КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.962
УДК 004.6

Смірнова Тетяна Віталіївна
кандидат технічних наук,
доцент кафедри кібербезпеки та програмного забезпечення
Центрально український національний технічний університет, Кропивницький, Україна
ORCID: 0000-0001-6896-0612
sm.tetyana@gmail.com

ДОСЛІДЖЕННЯ МЕТОДІВ, МОДЕЛЕЙ ТА СУЧАСНИХ ІТ-РІШЕНЬ ДЛЯ ПІДТРИМКИ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ ДЕРЖАВИ

Анотація. У роботі проаналізовано критичну інфраструктуру в Європі, Азії, США та Україні (поняття, структура, загрози і виклики). Визначено, що в умовах кіберзагроз, глобальної цифровізації та необхідності оперативного реагування на надзвичайні ситуації виникає потреба у використанні сучасних методів і моделей підтримки технологічних процесів, які забезпечують гнучкість, масштабованість та високий рівень надійності. Визначено, сучасна підтримка технологічних процесів базується на поєднанні хмарних технологій, IIoT, цифрових двійників, аналітики великих даних та кіберзахисту, управління підприємством критичної інфраструктури, інтегрованих у єдину інфраструктуру інформаційно-комунікаційних технологій на основі сучасних мережевих протоколів. Для підприємств критичної інфраструктури основним критерієм відбору ІТ-рішень є забезпечення безперервності та стійкості технологічних процесів при одночасному дотриманні вимог надійності, безпеки (конфіденційності, цілісності, доступності (КДЦ)), масштабованості та економічної ефективності. Наведено основні методи та моделі підтримки (управління, моніторингу, оцінювання ефективності) технологічних процесів, визначені в результаті аналізу сучасних наукових публікацій та дослідницьких проєктів за напрямком підтримки технологічних процесів у критичній інфраструктурі. Встановлено, що не зважаючи на велику кількість наукових досліджень у цьому напрямку, залишається низка невирішених завдань, які потребують вирішення.

Ключові слова: безпека критичної інфраструктури**,** інформаційні технології, технологічні процеси, Інтернет речей, вимоги безпеки, вимоги надійності

ВСТУП

Постановка завдання дослідження

Останні десятиріччя характеризуються стрімким зростанням складності та взаємозалежності технологічних процесів (ТП) у критичній інфраструктурі (КІ) держави безпосередньо впливає на національну безпеку, економіку та соціальну стійкість. В умовах кіберзагроз, глобальної цифровізації та необхідності оперативного реагування на надзвичайні ситуації виникає потреба у використанні сучасних методів і моделей підтримки ТП, які забезпечують гнучкість, масштабованість та високий рівень надійності.

Постановка проблеми. Хмарні технології (ХТ) [4, 5] поступово стають ключовим інструментом модернізації КІ завдяки своїй здатності забезпечувати централізоване зберігання та обробку даних, інтеграцію розподілених систем і підвищення рівня

© Т.В. Смірнова, 2025

кібербезпеки [6]. Вони дозволяють реалізувати адаптивні механізми управління ТП, застосовувати алгоритми штучного інтелекту (ШІ, AI) для аналізу великих масивів даних Це відкриває нові можливості для побудови інтелектуальних систем підтримки прийняття рішень (СППР) у КІ. Разом з тим, впровадження ХТ в КІ супроводжується низкою викликів, серед яких – забезпечення конфіденційності (К), цілісності (Ц), доступності (Д) даних, сумісність із наявними апаратно-програмними комплексами наукових досліджень є систематизація та аналіз існуючих підходів, моделей і методів підтримки ТП на основі ХТ, з метою виявлення їх переваг, обмежень і перспектив подальшого розвитку.

Аналіз останніх досліджень і публікацій. У роботах [8, 9] розглянуті питання критичної інфраструктури США, у роботах [10, 11] розглянуті питання критичної інфраструктури Європи, у роботах [21, 22] розглянуті питання критичної інфраструктури Великої Британії, у роботах [12-20] розглянуті питання критичної інфраструктури країн Азії. Робота [24] присвячена виокремленню секторів критичної структури України. У роботах [25-27] виділяються особливості формування і захисту критичної структури України. Роботи [28-34] присвячені ІТ-рішенням для підтримки технологічних процесів у критичній інфраструктурі держави та методам й моделям підтримки технологічних процесів.

Метою даної статті є дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави та визначення актуальних напрямків подальших досліджень на основі проведеного аналізу.

Об’єктом дослідження є процес формування методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави.

Предметом дослідження є методи, моделі та ІТ-рішення для підтримки технологічних процесів у критичній інфраструктурі держави.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Критична інфраструктура в США, Європі, Азії та Україні: поняття, структура, загрози і виклики

Під КІ у світі зазвичай розуміють системи, мережі та послуги, збій яких спричиняє суттєвий вплив на безпеку, економіку, здоров’я чи добробут населення. У підходах останніх років помітна еволюція від суто «об’єктного» захисту до керування ризиками для взаємопов’язаних кібер-фізичних систем і їхніх ланцюгів постачання.

США

Наприклад, у США цей підхід формалізовано як партнерську модель держави й операторів для 16 визначених секторів [8]. У США в квітні 2024 р. видано National призначив за кожним «агентства з управління ризиками сектору» (SRMA) та підкреслив рух до мінімальних обов’язкових вимог безпеки там, де добровільні підходи не спрацьовують. Практична реалізація залишається партнерською: CISA координує оцінку ризиків, обмін інформацією та галузеві настанови для оператора інфраструктури. Сучасна модель США відзначається жорсткішим регулюванням, переходом від добровільних стандартів до обов’язкових, широким використанням інновацій і акцентом на колективну відповідальність бізнесу та держави у сфері захисту КІ. Особливістю

підходу є модель розподіленої відповідальності: уряд встановлює рамкові стандарти та координує реагування, але значна частина CNI перебуває у приватній власності, і саме приватні компанії несуть головну відповідальність за безпеку. Для цього створено систему Information Sharing and Analysis Centers (ISACs) та Public-Private Partnerships , які забезпечують обмін інформацією між урядом і бізнесом.

Європа

У Європі рамку задають дві взаємодоповнювальні директиви: NIS2 (кіберстійкість мереж і інформаційних систем) [10] та CER (фізична/операційна стійкість критичних суб'єктів) [11]. Держави-члени мали транспонувати NIS2 до 17 жовтня 2024 р., розширивши коло «суттєвих» й «важливих» організацій у секторах від енергетики й транспорту до охорони здоров'я, водопостачання, ІКТ та державного управління. Директива CER застосовується з жовтня 2024 р. і зобов'язує до липня 2026 р. ідентифікувати критичних суб'єктів в 11 секторах та вимагати від них оцінок ризиків і заходів стійкості.

У Великій Британії система захисту національної КІ (CNI) координується на найвищому державному рівні через Національний центр кібербезпеки (NCSC), який є підрозділом розвідслужби GCHQ та відповідає за розробку політик, реагування на кіберінциденти й підтримку операторів критичних секторів. До CNI віднесено 13 секторів, серед яких енергетика, транспорт, фінанси, охорона здоров'я, вода, телекомунікації, урядові послуги, оборона та продовольча безпека. Законодавчу основу становлять Investigatory Powers Act (2016) [21], UK National Cyber Strategy (2022-2030) [22] та нормативні акти в межах National Security and Investment Act (2021) [23], що передбачають жорсткі вимоги до кіберзахисту, аудитів і управління ризиками. Британська модель вирізняється поєднанням централізованої координації та децентралізованої відповідальності: кожен оператор CNI зобов'язаний самостійно забезпечувати кіберзахист згідно з вимогами NCSC, але отримує підтримку від держави у вигляді методологій, аналітики та сервісів кіберрозвідки. Важливою особливістю є активна взаємодія з приватним сектором і створення Public-Private Partnerships (PPP) для обміну інформацією про загрози. Крім того, Велика Британія інвестує у системи AI/ML та big data для прогнозування атак і підвищення кіберстійкості, а також має сильний акцент на міжнародному співробітництві в межах НАТО, ЄС (попри Brexit у сфері кібербезпеки зберігається співпраця) та «Five Eyes». Унікальною рисою британського підходу є орієнтація на довіру й прозорість, де оператори CNI зобов'язані ділитися з державою реальними даними про кіберінциденти, що дозволяє будувати спільну стратегію протидії загрозам.

Азія

Підходи в Азії неоднорідні, але тренд схожий – у пріоритеті критичні інформаційні інфраструктури (КІІ) і регуляторний нагляд за операторами:

–***у Сінгапурі*** Cybersecurity Act (оновлення 2024 р.) [12] створює режим для операторів КІІ в 11 секторах (енергетика, водопостачання, охорона здоров'я, фінанси, транспорт, інформаційні комунікації, урядові послуги, безпека, а також медіа та космічні технології) із повноваженнями агентства CSA щодо запобігання та реагування. Сінгапурська модель базується на принципах жорсткого регулювання, технологічної інноваційності та партнерства з приватним сектором, при цьому особливий акцент робиться на розбудові національних SOC, систем раннього попередження та обміні даними про загрози. Важливою особливістю є інтеграція кіберзахисту в загальну стратегію розвитку «Smart Nation», де КІ розглядається як фундамент цифрової економіки та смарт-сервісів для населення. Унікальною рисою підходу Сінгапуру є

проактивна політика кіберстійкості, що включає моделювання кібератак, обов'язкові навчання для державних і приватних структур, а також масштабні програми з підготовки кадрів у сфері кібербезпеки;

–***в Індії*** визначення КІІ [13] закріплене в ІТ-Акті 2000 (ст. 70) [14]; національний центр NCIIPC виділяє сфери енергетики, телекомунікацій, банківської та фінансової системи, транспорту, урядових мереж, космічних та оборонних технологій, а також охорони здоров'я. Індійська модель базується на принципах централізованого державного контролю та міжвідомчої координації, проте активно залучає приватний сектор до партнерства через обов'язкову сертифікацію систем, аудит безпеки та обмін інформацією про інциденти. Особливий акцент робиться на розбудові національних центрів моніторингу й реагування (CERT-In), що відповідають за обробку кіберінцидентів, а також на розвитку нормативної бази, включно із законом [14]. Унікальною рисою індійського підходу є поєднання політики цифрової трансформації з масштабними державними програмами (Digital India, Smart Cities Mission), де КІ розглядається не лише як об'єкт захисту, а й основою соціально-економічного розвитку;

–***у Японії*** захист КІ координується на державному рівні через Національний центр готовності до інцидентів та стратегії кібербезпеки (NISC) [15], який підпорядковується Кабінету міністрів і відповідає за формування політики, оцінку ризиків та координацію між державними органами й приватними операторами. Офіційно виділено 14 секторів КІ, серед яких енергетика, транспорт, фінанси, інформаційні комунікації, медицина, водопостачання, урядові системи тощо. Японська модель вирізняється добровільно-обов'язковим підходом, коли держава встановлює рамкові вимоги та рекомендації, а приватні оператори зобов'язані реалізовувати заходи безпеки через механізм саморегуляції та партнерства. Важливою особливістю є тісний зв'язок із концепцією акцентом на стійкість і відновлення роботи систем після інцидентів. Крім того, Японія активно впроваджує AI, IoT та XT у моніторинг і управління інфраструктурою, розвиваючи пілотні проекти в галузі смарт-міст, енергетичних мереж і транспортних систем. Усе це робить японську модель CIP унікальною комбінацією державної координації, приватної відповідальності та технологічних інновацій;

–***у КНР*** поняття КІІ закріплене в Законі про кібербезпеку (Cybersecurity Law, 2017 [16]) та розвинуте в Regulations on the Security Protection of Critical Information Infrastructure (2021) [17]. Відповідно до цих документів, КІІ охоплює інформаційні системи та сервіси в сферах публічних комунікацій, енергетики, транспорту, фінансів, державного управління, оборони, науки і техніки, охорони здоров'я та інших, що мають значення для національної безпеки та суспільного добробуту. Китайська модель відрізняється від європейської та американської більш централізованим і директивним характером що поєднується з політикою «кіберсуверенітету», яка надає державі широкі повноваження щодо регулювання та моніторингу всього національного кіберпростору. З практичного боку, КНР робить наголос на поєднанні традиційної фізичної безпеки з кіберзахистом та активно впроваджує інструменти AI, Big Data та XT у моніторинг КІ. Це створює потужну, але вкрай закриту для міжнародного співробітництва систему, що відображає специфіку китайської державної моделі управління;

–***у Республіці Корея*** захист КІ здійснюється в межах комплексної системи національної кібербезпеки, координованої Національним агентством розвідки (NIS) та Міністерством науки і ІКТ, що відповідають за політику у сфері кіберзахисту, кіберінцидентів та безперервності роботи стратегічних об'єктів. До секторів КІ віднесено енергетику, транспорт, фінансові системи, телекомунікації, урядові й оборонні

мережі, медицину та виробничі підприємства, причому велика увага приділяється кіберзагрозам проти високотехнологічної промисловості та індустрії напівпровідників. Корейська модель відрізняється високим рівнем цифрової інтеграції: тут широко застосовуються системи моніторингу в режимі реального часу, AI та Big Data для аналізу кіберзагроз і прогнозування атак. Законодавчу основу становить Framework Act on National Informatization [18] та Act on Promotion of Information and Communications Network Utilization and Information Protection [19], які передбачають суворі вимоги до операторів КІ щодо кіберзахисту, аудиту та сертифікації. Особливістю південнокорейського підходу є поєднання жорсткого державного регулювання з високим рівнем технологічних інновацій, а також постійна готовність до зовнішніх кіберзагроз з боку КНДР, що формує стратегію із сильним акцентом на кібероборону, інформаційний обмін і стійкість до гібридних атак;

–***у Казахстані*** система захисту КІ формується в рамках державної політики кібербезпеки «Кіберщит Казахстану» [20], що була затверджена у 2017 році й визначає стратегічні напрями протидії кіберзагрозам. Координацію здійснюють Міністерство цифрового розвитку, інновацій та аерокосмічної промисловості спільно з Комітетом національної безпеки, які контролюють діяльність операторів зв'язку, державних інформаційних систем та стратегічних підприємств. До КІ віднесено енергетику, транспорт, фінансово-банківську сферу, ІКТ, ОПК і державні інформаційні ресурси, для яких передбачені обов'язкові стандарти кіберзахисту, аудит та ліцензування діяльності у сфері інформаційної безпеки. Важливою особливістю моделі є створення Національного центру кібербезпеки, який відповідає за моніторинг і реагування на інциденти, а також за роботу урядової команди реагування KZ-CERT. На відміну від європейських підходів, Казахстан робить ставку на жорстке регулювання та централізований контроль, включно з можливістю обмеження доступу до інтернет-ресурсів у разі кібератак чи загроз національній безпеці.

Україна

В Україні відповідно до [24] виокремлено 24 сектори КІ держави (Табл. 1). Було наведено кількість підсекторів у кожному секторі, а також наявність певних ТП.

Таблиця 1

Сектори КІ України згідно чинного законодавства

Сектор	Підсектори	ТП
Паливно-енергетичний сектор		
Цифрові технології		
Захист інформації		
Харчова промисловість та агропромисловий комплекс		
Державний матеріальний резерв		–
Охорона здоров'я		
Ринки капіталу та організовані товарні ринки		–
Фінансовий сектор		–
Транспорт і пошта		
Системи життєзабезпечення		
Місцеве самоврядування		–
Промисловість		
Сектор громадської безпеки		+/–
Цивільний захист населення і територій		
Охорона навколишнього природного середовища		+/–
Сектор оборони		
Правосуддя		–

Виконання кримінальних покарань, тримання під вартою та утримання військовополонених		–
Державна реєстрація		–
Наукові дослідження та розробки		
Фінансовий сектор		–
Вибори та референдуми		–
Соціальний захист		–
Інформаційний сектор		–
Державна влада		–

Враховуючи повномасштабну агресію рф і її вплив на КІ України, можна виділити такі особливості формування і захисту КІ [25-27]:

Загрози:

– поєднання ракетно-дронових ударів, диверсій, кібератак і інформаційних операцій;

– основні мішені: енергетика (ГЕС/ТЕС/ВЕС/мережі), паливна логістика, зв'язок/ІКТ, транспортні вузли, водопостачання, охорона здоров'я, держреєстри та платежі [25].

Резильєнтність:

– децентралізація та розосередження активів: мікрогрід/генератори, дублювання підстанцій, резервні ЦОДи;

– масштабне резервування: дизель/газо- та ВДЕ-джерела, автономні вузли зв'язку (у т.ч. супутникові канали), крос-регіональні схеми живлення;

– планування безперервності (BCP) і відновлення (DRP) як обов'язковий атрибут операторів КІ.

Кіберзахист:

– сегментація та ізоляція OT/ICS, моніторинг 24/7 (SOC), реагування на інциденти із практикою "purple team";

– Zero Trust, багатофакторна автентифікація, управління вразливостями й патч-менеджмент у скорочених циклах;

– обов'язкова взаємодія з нац. центрами (наприклад, CERT-подібними), обмін індикаторами компрометації та швидке звітування про інциденти;

– захист ланцюгів постачання: перевірка постачальників, підпис оновлень ПЗ/ПЛК, "bill of materials" (SBOM).

Нормативне забезпечення:

– перехід до ризик-орієнтованого регулювання, гармонізація з ЄС (NIS2/CER, галузеві стандарти);

– визначені "життєво важливі" та "важливі" оператори; секторальні органи нагляду; спільні навчання, аудити, стрес-тести;

– публічно-приватна взаємодія: обмін даними, спільні вправи, координація під час криз (енергетичних, кібератак, БПЛА-загроз);

Операційні практики на місцях:

– фізичний периметр: інженерні укриття, модульні/мобільні рішення, системи РЕБ/ППО навколо об'єктів, відеоаналітика й тепловізійний нагляд;

– "fail-safe / fail-secure" режими для ТП;

– ручні процедури на випадок втрати SCADA/зв'язку;

– регулярні ТТХ і red team вправи, тестування резервних маршрутів електро- та даталіній; навчання персоналу [26].

Ключові виклики:

–постійне виснаження обладнання та персоналу, дефіцит запчастин/трансформаторів, залежність від імпорту компонентів для ОТ/ІКТ.

–висока динаміка тактик противника (комбінування кінетики та кіберу), що вимагає швидких оновлень процедур і технологій.

Завдання операторам КІ:

–повна інвентаризація активів IT/OT та карту залежностей (включно з людьми й постачальниками);

–оновлення моделі загроз і наслідків, прив'язка контрзаходи до RTO/RPO;

–безперервна оцінка вразливостей / пентести, сегментацію мереж, журналювання й централізований моніторинг;

–мультирезервування: енергетика, зв'язок, обчислення, дані (offline-бекапи + георезервування);

–регулярно тренувати BCP/DRP, комунікації кризового штабу, взаємодію з держорганами та суміжними операторами;

–синхронізація з ЄС, крос-кордонні канали зв'язку, спільні CERT / CSIRT-механізми, програми допомоги з модернізації КІ [27].

Сучасні ІТ-рішення для підтримки технологічних процесів у секторах критичної інфраструктури держави

Технологічні процеси в КІ України

У Табл. 1 було визначено сектори КІ (12 з 24), що пов'язані з певними ТП. Деталізуємо інформацію про самі процеси:

1) Паливно-енергетичний сектор:

–генерація енергії: атомна, теплова, гідро-, відновлювальна;

–передача і розподіл: електромережі, підстанції, диспетчерське управління;

–видобуток і транспортування: нафта, газ, вугілля, трубопроводи;

–зберігання і переробка: нафтобази, НПЗ, газосховища;

–моніторинг і балансування: SCADA/EMS-системи, smart grid.

2) Цифрові технології:

–телекомунікації: мобільний зв'язок, інтернет, супутниковий доступ;

–дата-центри та ХТ: обробка, зберігання і резервування;

–національні реєстри та електронні сервіси;

–критичні інформаційні системи: e-Government, е-послуги;

–захист каналів зв'язку: шифрування, VPN, кібермоніторинг.

3) Захист інформації:

–управління інформаційними ресурсами: бази даних, документообіг;

–захист державної таємниці і персональних даних;

–функціонування SOC і CERT;

–реагування на інциденти та кіберзагрози;

–впровадження стандартів.

4) Харчова промисловість та агропромисловий комплекс:

–виробництво с/г продукції: рослинництво, тваринництво;

–переробка/зберігання: елеватори, холодильники, м'ясо- та молокозаводи;

–логістика продуктів: транспортування, експорт, імпорт;

–контроль якості та безпеки харчів;

–системи агроаналітики та смарт-ферми (AgroTech, IoT).

5) Охорона здоров'я:

– функціонування лікарень і клінік;
– медичні інформаційні системи: e-Health, телемедицина;
– забезпечення ліками та вакцинами: ланцюги постачання;
– санітарно-епідеміологічний моніторинг;
– реагування на НС (швидка допомога, мобільні госпіталі).

6) Транспорт і пошта:
– управління рухом: авіа, залізниця, метро, морський транспорт;
– інфраструктура безпеки: світлофори, навігація, сигналізація;
– логістика вантажів і поштових відправлень;
– інтелектуальні транспортні системи;
– інтеграція з міжнародними транспортними коридорами.

7) Системи життєзабезпечення:
– водопостачання і каналізація;
– теплопостачання і вентиляція;
– вивіз та утилізація відходів;
– моніторинг якості води, повітря, ресурсів;
– резервування (генератори, насосні станції, фільтрація).

8) Промисловість:
– металургія, хімія, машинобудування;
– виробничі лінії та автоматизація (MES, SCADA);
– ланцюги постачання і логістика;
– енергоспоживання та утилізація відходів;
– контроль якості та стандарти ISO/IEC.

9) Сектор громадської безпеки:
– функціонування поліції, ДСНС, прикордонної служби;
– системи 112 і аварійного реагування;
– муніципальна безпека: відеоспостереження, “Safe City”;
– антитерористичні та протидиверсійні заходи;
– координація дій у кризових ситуаціях.

10) Охорона навколишнього природного середовища:
– моніторинг довкілля: вода, повітря, ґрунт, радіація;
– управління відходами та викидами;
– попередження та ліквідація НС природного характеру (паводки, пожежі);
– еко-енергетика та зменшення вуглецевого сліду;
– системи раннього попередження (Earth Observation, IoT).

11) Сектор оборони:
– системи управління військами і зв’язку;
– озброєння та військова техніка (виробництво, ремонт, логістика);
– розвідка, кібер- та РЕБ-операції;
– захист баз, складів, об’єктів;
– спільні навчання та взаємодія з партнерами (НАТО, ЄС).

12) Наукові дослідження та розробки:
– державні та університетські наукові центри;
– прикладні НДДКР у сфері безпеки, енергетики, ІТ, медицини;
– інноваційні, наукові, індустріальні парки, стартап-екосистема;
– міжнародна наукова кооперація (Horizon Europe, NATO SPS, Erasmus);
– трансфер технологій і комерціалізація інновацій.

ІТ-рішення для підтримки технологічних процесів у критичній інфраструктурі держави

Сучасна підтримка ТП (у тому числі й у КІ держави) базується на поєднанні хмарних технологій (IaaS, PaaS, SaaS, Hybrid Cloud, Edge Cloud, Serverless Computing), IIoT, цифрових двійників, аналітики великих даних (Hadoop, Spark, Power BI, Tableau, Qlik) та кіберзахисту (SIEM, Zero Trust, PQC), управління підприємством КІ (ERP, MES, APS) інтегрованих у єдину інфраструктуру ІКТ на основі сучасних мережевих протоколів (наприклад, 5G/6G технологій) [28].

Для підприємств КІ основним критерієм відбору ІТ-рішень є забезпечення безперервності та стійкості ТП при одночасному дотриманні вимог надійності, безпеки (К, Ц, Д), масштабованості та економічної ефективності.

Методи та моделі підтримки технологічних процесів

1) Методи управління ТП можна представити як шкалу еволюції: від простих регуляторів (PID) → через оптимізаційні моделі (MPC) → до інтелектуальних (AI/ML) → і нарешті до цифрових двійників і хмарних платформ, які дозволяють управляти системами в умовах невизначеності та кіберризиків [29].

2) Методи моніторингу ТП можна представити як багаторівневу систему:

– базовий рівень – SCADA/DCS для збору даних;

– аналітичний рівень – статистичні й ML-моделі для виявлення відхилень;

– прогнозний рівень – цифрові двійники й AI для передбачення розвитку ситуацій*;*

– інфраструктурний рівень – хмарні та IoT-платформи, які забезпечують масштабованість і інтеграцію.

) Методи оцінювання ефективності ТП можна поділити на три рівні:

– операційний рівень – KPI, OEE, SPC;

– аналітичний рівень – DEA, SFA, багатокритеріальні моделі;

– прогнозно-стратегічний рівень – цифрові двійники, ML/AI, імітаційні моделі з урахуванням ризиків і стійкості (резильєнтності) [30].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі проаналізовано КІ в Європі, Азії, США та Україні (поняття, структура, загрози і виклики), сучасні ІТ-рішення для підтримки ТП в різних секторах КІ держави, методи та моделі підтримки технологічних процесів та здійснено огляд наукових публікацій та дослідницьких проєктів щодо підтримки ТП в КІ.

Не зважаючи на велику кількість наукових досліджень у цьому напрямку, залишається низка невирішених завдань, зокрема:

– відсутність ефективних моделей підтримки ТП з використанням ХТ;

– відсутність засобів багатопараметричного моніторингу ключових індикаторів ефективності ТП у КІ;

– не достатня кількість спеціалізованих інформаційно-комунікаційних систем та мереж для автоматизації виробничих процесів;

– недоліки у захищеності даних (з точки зору забезпечення К, Ц, Д) в інформаційно-комунікаційних системах та мережах, пов’язаних з ТП у КІ;

– не достатньо вивчене питання використання ХТ як бази для підтримки ТП у КІ;

– відсутність цілісних підходів (стандартів, рекомендацій, методологій) щодо підтримки ТП у КІ держави.

Вирішенню цих завдань будуть присвячені подальші роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Potii, O., & Tsyplinsky, Y. (2020). Methods of classification and assessment of critical information infrastructure objects. *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 389–393. Kyiv, Ukraine. https://doi.org/10.1109/DESSERT50317.2020.9125028
2. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., & Polozhentsev, A. (2022). The model for calculating the quantitative criteria for assessing the security level of information and telecommunication systems. *CEUR Workshop Proceedings*, *3156*, 390–399.
3. Toliupa, S., Parkhomenko, I., & Shvedova, H. (2019). Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assessment. *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 463–468. Lviv, Ukraine. https://doi.org/10.1109/AIACT.2019.8847746
4. Habiba, M., & Criveti, M. (2022). *Hybrid cloud infrastructure and operations explained: Accelerate your application migration and modernization journey on the cloud with IBM and Red Hat.* Packt Publishing.
5. Gnatyuk, S., Berdibayev, R., Smirnova, T., Avkurova, Z., & Iavich, M. (2021). Cloud-based cyber incidents response system and software tools. *Communications in Computer and Information Science*, *1486*, 169–184.
6. Svanadze, V., Iavich, M., & Gnatyuk, S. (2024). Challenges and solutions for cybersecurity and information security management in organizations. *CEUR Workshop Proceedings*, *3654*, 497–504.
7. Dong, Z. (2022). Research of big data information mining and analysis: Technology based on Hadoop technology. *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, 173–176. Sanya, China. https://doi.org/10.1109/BDICN55575.2022.00041
8. Cybersecurity and Infrastructure Security Agency. (2025, August 15). *Critical infrastructure sectors.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
9. The White House. (2024, April 30). *National security memorandum on critical infrastructure security and resilience.* https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience
10. European Commission. (2025, August 15). *NIS2 directive: Securing network and information systems.* https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
11. *Critical entities resilience directive (CER).* (2025, August 15). https://www.critical-entities-resilience-directive.com
12. Cyber Security Agency of Singapore. (2025, August 15). *Cybersecurity Act: Information on the Cybersecurity Act.* https://www.csa.gov.sg/legislation/cybersecurity-act
13. Ministry of Finance of India. (2025, August 16). *Critical information infrastructure (India).* https://financialservices.gov.in/beta/en/page/cii
14. Government of India. (2025, August 16). *Section 70 of IT Act (India).* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=91
15. National Center of Incident Readiness and Strategy for Cybersecurity. (2024). *Overview of cybersecurity policy for CIP (Japan).* https://www.nisc.go.jp/eng/pdf/cip_policy_abst_2024_eng.pdf
16. *Cybersecurity Law of the People's Republic of China.* (2025, August 16). https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3
17. *Translation: Critical information infrastructure security protection regulations (Effective Sept. 1, 2021).* (2025, August 16). https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021
18. Korea Legislation Research Institute. (2025, August 16). *Framework Act on National Informatization (Republic of Korea).* https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42620&lang=ENG
19. Korea Legislation Research Institute. (2025, August 16). *Act on promotion of information and communications network utilization and information protection (Republic of Korea).* https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG
20. National Security Committee of the Republic of Kazakhstan. (2025, August 15). *Cyber Shield.* https://www.gov.kz/memleket/entities/knb/activities/250
21. UK Government. (2016). *Investigatory Powers Act 2016.* https://www.legislation.gov.uk/ukpga/2016/25/contents
22. UK Government. (2022). *Government cyber security strategy: 2022 to 2030.* https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

23. UK Government. (2021). *National Security and Investment Act 2021*. https://www.legislation.gov.uk/ukpga/2021/25/contents
24. Кабінет Міністрів України. (2022). *Порядок віднесення об'єктів до критичної інфраструктури (Постанова № 1109, в ред. від 16 грудня 2022 р. № 1384).* https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42
25. Patias, I. (2025). Cost distribution in ICT infrastructure during the AI era: A model for data centers, power grids, and telecommunications. *2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA)*, 1–8. Ankara, Turkiye. https://doi.org/10.1109/ICHORA65333.2025.11017137
26. Zeng, R., et al. (2024). A general real-time cyberattack risk assessment method for distribution network involving the influence of feeder automation system. *IEEE Transactions on Smart Grid*, *15*(2), 2102–2115. https://doi.org/10.1109/TSG.2023.3302287
27. Penedo, D. (2006). Technical infrastructure of a CSIRT. *International Conference on Internet Surveillance and Protection (ICISP'06)*, 27–27. Cote d'Azur, France. https://doi.org/10.1109/ICISP.2006.32
28. Otero-Mosquera, J., Meleiro-Estévez, A., Fondo-Ferreiro, P., Luque-Schempp, F., Gil-Castineira, F., & Merino, P. (2025). Reproducible key performance indicator (KPI) measurement experiments in 6G networks under mobility conditions. *2025 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 446–451. Poznan, Poland. https://doi.org/10.1109/EuCNC/6GSummit63408.2025.11036984
29. Semertzis, I., Rajkumar, V. S., Ştefanov, A., Fransen, F., & Palensky, P. (2022). Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs. *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 1–6. Milan, Italy. https://doi.org/10.1109/MSCPES55116.2022.9770140
30. Deffenbaugh, G., & Kameneni, S. (2025). Cyber resilience strategies throughout the system development lifecycle. *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 504–509. Chania, Crete, Greece. https://doi.org/10.1109/CSR64739.2025.11129978
31. Smirnova, T., Al-Oraiqat, A. M., Drieiev, O., Smirnov, O., Polishchuk, L., Khan, S., Hasan, Y. M. Y., Amro, A. M., & AlRawashdeh, H. S. (2022). Method for determining treated metal surface quality using computer vision technology. *Sensors*, *22*(16), 6223. https://www.scopus.com/pages/publications/85137126823
32. Smirnova, T., Odarchenko, R., Smirnov, O., Bondar, S., & Volosheniuk, D. (2023). Optimal structure construction of private 5G network for the needs of enterprises. *Lecture Notes on Data Engineering and Communications Technologies*, *178*, 208–223. https://www.scopus.com/pages/publications/85162950840
33. Al-Mudhafar, A. M., Smirnova, T., Buravchenko, K., & Smirnov, O. (2023). 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*, *7*(2), 49–56. https://www.scopus.com/pages/publications/85176960353
34. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., & Dorenskyi, O. (2025). Cloud-based information system for evaluating caverns in the process of blasting metal surfaces of details. *International Review on Modelling and Simulations*, *18*(1), 32–42. https://doi.org/10.15866/iremos.v18i1.25596

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

Tetiana Smirnova
Candidate of Science (Engineering),
Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID: 0000-0001-6896-0612
sm.tetyana.gmail.com

RESEARCH OF METHODS, MODELS AND MODERN IT SOLUTIONS TO SUPPORT TECHNOLOGICAL PROCESSES IN CRITICAL INFRASTRUCTURE OF THE STATE

Abstract. The paper analyzes critical infrastructure in Europe, Asia, the USA and Ukraine (concept, structure, threats and challenges). It is determined that in the context of cyber threats, global digitalization and the need for rapid response to emergencies, there is a need to use modern methods and models of technological process support that provide flexibility, scalability and a high level of reliability. It is determined that modern technological process support is based on a combination of cloud technologies, IIoT, digital twins, big data analytics and cyber protection, critical infrastructure enterprise management, integrated into a single infrastructure of information and communication technologies based on modern network protocols. For critical infrastructure enterprises, the main criterion for selecting IT solutions is to ensure the continuity and stability of technological processes while simultaneously meeting the requirements of reliability, security (confidentiality, integrity, availability (CIA)), scalability and cost-effectiveness. The main methods and models of support (management, monitoring, efficiency assessment) of technological processes, determined as a result of the analysis of modern scientific publications and research projects in the field of support of technological processes in critical infrastructure, are presented. It is established that despite the large number of scientific studies in this area, there are a number of unresolved problems that need to be solved.

Keywords: critical infrastructure security, information technology, technological processes, Internet of Things, security requirements, reliability requirements

REFERENCES

1. Potii, O., & Tsyplinsky, Y. (2020). Methods of classification and assessment of critical information infrastructure objects. *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 389–393. Kyiv, Ukraine. https://doi.org/10.1109/DESSERT50317.2020.9125028
2. Gnatyuk, S., Yudin, O., Sydorenko, V., Smirnova, T., & Polozhentsev, A. (2022). The model for calculating the quantitative criteria for assessing the security level of information and telecommunication systems. *CEUR Workshop Proceedings, 3156*, 390–399.
3. Toliupa, S., Parkhomenko, I., & Shvedova, H. (2019). Security and regulatory aspects of the critical infrastructure objects functioning and cyberpower level assessment. *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 463–468. Lviv, Ukraine. https://doi.org/10.1109/AIACT.2019.8847746
4. Habiba, M., & Criveti, M. (2022). *Hybrid cloud infrastructure and operations explained: Accelerate your application migration and modernization journey on the cloud with IBM and Red Hat.* Packt Publishing.
5. Gnatyuk, S., Berdibayev, R., Smirnova, T., Avkurova, Z., & Iavich, M. (2021). Cloud-based cyber incidents response system and software tools. *Communications in Computer and Information Science, 1486*, 169–184.
6. Svanadze, V., Iavich, M., & Gnatyuk, S. (2024). Challenges and solutions for cybersecurity and information security management in organizations. *CEUR Workshop Proceedings, 3654*, 497–504.
7. Dong, Z. (2022). Research of big data information mining and analysis: Technology based on Hadoop technology. *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, 173–176. Sanya, China. https://doi.org/10.1109/BDICN55575.2022.00041

8. Cybersecurity and Infrastructure Security Agency. (2025, August 15). *Critical infrastructure sectors.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
9. The White House. (2024, April 30). *National security memorandum on critical infrastructure security and resilience.* https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience
10. European Commission. (2025, August 15). *NIS2 directive: Securing network and information systems.* https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
11. *Critical entities resilience directive (CER).* (2025, August 15). https://www.critical-entities-resilience-directive.com
12. Cyber Security Agency of Singapore. (2025, August 15). *Cybersecurity Act: Information on the Cybersecurity Act.* https://www.csa.gov.sg/legislation/cybersecurity-act
13. Ministry of Finance of India. (2025, August 16). *Critical information infrastructure (India).* https://financialservices.gov.in/beta/en/page/cii
14. Government of India. (2025, August 16). *Section 70 of IT Act (India).* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=91
15. National Center of Incident Readiness and Strategy for Cybersecurity. (2024). *Overview of cybersecurity policy for CIP (Japan).* https://www.nisc.go.jp/eng/pdf/cip_policy_abst_2024_eng.pdf
16. *Cybersecurity Law of the People's Republic of China.* (2025, August 16). https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3
17. *Translation: Critical information infrastructure security protection regulations (Effective Sept. 1, 2021).* (2025, August 16). https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021
18. Korea Legislation Research Institute. (2025, August 16). *Framework Act on National Informatization (Republic of Korea).* https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42620&lang=ENG
19. Korea Legislation Research Institute. (2025, August 16). *Act on promotion of information and communications network utilization and information protection (Republic of Korea).* https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG
20. National Security Committee of the Republic of Kazakhstan. (2025, August 15). *Cyber Shield.* https://www.gov.kz/memleket/entities/knb/activities/250
21. UK Government. (2016). *Investigatory Powers Act 2016.* https://www.legislation.gov.uk/ukpga/2016/25/contents
22. UK Government. (2022). *Government cyber security strategy: 2022 to 2030.* https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030
23. UK Government. (2021). *National Security and Investment Act 2021.* https://www.legislation.gov.uk/ukpga/2021/25/contents
24. Кабінет Міністрів України. (2022). *Порядок віднесення об'єктів до критичної інфраструктури (Постанова № 1109, в ред. від 16 грудня 2022 р. № 1384).* https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42
25. Patias, I. (2025). Cost distribution in ICT infrastructure during the AI era: A model for data centers, power grids, and telecommunications. *2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA)*, 1–8. Ankara, Turkiye. https://doi.org/10.1109/ICHORA65333.2025.11017137
26. Zeng, R., et al. (2024). A general real-time cyberattack risk assessment method for distribution network involving the influence of feeder automation system. *IEEE Transactions on Smart Grid*, *15*(2), 2102–2115. https://doi.org/10.1109/TSG.2023.3302287
27. Penedo, D. (2006). Technical infrastructure of a CSIRT. *International Conference on Internet Surveillance and Protection (ICISP'06)*, 27–27. Cote d'Azur, France. https://doi.org/10.1109/ICISP.2006.32
28. Otero-Mosquera, J., Meleiro-Estévez, A., Fondo-Ferreiro, P., Luque-Schempp, F., Gil-Castineira, F., & Merino, P. (2025). Reproducible key performance indicator (KPI) measurement experiments in 6G networks under mobility conditions. *2025 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 446–451. Poznan, Poland. https://doi.org/10.1109/EuCNC/6GSummit63408.2025.11036984
29. Semertzis, I., Rajkumar, V. S., Ştefanov, A., Fransen, F., & Palensky, P. (2022). Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs. *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 1–6. Milan, Italy. https://doi.org/10.1109/MSCPES55116.2022.9770140

30. Deffenbaugh, G., & Kameneni, S. (2025). Cyber resilience strategies throughout the system development lifecycle. *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 504–509. Chania, Crete, Greece. https://doi.org/10.1109/CSR64739.2025.11129978
31. Smirnova, T., Al-Oraiqat, A. M., Drieiev, O., Smirnov, O., Polishchuk, L., Khan, S., Hasan, Y. M. Y., Amro, A. M., & AlRawashdeh, H. S. (2022). Method for determining treated metal surface quality using computer vision technology. *Sensors*, *22*(16), 6223. https://www.scopus.com/pages/publications/85137126823
32. Smirnova, T., Odarchenko, R., Smirnov, O., Bondar, S., & Volosheniuk, D. (2023). Optimal structure construction of private 5G network for the needs of enterprises. *Lecture Notes on Data Engineering and Communications Technologies*, *178*, 208–223. https://www.scopus.com/pages/publications/85162950840
33. Al-Mudhafar, A. M., Smirnova, T., Buravchenko, K., & Smirnov, O. (2023). 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*, *7*(2), 49–56. https://www.scopus.com/pages/publications/85176960353
34. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., & Dorenskyi, O. (2025). Cloud-based information system for evaluating caverns in the process of blasting metal surfaces of details. *International Review on Modelling and Simulations*, *18*(1), 32–42. https://doi.org/10.15866/iremos.v18i1.25596

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.