Володимир КИСЕЛЬОВ,
доктор технічних наук, професор,
директор навчально-наукового інституту
муніципального управління та міського господарства
Таврійського національного університеті імені В. І. Вернадського
м. Київ, Україна
ORCID: https://orcid.org/0000-0003-3437-2825,
e-mail: kvbglush1953@gmail.com

Сергій ЧУМАЧЕНКО,
доктор технічних наук, с.н.с.,
провідний науковий співробітник
Державного науково-дослідного інституту авіації,
м. Київ, Україна
ORCID: https://orcid.org/0000-0002-8894-4262,
e-mail: s_chum@ukr.net

Олександр ГУЙДА,
кандидат наук з державного управління, професор,
завідувач кафедри комп'ютерних та інформаційних технологій
Навчально-наукового інституту
муніципального управління та міського господарства
Таврійського національного університеті імені В. І. Вернадського
м. Київ, Україна
ORCID: https://orcid.org/0000-0002-2019-2615,
e-mail: guydasg@ukr.net

DOI: https://doi.org/10.32620/pls.2025.8.57

РОЗРОБКА АРХІТЕКТУРИ СИТУАЦІЙНОГО ЦЕНТРУ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: *У статті розглянуто концепцію створення ситуаційного центру для забезпечення резильєнтності критичної енергетичної інфраструктури. Запропоновано архітектурну модель, яка поєднує сучасні технології моніторингу, аналізу даних та управління ризиками. Визначено ключові функціональні модулі центру, їх взаємодію та роль у підвищенні стійкості енергетичних систем до зовнішніх та внутрішніх загроз.*

Ключові слова: *резильєнтність, критична інфраструктура, енергетика, ситуаційний центр, кібербезпека, управління ризиками.*

Критична енергетична інфраструктура є основою функціонування економіки та національної безпеки. В умовах зростання кіберзагроз, фізичних атак у вигляді ракетно-дронових ударів рф та природних катастроф виникає потреба у створенні спеціалізованих ситуаційних центрів, здатних забезпечити оперативне реагування та довгострокову резильєнтність систем.

Метою дослідження є розробка архітектури ситуаційного центру, який інтегрує інструменти моніторингу, прогнозування та управління для захисту енергетичних об’єктів (рис. 1).

Резильєнтність визначається як здатність системи протистояти деструктивним впливам, швидко відновлюватися та адаптуватися до нових умов.

Для енергетичної інфраструктури це означає: мінімізацію часу простою; збереження критичних функцій; адаптацію до змін у середовищі загроз.

До складу архітектури ситуаційного центру входять такі основні компоненти:

1. Модуль збору даних

сенсори та SCADA-системи;

інтеграція з кібермоніторингом;

канали отримання інформації від зовнішніх джерел (метео, розвідка, соціальні мережі).

2. Аналітичний модуль

системи штучного інтелекту для прогнозування ризиків;

моделі оцінки вразливостей;

симуляції сценаріїв розвитку кризових ситуацій.

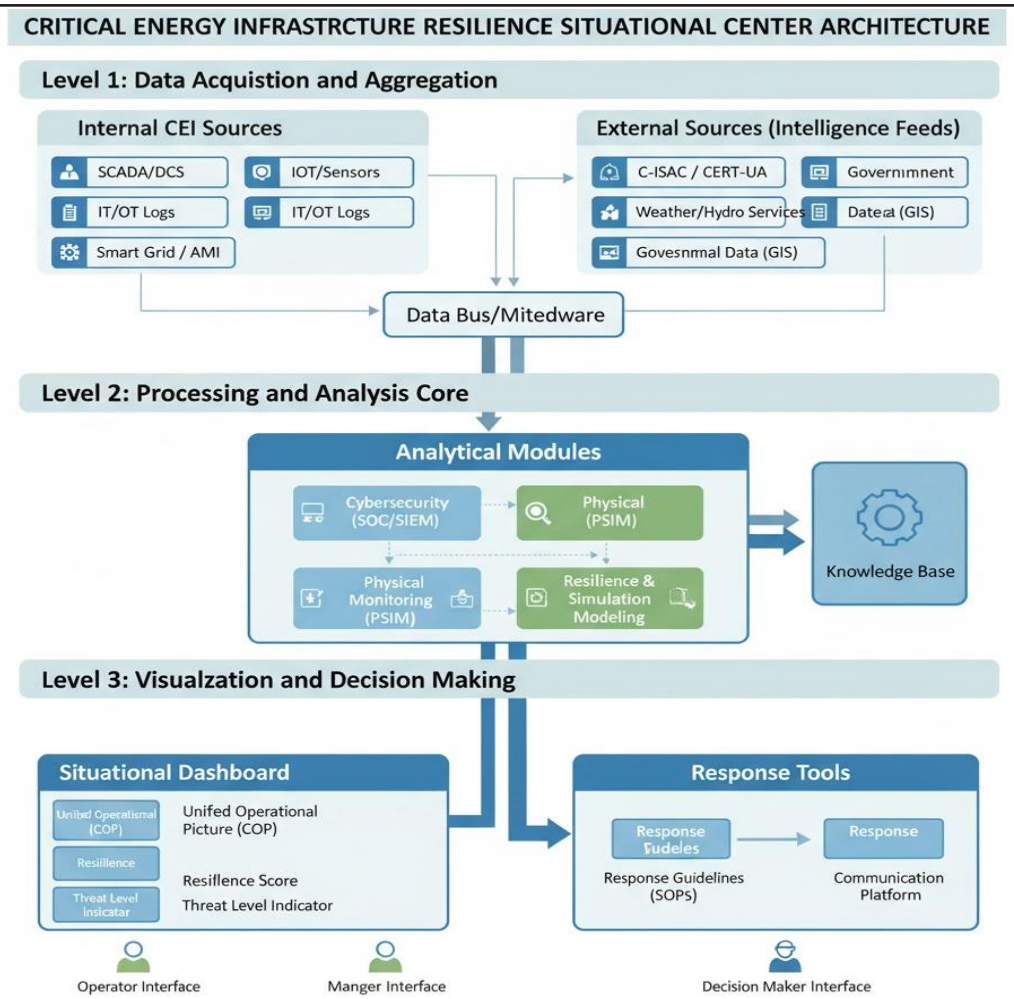

Рис.1. Архітектура Ситуаційного центру забезпечення резильєнтності критичної енергетичної інфраструктури

3. Модуль управління інцидентами

автоматизовані протоколи реагування;

координація дій між операторами та державними структурами;

підтримка прийняття рішень у реальному часі.

4. Комунікаційний модуль

захищені канали зв'язку;

інтеграція з міжнародними енергетичними центрами;

інтерфейси для взаємодії з громадськістю.

5. Модуль навчання та симуляцій

тренажери для персоналу;

моделювання кризових сценаріїв;

оцінка ефективності заходів резильєнтності.

На рівні 1 здійснюється збір та агрегація даних (data acquisition and aggregation). Цей рівень виконує функцію **сенсорного поля** СЦ, забезпечуючи постійний приплив різнорідної інформації.

Системи всередині енергетичної мережі (SCADA/DCS, IT/OT Logs, IoT/Сенсори, Smart Grid / AMI) безперервно генерують дані про поточні операційні параметри, стан обладнання та мережеву активність. Це дані **операційного рівня**.

Збирається інформація від зовнішніх партнерів (CERT-UA, Державні Органи, Метео/Гідрослужби) та геопросторові дані (GIS). Це дані **рівня загроз та контексту.**

Всі зібрані дані, які часто мають різні формати, проходять через централізовану шину. Шина **нормалізує та агрегує** ці потоки, забезпечуючи єдиний стандартизований інтерфейс для подальшої обробки на Рівні 2.

Ядро СЦ перетворює зібрані сирі дані на **ситуаційну поінформованість** та інтелектуальні висновки.

Аналітичні Модулі (Analytical Engines) включають до свого складу:

Cybersecurity (SOC/SIEM) та Physical Monitoring (PSIM): Ці модулі працюють паралельно, аналізуючи внутрішні та зовнішні дані в реальному часі. SOC/SIEM виявляє кібераномалії (наприклад, несанкціонований доступ або зловмисну активність в OT-мережі), тоді як PSIM об'єднує сенсорні та відеодані для виявлення фізичних загроз (наприклад, проникнення на об'єкт).

Прогностична Аналітика: Використовує моделі машинного навчання для прогнозування потенційних відмов обладнання до того, як вони

відбудуться, або ймовірності атаки на основі зовнішніх загроз.

Моделювання Резильєнтності (Resilience & Simulation): Це ключовий модуль. Він бере поточну ситуацію, моделює вплив виявленої чи потенційної відмови (наприклад, втрата трансформатора або кібератака на контролер) і оцінює здатність мережі продовжувати роботу (резильєнтність), а також визначає найшвидший шлях відновлення.

База Знань та Патернів (Knowledge Base): Результати аналізу (інциденти, патерни атак) та стандартні операційні процедури (SOPs) зберігаються тут. Ця база слугує зворотним зв'язком, навчаючи аналітичні модулі та інструменти реагування на основі історичного досвіду.

Рівень 3 Представлення та Прийняття Рішень (Visualization and Decision Making) забезпечує керівництво та операторів концентрованою інформацією для швидкого та ефективного реагування.

Ситуаційна Панель (Dashboard): Представляє Єдину Операційну Картину (COP), де всі кібер-, фізичні та операційні дані інтегровані на географічній основі (GIS). Найважливішим показником є Рівень Резильєнтності (Resilience Score) та Індикатор Рівня Загрози (Threat Level Indicator), які кількісно відображають загальну стійкість КЕІ.

Інструменти Реагування (Response Tools): СЦ переходить від аналізу до дії. На основі висновків Моделювання Резильєнтності (Рівень 2) автоматично генеруються Керівництва по Реагуванню (SOPs) та Плани Дій, які є найкращими рекомендаціями для персоналу.

Комунікаційна Платформа: Забезпечує негайний захищений зв'язок з бригадами, аварійними службами та вищим керівництвом/державними органами для координації відновлювальних робіт.

Схема демонструє, що СЦ функціонує як замкнутий цикл. Дані (Рівень 1) живлять аналіз та моделювання (Рівень 2), що призводить до обґрунтованих рішень та дій (Рівень 3), які, у свою чергу, впливають на стан КЕІ, забезпечуючи її стійкість.

Висновки. Запропонована архітектура ситуаційного центру є комплексним рішенням для забезпечення резильєнтності критичної енергетичної інфраструктури. Її впровадження дозволить створити адаптивну систему управління, здатну ефективно протидіяти сучасним загрозам та забезпечувати безперервність енергопостачання.

Очікувані результати від впровадження цієї архітектури:

Підвищення стійкості енергетичних систем до кібер- та фізичних атак.

Зменшення часу реагування на інциденти.

Формування єдиної інформаційної екосистеми для управління ризиками.

Підготовка персоналу до роботи в умовах кризових ситуацій.

Бібліографічні посилання

1. Кисельов В.Б., Морщ Є.В., Чумаченко С.М., Гуйда О.Г., Ромащенко Р.А. Модель попередження надзвичайних ситуацій в системі підтримки прийняття рішень на об’єктах критичної інфраструктури. Вчені записки Таврійського національного університету імені В. І. Вернадського", серія "Технічні науки": зб. наук. праць. Одеса. Видавничий дім «Гельветика» Том 36 (75) № 2 2025 Частина 2. С 94-103. DOI: https://doi.org/10.32782/2663-5941/2025.2.2/13

V. Kiselyov, S. Chumachenko, O. Guyda

Development of the architecture of a situational center to ensuring resilience of critical energy infrastructure.

Abstract: The article considers the concept of creating a situational center to ensure the resilience of critical energy infrastructure. An architectural model is proposed that combines modern technologies for monitoring, data analysis and risk management. The key functional modules of the center, their interaction and role in increasing the resilience of energy systems to external and internal threats are identified.

Keywords: resilience, critical infrastructure, energy, situational center, cybersecurity, risk management.

Зразок для цитування:

Кисельов В., Чумаченко С., Гуйда О. Розробка архітектури ситуаційного центру забезпечення резильєнтності критичної енергетичної інфраструктури. Пропілеї права та безпеки, 2025. №8. С. 226-228. DOI: https://doi.org/10.32620/pls.2025.8.57.