровадженням систем моніторингу, аналітики та автоматизованих сценаріїв реагування.

– *Інтелектуальне управління*. Метою є автоматизація управління технологічними процесами з використанням алгоритмів штучного інтелекту та машинного навчання, прогнозування навантажень, оптимізація ресурсів, адаптація до змін у режимі реального часу.

– *5G-мережа та її кіберзахист*. Метою є забезпечення високошвидкісного, надійного і захищеного каналу зв'язку для КІ, інтеграція 5G для критично важливих процесів, впровадження багаторівневих засобів кіберзахисту (шифрування, аутентифікація, IDS/IPS) зі стабільною передачею даних з мінімальною затримкою та максимальним рівнем безпеки.

Аналіз існуючих досліджень

У роботі [1] розглянуто прийняття рішень за допомогою процесу аналітичної ієрархії, а праця [2] посвячена розгляду системи підтримки рішень та бізнес-аналітиці. Робота [3] присвячена прийняттю рішень у нечіткому середовищі. У роботі [4] розглянуто лінійне програмування та мережеві потоки. Робота [5] присвячена побудовам експертних систем. Принципи реалізації та побудови технологій штучного інтелекту розглянуті у роботі [6]. Роботи [7, 8] присвячені питанням проектування в

досліджені інформаційних систем. У роботі [9] розглянуті інтелектуальні системи керування в 5G. Питання забезпечення рівня безпеки у інформаційно-телекомунікаційних системах, хмарних системах та Інтернеті речей розглянуті у роботах [10-17]. Але методологія підтримки технологічних процесів критичної інфраструктури на базі хмарних технологій на даний момент відсутня у науковій літературі. Таким чином, виникають труднощі при побудові критичної інфраструктури держави, що потребує нових підходів для забезпечення надійності, адаптивності та інформаційної безпеки технологічних процесів. При цьому, хмарні технології відкривають нові можливості для масштабованого моніторингу, аналізу та управління критичної інфраструктури в умовах гібридних загроз.

Метою даної роботи є забезпечення безперервної, безпечної та стійкої роботи технологічних процесів об'єктів критичної інфраструктури держави за рахунок впровадження хмарних технологій для моніторингу, аналізу та автоматизованого управління в умовах високих ризиків.

Основна частина дослідження

Для визначення способу збору та аналізу інформації та загальної логіки, розроблені методологічні компоненти, які тісно пов'язані між собою і утворюють цілісну систему, що забезпечує науковість і обґрунтованість дослідження.

Інтелектуальна система підтримки прийняття рішень для вибору методу проєктування

Сучасні критичні об’єкти інфраструктури стикаються з необхідністю інтеграції складних проєктних та технологічних рішень. Для підтримки процесу прийняття рішень щодо вибору оптимального методу проєктування застосовуються інтелектуальні системи підтримки прийняття рішень (СППР), що базуються на сучасних математичних моделях, знаннях експертів та алгоритмах машинного навчання.

СППР впроваджує аналіз вхідних даних про стан технологічних процесів, вибирає оптимальні методи конструкторського й технологічного проектування, використовує методи штучного інтелекту для моделювання сценаріїв і рекомендацій.

Інтелектуальні СППР передбачають комбінацію формальних методів вибору (AHP – Analytic Hierarchy Process), які передбачають rule-based підходи (системи правил), та методики нечіткої логіки. Задача вибору методу проєктування формалізується як задача багатокритеріального аналізу альтернатив (MCDA) [1]. Метод аналітичної ієрархії (AHP) є теорією вимірювання через парні порівняння і базується на судженнях експертів для визначення пріоритетних шкал. Саме ці шкали вимірюють нематеріальні аспекти в абсолютних значеннях. Порівняння проводяться за допомогою шкали абсолютних суджень, яка показує, наскільки один елемент домінує над іншим щодо певної властивості. Судження можуть бути непослідовними, і питання про те, як виміряти непослідовність і покращити судження, де це можливо для отримання кращої послідовності, є предметом дослідження AHP [2]. Отримані пріоритетні шкали синтезуються шляхом множення їх на пріоритети батьківських вузлів і підсумовування для всіх таких вузлів.

Математичну модель СППР можливо описати як множину альтернатив проєктування $A = \{a_1, a_2, ..., a_n\}$, та множину критеріїв $K = \{k_1, k_2, ..., k_m\}$. Кожна альтернатива оцінюється за допомогою функції корисності $u(a_i)$, яка обчислюється як:

$$u(a_i) = \sum w_j \times r_j(a_i), j = 1... . \quad (1)$$

де:

– w_j – вага критерію j,

– $r_j(a_i)$ – нормалізована оцінка альтернативи a_i за критерієм k_j.

Далі приведено розроблена спрощена архітектура побудови СППР для вибору методу проєктування (рис. 2).

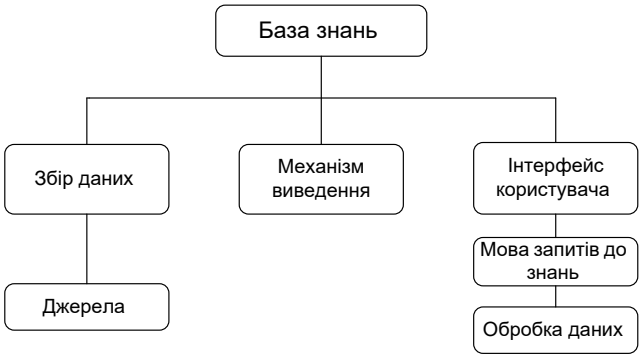

Рис. 2. Архітектура побудови СППР для вибору методу проєктування

До представленої архітектури (рис. 2) включено:

– *База знань (Knowledge Base)*. Центральний елемент системи, що акумулює структуровані й неструктуровані знання, правила, шаблони рішень, кейси, нормативні документи, технічні інструкції тощо. Ця база формується з урахуванням оновлень, накопиченого досвіду та результатів аналізу.

– *Збір даних (Data Acquisition)*. Компонент відповідає за підключення та отримання інформації з сенсорів, SCADA-систем, телеметрії, промислових систем моніторингу.

– *Джерела (Sources).* Конкретні точки даних: сенсорні вузли, бази технічного обліку, ERP-системи, системи контролю доступу, камери, IoT-пристрої тощо.

– *Механізм виведення / логічного виводу (Inference Engine)*. Це ядро інтелектуальної обробки, що виконує логічні операції на основі правил, збережених у базі знань; приймає рішення; прогнозує можливі відмови; генерує рекомендації або управляючі сигнали.

– *User Interface (Інтерфейс користувача)*. Дає змогу взаємодіяти з системою, формулювати запити, переглядати дані або управляти процесами.

– *Knowledge Query Language (Мова запитів до знань)*. Дає змогу ставити запити у зрозумілій формі, з можливістю уточнення: для прикладу ("Що робити при зниженні тиску?", "Який прогноз простою обладнання?");

– *Processio Data (Обробка даних)*. Виконує попередню обробку; фільтрує, нормалізує, перетворює вхідні дані для використання в системі.

Взаємозв'язки наведених вище елементів можна подати наступним чином. Knowledge Base централізовано підтримує зв'язок з усіма підсистемами. Inference Engine працює безпосередньо з базою знань і даними, що надходять. User Interface дозволяє як отримувати інформацію, так і ініціювати запити на аналіз.

Таким чином, для даної архітектури можливе застосування в критичній інфраструктурі і зокрема:

– підтримка операторських рішень в режимі реального часу;

– автоматичне попередження про збої;

– оптимізація технологічних процесів;

– виявлення аномалій на основі знань та актуальних даних.

Інтелектуальні СППР дозволяють систематизувати процес вибору методу проєктування, враховуючи множину критеріїв, експертні знання та дані з попереднього досвіду. Застосування таких систем дозволяє підвищити обґрунтованість рішень, скорочує час прийняття рішень та знижує людський фактор.

Процес оптимізації технологічного процесу у КІ

Оптимізація технологічних процесів у критичній інфраструктурі передбачає визначення найефективніших способів виконання виробничих операцій з урахуванням обмежень ресурсів, часу, безпеки та надійності. У хмарно-орієнтованому середовищі це означає також адаптацію до змін умов і наявних сервісів у реальному часі.

Серед основних підходів до оптимізації варто виділити [3,4]:

– Лінійне та нелінійне програмування (для моделей з чітко формалізованими функціями витрат та обмежень);

– Методи динамічного програмування (для задач із часовою залежністю);

– Стохастичне програмування (для врахування невизначеності в параметрах);

– Еволюційні алгоритми (генетичні алгоритми, алгоритми рою частинок) для задач з великим простором рішень та складною залежністю між параметрами.

Математична модель оптимізації технологічного процесу має наступні параметри:

– $x = \{x_1, x_2, ..., x_n\}$ – набір параметрів технологічного процесу (наприклад, температура, тиск, час обробки);

– $f(x)$ – цільова функція (наприклад, мінімізація часу, витрат або енергоспоживання);

– $q_i(x) \le 0, i = 1,...,m$ – система обмежень (ресурси, надійність, екологічні норми);

$$x \in X \subseteq \mathbb{R}^n. \quad (2)$$

Загальний вигляд задачі оптимізації можна уявити як:

$$\min_{x \in X} f(x) \text{ – при умові: } q_i(x) \le 0,\ i = 1,...,m. \quad (3)$$

Для багатокритеріального випадку:

$$\min_{x \in X} (f_1(x), f_2(x), ..., f_k(x)). \quad (4)$$

з подальшим використанням методу зважених коефіцієнтів або Парето-оптимальності.

Тоді архітектурна схема оптимізації в хмарному середовищі буде мати вигляд:

mermaid

flowchart TD

Start [Початок]

Input [Збір вхідних параметрів з технологічного середовища]

CloudOpt [Передача даних у хмару]

Model [Оптимізаційна модель / обчислення]

Decision [Визначення оптимального набору параметрів]

Feedback [Передача результатів назад до виробничої системи]

End [Впровадження оптимізованого сценарію]

Start – -> Input – -> CloudOpt – -> Model – -> Decision – -> Feedback – -> End

Результатом реалізації прикладу є графік залежності цільової функції від двох параметрів (time, temperature), рис 3.

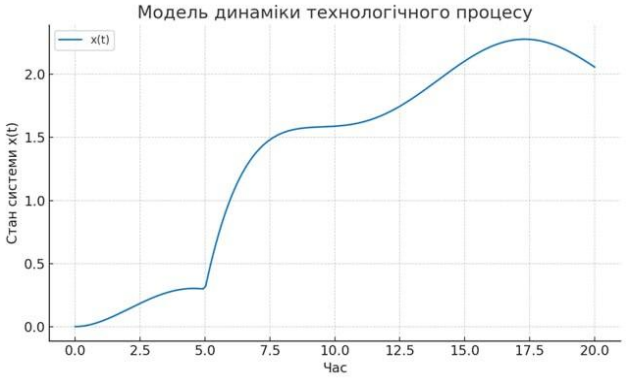

Рис. 3. Графік залежності цільової функції від часу та температури процесу

Цей графік демонструє, як система реагує на включення керуючого впливу (починається після 5 секунд), та вплив зовнішнього гармонічного збурення (перешкоди).

Підсумовуючи, можна зробити висновки що:

– оптимізація дозволяє знизити витрати на виконання технологічних процесів без втрати якості та надійності;

– інтеграція хмарних ресурсів забезпечує адаптивність та масштабованість розрахунків;

– врахування обмежень забезпечує відповідність стандартам безпеки та сталого розвитку.

Розробка Бази знань для визначення вхідних даних

База знань (БЗ) – це структуроване середовище, що накопичує, формалізує та забезпечує доступ до знань про предметну область. У структурі дослідження, це знання про технологічні процеси, критерії оптимізації, типові конфігурації та обмеження для критичної інфраструктури.

Формально БЗ складається з:

– фактів – дескриптивна інформація про об'єкти процесу;

– правил – умовно-логічні оператори типу «якщо–то»;

– моделей – математичні або симуляційні залежності;

– онтологій – формалізоване представлення взаємозв'язків між сутностями;

– підсистеми навчання – накопичення нових знань через машинне навчання або експертне введення.

Архітектурна схема побудови БЗ має вигляд:

Input – -> Preproc – -> KB – -> Inference – -> Output

Output – -> Feedback – -> KB

```
mermaid
graph TD
  Input [Сенсори / Введення вручну]
  Preproc [Модуль попередньої обробки]
  KB [База знань]
  Inference [Механізм логічного висновку]
  Output [Рекомендації / Налаштування]
  Feedback [Зворотний зв'язок від користувача]

  Input – -> Preproc – -> KB – -> Inference – -> Output
  Output – -> Feedback – -> KB
```

Перелік основних функцій, які виконує база знань, має наступний вигляд

– категоризації вхідних даних;

– ініціалізації параметрів для оптимізації;

– забезпечення пояснюваності рішень;

– підтримки оновлення моделі на основі нових даних.

Математичну модель бази знань можна подати як множину правил та фактів у вигляді продукційної системи:

– множина фактів (вхідних параметрів, станів):

$$F = \{f_1, f_2, ..., f_n\}\ ; \quad (5)$$

– множина правил у формі:

$$R = \{r, r_2, ...r_m\}\ ; \quad (6)$$

– у формі:

$$r_i : if a_1 \wedge a_2 \wedge ... \wedge a_k \Rightarrow b\ . \quad (7)$$

Тоді логічний висновок можна сформулювати як:

$$\forall r_i \in R: \text{ Antecedents} \subseteq F \Rightarrow \text{ Consequent} \in F_{new}\ . \quad (8)$$

Таким чином, можна констатувати, що система ітеративно збагачує множину фактів для досягнення цільового стану.

Правила в базі знань

Правила – це умовно-логічні конструкції (наприклад, "Якщо KPI падає нижче 90% протягом 5 хвилин, сповістити CERT- команду, яка відповідає за реагування на інциденти кібербезпеки "), які дозволяють системі:

– автоматично виявляти аномалії;

– робити рекомендації;

– активувати процедури реагування;

– забезпечувати зв'язок між входами (сенсори, логи) та діями (реакції, звіти, алерти).

У якості ілюстрації приведен графік кількісті нових правил у БЗ в залежності від часу (рисунок 4).

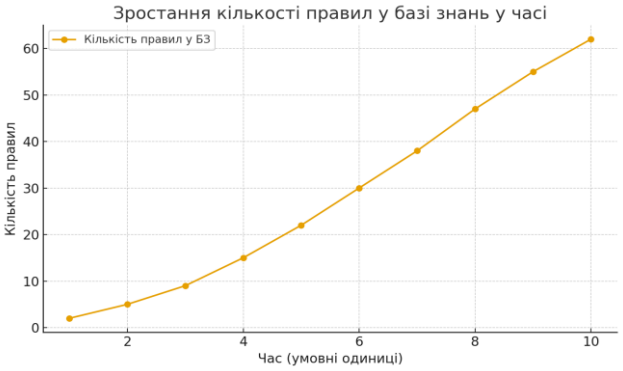

Рис. 4.Кількість нових правил у базі знань у залежності від часу

Горизонтальна вісь показує час (наприклад, щомісячно або щотижнево). Вертикальна вісь кількість нових правил, які були додані у базу знань. Кожна точка показує обсяг збагачення системи знаннями, тобто її "інтелектуальний розвиток".

Графік візуалізує динаміку зростання бази знань (БЗ) демонструє поступове й стабільне збільшення обсягу бази знань, що відображає активну фазу її наповнення на етапі розробки інтелектуальній системі підтримки прийняття рішень яка використовується для моніторингу, аналізу та реагування в ІКС.

Аналізуючи даний графік, можна зробити наступні висновки:

– Дає можливість аналізу розвитку системи – можна наочно побачити, в які періоди система розвивалася швидше (наприклад, після кіберінцидентів).

– Оцінка ефективності аналітиків – якщо правила додаються вручну, це показує продуктивність команди.

– Контроль за навчанням AI – у випадку автоматичного генератора знань можна оцінити стабільність моделі.

Резюмуючи можливо зробити висновки що, база знань:

– дозволяє стандартизувати введення вхідних параметрів;

– забезпечує гнучке масштабування за рахунок додавання нових правил;

– підвищує ефективність рішень оптимізації, знижуючи обчислювальні витрати.

Актуальність бази підтримується шляхом зворотного зв'язку та автоматизованого навчання;

Моніторинг ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі на основі хмарних технологій

Моніторинг KPI (Key Performance Indicators) – в нашому випадку це систематичний процес збору, обробки та візуалізації даних ефективності технологічних процесів. У контексті критичної інфраструктури це має особливу важливість для забезпечення надійності, безпеки, стабільності та відповідності нормативам.

Основні напрями моніторингу [10] можна представити наступним чином:

– технічні KPI**,** час простою, кількість відмов, швидкість обробки;

– операційні KPI, використання ресурсів, рівень автоматизації;

– безпекові KPI, кількість інцидентів, середній час реагування;

– економічні KPI, витрати, ефективність інвестицій.

В свою чергу, хмарні технології в даному випадку дозволяють уніфікувати збирання даних, масштабувати обчислення та забезпечувати доступ до аналітики в режимі реального часу.

KPI в ІКС (інформаційно-комунікаційній системі), яка працює в режимі реального часу, визначається не лише якістю виконання функцій, але й часом реагування**,** надійністю та ефективністю використання ресурсів**.**

Архітектура моніторингової системи має вигляд:

Sensors – -> Gateway – -> Cloud – -> DB – -> Analytics – -> Dashboard

Analytics – -> Alerting

KPI (ключовий показник ефективності) в таких системах часто формалізується як функція від кількох параметрів:

$$KPI = f\left(Q, T_{\text{упр}}, E\right), \qquad (9)$$

де:

– Q – якість вихідного результату (точність, відмовостійкість, енергоспоживання тощо);

– $T_{\text{упр}}$ – тривалість управлінського циклу, включно з аналізом, прийняттям рішення та дією;

– E – ефективність використання ресурсів.

Формалізація KPI виглядає наступним чином:

$$KPI = \alpha \cdot \left(1 - \frac{T_{\text{упр}}}{T_{\text{макс}}}\right) + \beta \cdot Q + \gamma \cdot \left(1 - \frac{R}{R_{\text{макс}}}\right), \qquad (10)$$

де:

– $T_{\text{упр}}$ – фактичний час управлінського циклу (с),

– $T_{\text{макс}}$ – допустимий поріг часу управління (с),

– $Q \in [0,1]$ коефіцієнт якості рішення (відносна точність, надійність),

– R – використані ресурси (CPU, мережа, пам'ять),

– Rмакс – граничні ресурси,

– a, β, γ – вагові коефіцієнти (залежно від пріоритетів системи).

В свою чергу Tупр включає:

$$T\text{упр} = T\text{дат} + T\text{аналіз} + T\text{ухв} + T\text{вик}, \qquad (11)$$

де:

– Tдат – час збору та агрегації даних,

– Tаналіз – час на обробку / прогнозування (наприклад, AI-моделлю),

– Tухв – час на прийняття рішення (інференс),

– Tвик – виконання команди або реакції на подію.

На рис. 5 приведена візуальна ілюстрація складових фактичного часу управлінського циклу

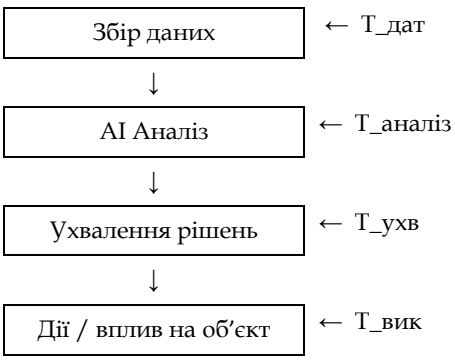

Рис. 5. Складові фактичного часу управлінського циклу

На прикладі коду можна зробити наступний аналіз:

– якщо Тупр → 0, то KPI підвищується;

– якщо якість рішення низька (наприклад, Q < 0.7), KPI знижується, навіть при швидкому управлінні;

– якщо ресурси надмірно споживаються (наприклад, 90% CPU), KPI також погіршується.

Таким чином модель може використовуватись для:

– оцінки ефективності AI-модуля в режимі реального часу;

– оптимізації балансування навантажень у хмарному середовищі;

– адаптивного управління ресурсами (наприклад, autoscaling).

Далі наведено графік, який показує залежність KPI від часу управління (*T*упр) при фіксованих значеннях якості процесу (*Q* = 0.85) та використання ресурсів (*R* = 50)(рис.6), по горизонтальній осі – час управління (*T*упр), від 0 до 100 год,по вертикальній осі – значення KPI.

З коефіцієнтами: α=0.4;β=0.4;γ=0,2.

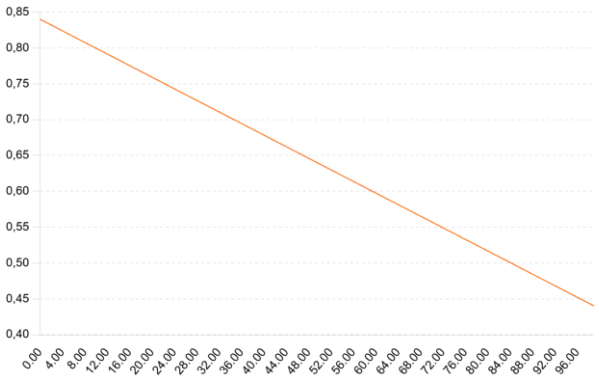

Рис. 6. Залежність KPI від часу управління *T*упр (за фіксованих *Q*=0.85, *R*=50)

На графіку можна спостерігати зменшення KPI зі збільшенням часу *T*упр , тобто чим довше виконується процес, тим менше ефективність.

Виходячи з принципів побудови моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі можна сформулювати основні вимоги:

– Всі KPI мають обчислюватися в реальному часі;

– Візуалізація має оновлюватися мінімум раз на 5 хвилин;

– Хмарні сервіси повинні відповідати стандартам безпеки ISO 27017/27018;

– Варто реалізувати ML-передбачення відмов на основі історичних KPI.

Застосування AI-аналізу для моніторингу KPI Критичної Інфраструктури

AI-модуль в системі CIPS (Critical Infrastructure Process Supervision) виконує наступні функції:

– аналіз трендів KPI;

– виявлення аномалій у процесах;

– формування рекомендацій щодо коригування процесів;

– автоматичне оновлення бази знань на основі нових інцидентів;

– пріоритизацію ризиків на основі впливу на критичні показники.

Математична модель виявлення аномалій (індикатор відхилення KPI) має наступний вигляд [12]:

$$\left|KPI_t - \mu_t\right| > k \cdot \sigma_t , \qquad (12)$$

де:

– KPI_t - значення KPI у момент часу *t*,

– μ_t – ковзне середнє за останні *N* значень,

– σ_t - стандартне відхилення.

– k -параметр чутливості (зазвичай *k*=2 або 3).

Як приклад:

$$\mu_t = \frac{1}{N}\sum_{i=t-N+1}^{t} KPI_t, \qquad (13)$$

$$\sigma_t = \sqrt{\frac{1}{N}\sum_{i=t-N+1}^{t}\left(KPI_t - \mu_t\right)^2} . \qquad (14)$$

Для обгрунтування рекомендацій використовується дерево рішень, яке враховує:

– рівень KPI;

– об'єкт інциденту;

– тип інфраструктурного модуля (електроживлення, зв'язок, охолодження тощо);

– погодинне навантаження.

Алгоритм роботи AI-аналітики має наступний вигляд:

1. Збір KPI та логів за останні 24 години

2. Обчислення ковзного середнього та стандартного відхилення

3. Виявлення відхилень за формулою

4. Аналіз контексту (логів, погодинного навантаження)

5. Вибір правила в базі знань або формування нового Формування рекомендації

7. Додавання запису до логів/бази знань

Приклад автоматичного формування рекомендацій приведений у таблиці 1, в якій для кожного типу інфраструктури є заздалегідь підготовлений шаблон рекомендацій**.**

Таблиця 1

Автоматичне формування рекомендацій

Тип аномалії	**Компонент**	**Рекомендація**
KPI < 92	Модуль живлення	Перевірити стан ДБЖ, рівень напруги живлення
KPI > 98	Система охолодж.	Можлива перевитрата енергії – перевірити роботу
Різкі стрибки швидкості	Зв'язок	Перевірити модулі маршрутизаторів, канали зв'язку

Стосовно Бази знань та навчання, система AI самостійно доповнює базу знань на основі:

– експертного втручання (feedback loop);

– виявлених інцидентів;

– ефективності попередніх рішень (reinforcement learning).

Роблячи висновки можна констатувати,що AI-модуль значно підвищує швидкість та якість реагування на аномальні ситуації. Використання адаптивних моделей дозволяє уникнути помилкових спрацювань.

Подальший розвиток AI це інтеграція з LLM-моделями для генерації описів інцидентів у природній мові.

Розробка інтегрованої комунікаційної системи (ІКС) моніторингу технологічних процесів критичної інфраструктури на основі 5G

В умовах цифрової трансформації критичної інфраструктури (КІ) зростає потреба у високошвидкісному, захищеному та надійному обміні даними між різнорідними компонентами систем управління технологічними процесами. Використання 5G як базової платформи для побудови Інтегрованої комунікаційної системи (ІКС) дозволяє забезпечити:

– Низьку затримку (<1 мс),

– Широкий діапазон пропускної здатності (>10 біт/с),

– Масове підключення пристроїв (до 1 млн на км²),

– Розподілену архітектуру (Edge/Cloud split).

Таким чином, ключовими компонентами ІКС на базі 5G є:

– IoT-шлюзи для збору даних з сенсорів.

– Мережевий рівень 5G з підтримкою network slicing (розділення мережі за пріоритетами сервісів).

– Edge-обчислювальні модулі для обробки на межі (відгук у реальному часі).

– Хмарна платформа для глибокої аналітики.

– Системи управління інцидентами, що реагують на KPI відхилення.

На рис.7 приведена архітектурна модель ІКС на базі 5G.

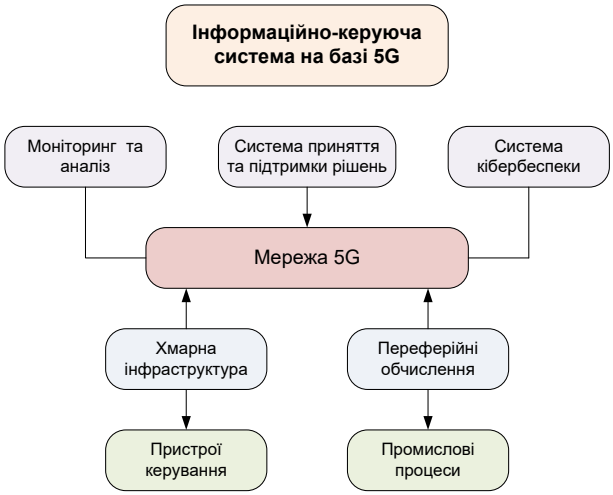

Рис. 7. Архітектурна модель ІКС на базі 5G

Ілюстрація (рис. 7) демонструє архітектуру ІКС, яка використовує інфраструктуру 5G для моніторингу, обробки даних у реальному часі та прийняття рішень щодо ключових технологічних процесів. Така модель дозволяє інтегрувати модулі аналізу, штучного інтелекту, кібербезпеки та обміну даними з розподілених сенсорних систем у межах критичної інфраструктури.

Основні компоненти архітектури включають:

– датчики та сенсори на рівні об'єктів критичної інфраструктури;

– канали передачі даних через 5G;

– інтелектуальний обробник даних з модулем AI-аналітики;

– модуль кіберзахисту для перевірки даних у реальному часі;

– хмарна система зберігання, бази знань та інтерфейси користувача;

– центр управління для прийняття рішень і візуалізації KPI.

Далі розглянута математична модель моніторингу інфраструктури ІКС каналами передачі 5G.

Формалізовану модель оцінки стану моніторингу можна представити у вигляді оцінки ризику перевищення порогових значень, яка здійснюється за допомогою ймовірнісної функції:

$$P_{alert}^{(i)} = \mathbb{P}\left(S_i(t) > T_{thr}^{(i)}\right), \quad (15)$$

де:

– $P_{alert}^{(i)}$ - ймовірність спрацювання тривоги для *i*-го сенсора або каналу;

– $S_i(t)$ - поточне значення контрольованого параметра сенсора *i* (наприклад, температура, тиск, вібрація, навантаження) в момент часу *t*;

– $T_{thr}^{(i)}$ - порогове значення, яке визначає критичний стан для відповідного параметра;

– $\mathbb{P}$ – оператор ймовірності.

– Δt - інтервал між циклами моніторингу.

– $f(S_i(t))$-функція оцінки стану параметра (наприклад, стохастична оцінка або нечітка логіка).

Оцінка загального ризику відхилень:

$$R_{total}(t) = \sum_{i=1}^{n} \omega_i \cdot P_{alert}^{(i)}, \quad (16)$$

де ω_i – ваговий коефіцієнт критичності параметра *i*.

Таким чином опис модель буде мати наступний вигляд:

– сенсорна мережа формує потік даних $S_i(t)$ з об'єктів моніторингу;

– 5G-канали забезпечують передачу даних з мінімальною затримкою та високою пропускною здатністю;

– хмарна та периферійна обробка виконує фільтрацію, нормалізацію та оцінку $P_{alert}^{(i)}$

– система прийняття рішень**:** реагує на перевищення порогів, активуючи відповідні сценарії керування.

Інформаційний потік у системі буде мати вигляд (табл. 2):

Таблиця 2

Інформаційний потік у системі

Операція	**Елемент системи**
Збір інформації	IoT сенсори
Транспорт	5G backhaul транспорт
Обробка	Edge/Cloud обчислення
Аналіз КПІ	Обробка в реальному часі

Реакція	Нотифікація,автозупинка, переналаштування

Таким чином впровадження моделі ІКС на базі 5G дає можливість:

– реалізувати реальний моніторинг стану процесів з мінімальною затримкою;

– робить можливою інтеграцію з AI-модулями та прогнозними моделями забезпечує превентивне виявлення інцидентів;

– забезпечує гнучкість розгортання (Edge та Cloud) для об'єктів з обмеженою інфраструктурою.

Інтеграція кіберзахисту в хмарно-орієнтовану архітектуру критичної інфраструктури

В умовах гібридної війни та цифрової трансформації державного управління особливої важливості набуває забезпечення інформаційної безпеки технологічних процесів, що реалізуються за допомогою хмарних технологій. Передавання, обробка і зберігання даних у хмарному середовищі потребує застосування багаторівневих моделей кіберзахисту, здатних протистояти як зовнішнім загрозам (APT, DDoS, фішинг), так і внутрішнім (інсайдерські загрози, неправильна конфігурація доступу).

Захищений обмін даними є критично важливою вимогою для будь-якої ІКС у сфері критичної інфраструктури. В умовах гібридної війни, кібератаки на об'єкти КІ стали не винятком, а постійною загрозою. У зв'язку з цим, інтеграція повнофункціональної системи кіберзахисту є обов'язковим компонентом запропонованої методології.

Архітектура системи кіберзахисту реалізується на основі концепції Defense-in-Depth, яка включає:

– Шифрування трафіку (TLS 1.3, IPSec, VPN tunnels);

– Сегментацію мережі (Zero Trust Architecture);

– Інтрузійно-детекційні системи (IDS) на рівні 5G/Edge;

– Багатофакторну автентифікацію (MFA) для всіх рівнів доступу;

– SIEM-системи для збору та аналізу логів. Методологією запропонована багаторівнева модель кіберзахисту в ІКС (рис. 8)

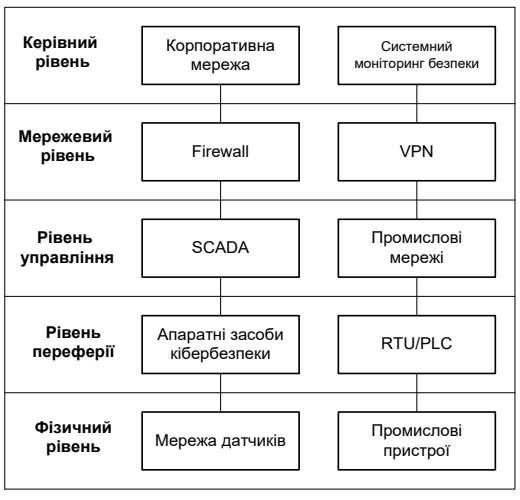

Рис. 8. Багаторівнева модель кіберзахисту в ІКС

Кібербезпека є ключовим елементом у захисті технологічних процесів критичної інфраструктури (КІ), особливо в умовах використання хмарних технологій, що відкривають нові вектори атак.

Для гарантування цілісності, конфіденційності та доступності даних в умовах розподіленої хмарної архітектури необхідна інтегрована система кіберзахисту з адаптивними механізмами реагування на загрози.

Структурна схема архітектури інтегрованої системи кіберзахисту (ІСК) має наступний вигляд (рис. 9):

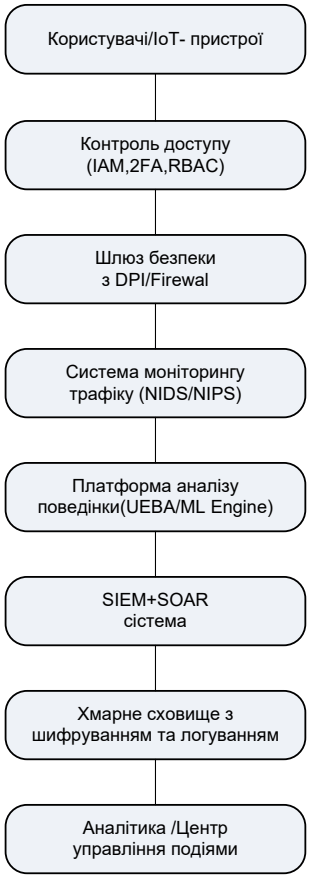

Рис. 9. Структурна схема архітектури інтегрованої системи кіберзахисту

Формалізована модель безпеки хмарної системи в якості оцінки ризику має вигляд:

$$R = \sum_{i=1}^{n} P_i \cdot I_i \,, \tag{17}$$

де:

– P_i – імовірність виникнення і-ої загрози

– I_i - вплив загрози на систему

Математична формалізація для процесу шифрування даних (наприклад, AES) може мати наступний вигляд:

$$C = E_K\left(M\right), \tag{18}$$

де:

– M – повідомлення;

– K – ключ шифрування;

– E_K – функція шифрування;

– C – зашифрований текст.

Таким чином, аналізуючи вищенаведене, можна зробити висновки про те, що інтеграція системи кіберзахисту повинна і буде забезпечувати:

– превентивне виявлення підозрілої активності;

– реагувати на інциденти у реальному часі;

– забезпечувати безпеку конфіденційних даних при зберіганні та передачі;

– відповідати міжнародним вимогам (ISO 27001, NIST CSF, OWASP Cloud Top 10).

Модель оцінки кіберризиків можна описати через оцінку ризику на основі моделі, наприклад, STRIDE та DREAD:

STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege,тоді DREAD буде:

$$R = \frac{(D + R + E + A + D)}{5}, \qquad (19)$$

де:

– D – шкода (Damage Potential),

– R – відтворюваність (Reproducibility),

– E – експлуатація (Exploitability),

– A – вплив на користувачів (Affected Users),

– D – виявлення (Discoverability).

Формалізована модель безпеки хмарної системи матиме, в свою чергу, представлення, де у якості ядра ІСКЗ пропонується реалізувати нейромережевий класифікатор атак.

Схема інтеграції системи кіберзахисту представлена на рис. 10.

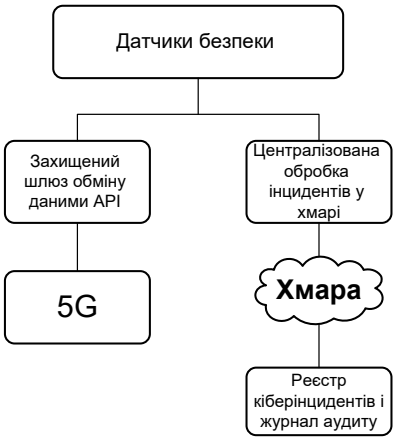

Рис. 10. Ілюстрація схеми інтеграції системи кіберзахисту в ІКС

Схема включає:

– Датчики безпеки на рівні 5G-мережі, що фіксують аномалії, трафік, вторгнення.

– Захищені шлюзи обміну даними (API), які шифрують і фільтрують трафік між компонентами системи.

– Централізована обробка інцидентів у хмарі – ядро логіки аналізу та реагування.

– Реєстр кіберінцидентів і журнал аудиту – системи обліку, розслідувань і форензики.

На базі системи кіберзахисту в ІКС, як приклад, розроблено сценарій реагування атаки типу "man-in-the-middle" .

Атака "людина посередині" (Man-in-the-Middle, MitM) (рис. 11) передбачає перехоплення, підміну або зміну даних, що передаються між двома сторонами (наприклад, між клієнтом і сервером). Зловмисник стає невидимим посередником, який може читати, змінювати або підмінювати інформацію в режимі реального часу.

Таким чином, сценарій реагування на атаку MitM буде мати наступний вигляд (табл. 3).

Таблиця 3

Сценарій реагування на атаку MitM

Компонент	**Функція**
Користувач	Жертва атаки, що не підозрює про перехоплення
Зловмисник (MitM)	Проникає в канал між користувачем і сервером
Snort IDS	Аналізує трафік на стороні сервера або у DMZ, детектує аномалії
WAF	Захищає веб-сервіси і автоматично блокує підозрілий трафік
SIEM	Отримує інформацію з усіх джерел, проводить аналіз, готує інцидент
CERT	Проводить подальшу відповідь, формує реакцію і звіт

Спираючись на аналіз системи КЗ та разробленого сценарію реагування на атаку MitM можна зробить наступні висновки:

– Автоматизація реагування дозволяє скоротити час між атакою та нейтралізацією.

– Інтеграція систем IDS → WAF → SIEM → CERT – ознака вдалого рішення архітектури кіберзахисту.

– Реєстр інцидентів дозволяє відстежувати історію атак і готуватися до майбутніх загроз.

– Для забезпечення цілісності та довіри до даних у хмарних середовищах необхідно використовувати модульну систему кіберзахисту;

– Доцільно також використовувати глибоку інтеграцію засобів SIEM + ML + SOC;

– Рекомендується, крім цього, формування локального профілю загроз для кожного об'єкта критичної інфраструктури;

– Необхідним є врахування вимог ЗУ "Про основні засади забезпечення кібербезпеки України".

Таким чином, інтеграція спроектованої системи кіберзахисту дозволяє:

– превентивно виявляти підозрілу активність;

– реагувати на інциденти у реальному часі;

– забезпечити безпеку конфіденційних даних при зберіганні та передачі;

– відповідати міжнародним вимогам (ISO 27001, NIST CSF, OWASP Cloud Top 10).

Рис. 11. Реалізація атаки MitM

Висновки

В даній роботі були отримані наступні результати:

1. Запропоновано архітектуру хмарно-орієнтованої платформи, яка забезпечує підтримку критичних технологічних процесів.

2. Розроблено метод оптимізації параметрів технологічного процесу з урахуванням KPI та обмежень середовища.

3. Запропоновано підхід до моніторингу в режимі реального часу на основі KPI та 5G-сенсорної інфраструктури.

4. Розроблено інтелектуальний модуль DSS, що взаємодіє з CAD/CAM/ERP-системами.

5. Впроваджено моделі для аналізу вразливостей та кіберзагроз, а також побудови модулю кіберзахисту.

На основі узагальнення результатів дослідження, запропоновано комплексну методологію підтримки технологічних процесів KI на базі хмарних технологій. Методологія включає в себе визначення набору KPI, побудову хмарної архітектури, інтелектуальне управління та кіберзахист. При цьому, особливу увагу приділено практичним компонентам: базі знань, інтеграції з CAD/SCADA, застосуванню 5G в якості комунікаційної платформи. Запропонована хмарно-орієнтована методологія охоплює весь життєвий цикл підтримки технологічних процесів – від вибору методу до забезпечення безпечного обміну даними. Модель базується на системному підході, який враховує як технічні, так і організаційні аспекти. Особливу увагу приділено адаптивності, оптимізації рішень, використанню штучного інтелекту, а також відповідності вимогам безпеки та надійності.

7. Розроблена методологія надала змогу:

– Підвищити ефективність технологічних процесів в умовах обмежених ресурсів;

– Забезпечити гнучкість та масштабованість IT-інфраструктури;

– Забезпечити проактивну безпеку при обміні даними між критичними системами;

– Надати інструменти візуалізації, аналітики та прийняття рішень для операторів і аналітиків.

Література

[1] Saaty T.L. Decision Making with the Analytic Hierarchy Process. Int. J. Services Sciences, 2008.

[2] Turban, E., Sharda, R., & Delen, D. (2011). Decision Support and Business Intelligence Systems (9th ed.). Pearson Education.

[3] Bellman, R.E., Zadeh, L.A. Decision-Making in a Fuzzy Environment. Management Science, 1970.

[4] Bazaraa M. S., Jarvis J. J., Sherali H. D. Linear Programming and Network Flows, Wiley, 2010.

[5] Giarratano J., Riley G. Expert Systems: Principles and Programming. Cengage Learning, 2004.

[6] Russell S., Norvig P. Artificial Intelligence: A Modern Approach, 3rd ed.

[7] Hevner A.R., March S.T., Park J., Ram S. Design Science in Information Systems Research, MISQ, 2004.

[8] Kaplan R. S., Norton D. P. The Balanced Scorecard – Measures then drive Performance // Harvard Business Review,- 1992

[9] Інтелектуальна система керування мережею для вирішення проблеми автономного моніторингу 5G-технологій / Колектив авторів. Київ: ДУТ, 2021. 6 с. Режим доступу: https://con.dut.edu.ua/index.php/communication/article/download/2515/2418

[10]Gnatyuk S., Yudin O., Sydorenko V., Smirnova T., Polozhentsev A., The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems, CEUR Workshop Proceedings, 2022, vol. 3156, pp. 390-399.

[11]Gnatyuk S., Berdibayev R., Smirnova T., Avkurova Z., Iavich M. Cloud-Based Cyber Incidents Response System and Software Tools, Communications in Computer and Information Science, Vol. 1486, pp. 169-184, 2021.

[12]Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

[13]Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622

[14]Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications,* 2025. 202-229

[15]Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings,* 2024, 3909, pp. 227–241.

[16]Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56

[17]Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265

УДК 004

Smirnova T.,** Usik **P.,** Lysenko **I., Buravchenko K., Smirnov O. Methodology for supporting technological processes in critical infrastructure with information security based on cloud technologies

Abstract. *This article proposes a methodology for supporting technological processes in critical infrastructure based on cloud technologies. The critical infrastructure of the state requires new approaches to ensure reliability, adaptability and information security of technological processes. At the same time, cloud technologies open up new opportunities for scalable monitoring, analysis and management of critical infrastructure in conditions of hybrid threats. Thus, the proposed methodology is aimed at forming an integrated digital platform based on the use of cloud technologies for monitoring, analysis and automated management of technological processes in conditions of high risks. The purpose of the developed methodology is to ensure continuous, safe and stable operation of technological processes of critical infrastructure facilities of the state through the implementation of cloud technologies for monitoring, analysis and automated management in conditions of high risks. The main task of this methodology is to develop a comprehensive architecture for supporting technological processes of critical infrastructure based on cloud solutions, increasing the level of technological readiness of critical infrastructure facilities for functioning in an unstable environment by implementing adaptive, scalable and secure solutions. The methodology proposed in this work is focused on functioning in conditions of increased threats, both man-made and cyber, taking into account the requirements for information security, communication reliability, redundancy of critical components and flexibility of the system architecture. This approach contributes to increasing the level of technological readiness of critical infrastructure objects to operate in an unstable environment, reduces the likelihood of failures and ensures resistance to external influences.*

Keywords: *technological processes, critical infrastructure, cloud technologies, artificial intelligence, knowledge base, 5G, modeling, vulnerability analysis, cyber threats, cybersecurity, Internet of Things, CAD/CAM/ERP, CAD/SCADA, 5G, IT infrastructure, decision support systems, objective function, KPI, performance indicators, intelligent management*

Смірнова Тетяна Віталіївна, к.т.н., старший викладач кафедри автоматизації виробничих процесів Центральноукраїнського національного технічного університету,
Tetiana Smirnova, Candidate of Science (Engineering), Senior Lecturer, Department of Automation of Production Processes, Central Ukrainian National Technical University

Усік Павло Сергійовий, доктор філософії (PhD), старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.
Pavlo Usik, Doctor of Philosophy (PhD), senior lecturer of Cybersecurity & Software Academic Department,Central Ukrainian National Technical University

Лисенко Ірина Анатоліївна, к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського
національного технічного університету.
Iryna Lysenko, Ph.D., Senior Lecturer at the Department of Cybersecurity and Software of the Central Ukrainian National Technical University.

Буравченко Костянтин Олегович, доцент, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет
Kostiantyn Buravchenko – associate professor, candidate of technical sciences, Associate Professor of Cybersecurity & Software Academic Department, Central Ukrainian National Technical University

Смірнов Олексій Анатолійович, професор, доктор технічних наук, завідувач кафедри кібербезпеки та програмного забезпечення, Центральноукраїнський національний технічний університет
Oleksii Smirnov – professor, Doctor of technical sciences, head of Cybersecurity & Software Academic Department, Central Ukrainian National Technical University, Kropyvnytskyi