КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.963
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 ХМАРНИХ ТЕХНОЛОГІЙ ТА МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ У КРИТИЧНІЙ ІНФРАСТРУКТУРІ ДЕРЖАВИ

Анотація. У роботі проведено дослідження наукових публікацій та дослідницьких проєктів щодо підтримки технологічних процесів у критичній інфраструктурі держави. Визначено об'єктивне протиріччя (проявляється між практичною необхідністю реалізації багатопараметричного моніторингу, автоматизації та кіберзахисту технологічних процесів у критичній інфраструктурі держави та науково-методичною недостатністю існуючих підходів, які не забезпечують комплексного використання хмарних технологій для підтримки таких процесів). Формалізовано постановку подальшого наукового завдання, яке полягає в розробленні методів та моделей підтримки технологічних процесів у критичній інфраструктурі держави на основі хмарних технологій, що забезпечать: підвищення ефективності та гнучкості управління технологічними процесами; створення засобів багатопараметричного моніторингу ключових індикаторів ефективності; удосконалення інформаційно-комунікаційних систем і мереж для автоматизації виробничих процесів; належний рівень кіберзахисту даних; формування цілісних підходів, методологій та рекомендацій для впровадження хмарних технологій у критичній інфраструктурі держави.

Ключові слова: безпека критичної інфраструктури**,** інформаційні технології, технологічні процеси, хмарні технології, штучний інтелект, Інтернет речей

ВСТУП

Постановка завдання дослідження

Останні десятиріччя характеризуються стрімким зростанням складності та взаємозалежності технологічних процесів (ТП) у критичній інфраструктурі (КІ) держави. Ефективність функціонування таких систем має безпосередній вплив на національну безпеку, економіку та соціальну стійкість. В умовах постійно зростаючого рівня кіберзагроз, впровадження 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. Модернізація КІ забезпечується за рахунок впровадження хмарних технологій (ХТ), які поступово стають ключовим інструментом завдяки своїй здатності забезпечувати централізоване зберігання та обробку даних, інтеграцію розподілених систем і підвищення рівня кібербезпеки [3]. Реалізація адаптивних механізмів управління ТП, застосовування алгоритмів штучного інтелекту (ШІ, AI) для аналізу великих масивів даних [7], а також створювання моделі прогнозування ризиків та сценаріїв розвитку інцидентів стає більш ефективним з застосуванням ХТ. Це відкриває

© Т.В. Смірнова, 2025

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 (АПК), відповідність міжнародним стандартам. Тому важливим завданням сучасних наукових досліджень є систематизація та аналіз існуючих хмарних технологій та методів штучного інтелекту для реалізації технологічних процесів у критичній інфраструктурі держави, з метою виявлення їх переваг, обмежень і перспектив подальшого розвитку.

Аналіз останніх досліджень і публікацій. У науковій статті [1] досліджуються колони-водонапірні башти, що використовуються для постачання питної води до віддалених населених пунктів. В статті [2] аналізується КІ від закладів охорони здоров'я до енергетичних систем. Дослідження [3] присвячене аналізу стану безпеки IoT та пов'язаних з ним ризиків у КІ. Стаття [4] присвячена перспективам виробництва в контексті проблем кібербезпеки в промисловій інфраструктурі. У [5] запропоновано передовий підхід, який зосереджується на мережевій програмі (NetApp) з підтримкою 5G для прогнозного технічного обслуговування КІ. У статті [6] досліджується концепція пильного контролю для інтелектуального аварійного енергопостачання КІ. Інша стаття [7] демонструє, як методи інженерії вимог (RE) можуть підтримати розвиток нетехнічних елементів у соціально-технічних системах, таких як керівні принципи. Наступна стаття [8] аналізує, як система на основі AI покращує можливості транспортної системи. Вплив AI на будівництво інфраструктури аналізується в [9]. В іншій статті [10] досліджуються методи збереження конфіденційності (К) для КІ мереж промислового IoT. Загроза технологічного старіння для кібербезпеки в енергетичному секторі описана в [11]. В іншій статті [12] описано наслідки зміни клімату для водопостачання в містах. Наступна стаття [13] аналізує роль нанотехнологій у водному секторі. Інша стаття [14] досліджує інтеграцію етики AI та технологічної грамотності в сучасній охороні здоров'я. Шлях до загального AI в охороні здоров'я описаний в [15]. Якість програмного забезпечення в IoT в [16] стосується секторів охорони здоров'я та торгівлі. У цій науковій роботі [17] досліджується застосування робототехнічних технологій у сфері охорони здоров'я. У дослідженні [18] розглядається трансформаційний вплив Health Care 4.0 на надання медичних послуг. В іншій статті [19] досліджується застосування біометричних технологій у транспортних компаніях. Нові технології для збереження К в енергетичній системі розглядаються в [20]. В іншій статті [21] досліджується інтелектуальна система водопостачання на базі IoT. Цифрова безпека ланцюгів постачання для операторів енергетичного сектору у світлі нових директив та регламентів ЄС описана в [22]. У дослідницькій роботі [23] досліджується кіберфізичне зміцнення цифрової водної інфраструктури. Тенденції в європейських дослідницьких проектах, орієнтованих на технологічну екосистему в секторі охорони здоров'я, вивчаються в [24]. Наступна стаття [25] описує структуру для візуалізації транзакцій блокчейну в КІ, орієнтовану на користувача. Процес оптимізації кіберстійкості в мережі КІ досліджується в [26]. В іншій статті [27] описується КІ на основі Індустрії 4.0. У статті [28] досліджуються випадки використання квантових обчислень для національної КІ. Реакція цифрових двійників на інциденти з метою підвищення безпеки КІ енергосистеми описана в [29]. У статті [30] досліджується AI для систем, критичних з точки зору безпеки, у промисловій та транспортній галузях. Однак інтеграція передових технологій ШІ з процесами та стандартами інженерії безпеки залишається серйозним викликом [31-33]. Роботи [34-37] присвячені IT-рішенням для підтримки технологічних процесів у критичній інфраструктурі держави та методам й моделям підтримки технологічних процесів.

Метою даної статті є дослідження хмарних технологій та методів штучного інтелекту для реалізації технологічних процесів у критичній інфраструктурі держави та визначення актуальних напрямків подальших досліджень на основі проведеного аналізу.

Об'єктом дослідження є процес забезпечення безпеки та надійності технологічних процесів у критичній інфраструктурі держави.

Предметом дослідження є хмарні технологій та методи штучного інтелекту для реалізації технологічних процесів у критичній інфраструктурі держави.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У науковій статті [1] досліджуються колони-водонапірні башти, що використовуються для постачання питної води до віддалених населених пунктів. У статті також пропонується методологія автоматизації колон, спрямована на використання електричних приводів для автоматичного регулювання роботи насосів. Проведено огляд існуючих автоматизованих систем і розроблено нове рішення у вигляді структурної схеми, в якій основною змінною управління є тиск у турботрубі. Математично визначено основні параметри та передавальні функції компонентів автоматичної системи. На основі цих результатів у спеціалізованому програмному середовищі створено імітаційну модель. Моделювання та імітація використовуються для визначення перехідних характеристик системи та оцінки ключових показників якості.

В іншій статті [2] аналізується КІ (від закладів охорони здоров'я до енергетичних систем), яка все частіше стає об'єктом кібератак, що створює системні вразливості з потенційно небезпечними для життя наслідками. Для усунення цих ризиків Європейський Союз прийняв Директиву NIS2 (Директива (ЄС) 2022/2555), яка значно розширює вимоги до кібербезпеки для основних і важливих суб'єктів у 18 ключових секторах.

У цій статті розглядаються основні правові зміни, передбачені директивою, зокрема розширення сфери її застосування, посилення зобов'язань з управління ризиками, більш суворий режим забезпечення дотримання (із значними штрафами та відповідальністю виконавчої влади) та вдосконалені механізми координації в масштабах ЄС. У ній також досліджуються практичні проблеми впровадження, такі як розбіжності в національних транспозиціях, навантаження на середні підприємства у зв'язку з дотриманням вимог та складнощі повідомлення про інциденти та безпеки ланцюгів постачання. На прикладі реальних випадків – атаки програм-вимагачів на Управління охорони здоров'я Ірландії у 2021 році та спалаху шкідливого програмного забезпечення NotPetya у 2017 році – аналіз показує, як NIS2 прагне усунути постійні вразливості. Нарешті, стаття розміщує NIS2 в ширшому контексті кібербезпеки ЄС, поряд з Директивою CER, DORA, CRA та майбутніми ініціативами з кіберзахисту, і робить висновок, що, хоча NIS2 є значним кроком вперед у законодавстві ЄС з кібербезпеки, його вплив буде залежати від послідовного виконання, ефективної регуляторної співпраці та міцного партнерства між державним і приватним секторами. Нарешті, стаття розміщує NIS2 в більш широкій рамках кібербезпеки ЄС, поряд з Директивою CER, DORA, CRA та майбутніми ініціативами з кіберзахисту, і робить висновок, що хоча NIS2 є значним прогресом у законодавстві ЄС з кібербезпеки, його вплив буде залежати від послідовного виконання, ефективної регуляторної співпраці та міцної стійкості державного та приватного секторів.

Дослідження [3] присвячене аналізу стану безпеки IoT та пов'язаних з ним ризиків у КІ. Технологія IoT відкриває величезні можливості для зв'язку та автоматизації в різних

секторах, але водночас створює серйозні проблеми безпеки, які вимагають негайного вирішення. У міру того як пристрої IoT все більше інтегруються в КІ, їхні вбудовані вразливості, такі як незахищене програмне забезпечення, стандартні облікові дані та приховані «задні двері», стають привабливою мішенню для кібератак, включаючи шпигунство та саботаж. Реальні інциденти продемонстрували, як такі слабкі місця можуть становити загрозу для К, безпеки та безперебійності послуг. Ця стаття зосереджується на ризиках для міської КІ, де використання IoT може спричинити серйозні наслідки, такі як відключення електроенергії, забруднення води та масштабні перебої в наданні послуг, особливо в густонаселених районах.

Аналіз підкреслює необхідність багатовимірного підходу до безпеки – що охоплює технологічні, правові, соціальні та економічні аспекти – для протидії цим загрозам. Він обґрунтовує необхідність постійного вдосконалення стратегій кібербезпеки відповідно до швидкого розвитку IoT, пропагуючи проактивні заходи для захисту систем та забезпечення безперебійної роботи цих незамінних компонентів сучасного життя.

Стаття [4] присвячена перспективам виробництва в контексті проблем кібербезпеки в промисловій інфраструктурі. Промисловий сектор стикається з дедалі більшими викликами в галузі кібербезпеки, оскільки промислові системи управління (ICS) все частіше стають мішенню зловмисних дій та шкідливого програмного забезпечення. Такі атаки можуть поставити під загрозу якість продукції, порушити виробництво, зашкодити репутації бренду, зменшити доходи та становити небезпеку для здоров'я та безпеки людей. Швидке впровадження технологій Індустрії 4.0, політики BYOD, мобільних обчислювальних технологій та IoT покращило процес прийняття рішень, оперативну ефективність та інтеграцію на світовому ринку, але також створило нові вразливості та ризики, особливо у виробничих середовищах.

Для протидії цим загрозам потрібні комплексні стратегії безпеки, що об'єднують людей, процеси та технології. У цій статті представлено вичерпний огляд тенденцій у сфері безпеки ICS, що охоплює кіберзагрози, вразливості, схеми атак, суб'єктів та пов'язані з ними ризики, а також їхній вплив на промислові операції. Дослідження має на меті підвищити обізнаність зацікавлених сторін, посилити компетенції у сфері безпеки та надати рекомендації щодо розробки та впровадження ефективних механізмів захисту та найкращих практик.

У [5] запропоновано передовий підхід, який зосереджується на мережевій програмі (NetApp) з підтримкою 5G для прогнозного технічного обслуговування КІ. Прогнозне технічне обслуговування є надзвичайно важливим для КІ, оскільки дозволяє передбачити несправності, запобігти уникненню пошкоджень обладнання та своєчасно планувати ремонтні роботи. Використовуючи AI, прогнозне технічне обслуговування може аналізувати операційні дані для надання точних прогнозів та підтримки негайних втручань щодо критичних активів. У цій статті представлено мережеву програму (NetApp) на базі 5G, призначену для профілактичного обслуговування в КІ, пов'язаних з енергетикою.

Запропонована NetApp інтегрує контейнерні компоненти, які збирають оперативні дані часових рядів з електростанцій та виявляють аномалії в роботі енергогенеруючих установок. Для виявлення аномалій використовується модель на основі автокодера, що дозволяє своєчасно розпізнавати несправності. Експериментальна оцінка демонструє ефективність та результативність запропонованої NetApp, підкреслюючи її потенціал для підвищення надійності та стійкості роботи в енергетичному секторі.

У статті [6] досліджується концепція пильного контролю для інтелектуального аварійного енергопостачання КІ. У разі катастрофічних подій надзвичайно важливим є

швидке відновлення КІ та обладнання. Такі важливі послуги, як інформаційно-комунікаційні технології (ІКТ), охорона здоров'я, реагування на надзвичайні ситуації та рятувальні операції, значною мірою залежать від стабільного електропостачання. Хоча резервні джерела живлення, такі як акумулятори та аварійні генератори, можуть тимчасово забезпечувати енергією під час відключень, вони часто обмежені тривалістю постачання, стаціонарним розміщенням або логістичними проблемами в надзвичайних ситуаціях. Для усунення цих обмежень потрібні більш гнучкі та динамічні рішення в галузі енергопостачання. Проект Smart Emergency, що фінансується Фондом клімату та енергетики уряду Австрії, досліджує такі підходи для забезпечення надійного, мобільного та адаптивного енергопостачання КІ в кризових ситуаціях.

Інша стаття [7] демонструє, як методи інженерії вимог (RE) можуть підтримати розвиток нетехнічних елементів у соціально-технічних системах, таких як керівні принципи. Адаптований підхід RE був застосований у рамках проекту ЄС Horizon 2020 DARWIN, метою якого було створення керівних принципів стійкості для управління кризовими ситуаціями. Спираючись на практику системної інженерії, цей підхід використовує паралелі між розробкою систем та процесом формулювання та оцінки керівних принципів.

У статті описано визначення вимог до керівних принципів щодо стійкості, висвітлено основні отримані уроки та наведено ілюстративні приклади. Результати дослідження мають на меті надати практикам і дослідникам методологічні знання, які слугуватимуть орієнтиром для посилення стійкості КІ та вдосконалення розробки керівних принципів у складних соціально-технічних контекстах.

Наступна стаття [8] аналізує, як система на основі AI покращує можливості транспортної системи. В останні роки забезпечення стійкості традиційних технологій у КІ стає все більш складним завданням, і AI відіграє дедалі більшу роль у вирішенні цих проблем. AI дозволив створити повсюдні додатки, що працюють у режимі реального часу та покращують інтелектуальні середовища в багатьох секторах, включаючи інтелектуальні міста, охорону здоров'я, виробництво, транспорт та IoT.

Завдяки розвитку таких технологій, як обробка природної мови, глибоке навчання та машинне навчання, ШІ перетворює галузь ІКТ та сприяє цифровій трансформації. Зокрема, транспорт зазнав значного впливу цих технологічних змін. Незважаючи на свою важливу роль в економічному зростанні, транспортні системи стикаються з постійними оперативними проблемами, такими як ненадійні розклади та небезпечна поведінка водіїв, що перешкоджає їх прийняттю громадськістю. У цій статті досліджується, як ШІ може забезпечити ефективні рішення цих проблем шляхом підвищення операційної ефективності, посилення безпеки та зменшення ризиків безпеки. У ній підкреслюється потенціал інтелектуальних транспортних систем на базі ШІ для надання більш надійних, безпечних та орієнтованих на користувача громадських послуг, позиціонуючи ШІ як основу майбутнього сталого розвитку мобільності.

Вплив AI на будівництво інфраструктури аналізується в [9]. AI став перетворювальною технологією для вирішення постійних проблем у будівництві інфраструктури, включаючи високий рівень аварійності, низьку продуктивність та нестачу робочої сили. Цей огляд містить комплексний аналіз сучасного стану застосування ШІ в цьому секторі, поєднуючи кількісну оцінку 594 досліджень з якісними висновками з 91 вибраних статей. Результати показують, що існуючі дослідження в основному зосереджені на моніторингу безпеки, контролі та управлінні процесами, а машинне навчання, комп'ютерний зір та обробка природної мови визначені як ключові технології. Значна увага також приділяється розвитку інтелектуальних будівельних

майданчиків. У перспективі перспективними напрямками досліджень є розширення спектру застосувань ШІ, використання різноманітних технологій ШІ та вдосконалення рішень за допомогою стандартизованих наборів даних та генеративних моделей ШІ. Ці напрямки мають потенціал для значного підвищення ефективності, безпеки та стійкості будівництва інфраструктури.

В іншій статті [10] досліджуються методи збереження К для КІ мереж промислового IoT. Поява інновацій, пов'язаних з IoT, привела до нових тенденцій в архітектурі мереж, особливо в промисловому IoT (IIoT). Завдяки взаємодії різнорідних пристроїв, датчиків та мереж для збору, моніторингу та аналізу промислових даних, IIoT підвищує оперативну ефективність, але також викликає значні занепокоєння щодо різнорідності пристроїв, безпеки та К. Якщо ці проблеми не вирішити, вони можуть поставити під загрозу як К користувачів, так і Ц інфраструктури. Для зменшення таких ризиків було досліджено стратегії збереження К, включаючи анонімізацію, збурення, К місцезнаходження та диференціальну К. Однак такі методи, як диференціальна К Дворка, залишаються обмеженими в своїй ефективності для захисту фізичної інфраструктури, що підтримує IIoT. У цій статті розглядаються вимоги до захисту К, відповідні моделі загроз, а також сильні та слабкі сторони існуючих технологій.

Крім того, в ній оцінюються підходи до збереження К в чотирьох критично важливих компонентах IIoT: мережі (SDN), аналіз даних (туманні обчислення), інтелектуальні мережі (інтелектуальні датчики) та додатки (попередня обробка). Результати дослідження висвітлюють існуючі прогалини та пропонують напрямки для майбутніх досліджень у сфері захисту мережевих інфраструктур на основі IIoT.

Загроза технологічного старіння для кібербезпеки в енергетичному секторі описана в [11]. Хоча хакерів часто уявляють як геніальних зловмисників, здатних здійснювати складне дистанційне управління, факти свідчать, що багато успішних атак на критично важливе обладнання, особливо в енергетичному секторі, є наслідком застарілого програмного забезпечення та неналежних політик оновлення. У цьому розділі розглядається реальна вразливість енергетичних компаній до кіберризиків, що зумовлена тривалим життєвим циклом обладнання та трансформацією екосистеми постачальників протягом останніх десятиліть. Зростаюча взаємопов'язаність систем та інтенсифікація автоматизації процесів ще більше посилили вразливість, привернувши увагу зловмисників, які прагнуть скористатися цими мінливими операційними середовищами. Для усунення цих ризиків зацікавлені сторони галузі та державні органи, зокрема у США та Європі, запровадили нові нормативні рамки, спрямовані на подолання технологічного старіння та посилення відповідальності. Ці заходи мають на меті зміцнити колективну безпеку та зменшити системну вразливість до кіберзагроз в енергетичному секторі.

В іншій статті [12] описано наслідки зміни клімату для водопостачання в містах. Вододефіцит у містах стає дедалі гострішою глобальною проблемою, спричиненою швидкою урбанізацією, зростанням населення та далекосяжними наслідками зміни клімату. У цій статті розглядається вплив зміни клімату на системи водопостачання міст, з особливим акцентом на вразливості та адаптаційній здатності міст у всьому світі. Зміни в режимі опадів, частіші екстремальні погодні явища та підвищення температури посилюють дефіцит води та створюють значне навантаження на і без того обмежені ресурси. З огляду на високу щільність населення та інтенсивне споживання води, міські райони є особливо вразливими до цих проблем. У цій статті узагальнено останні дослідження щодо гідрологічних наслідків зміни клімату, оцінено стійкість міської водопровідної інфраструктури та розглянуто інноваційні стратегії сталого управління.

Особливу увагу приділено інтегрованому управлінню водними ресурсами, новітнім технологіям та політичним рамкам, що підвищують адаптаційний потенціал. Висновки мають на меті допомогти зацікавленим сторонам та політикам у розробці ефективних заходів для пом'якшення водного стресу в містах в умовах невизначеного кліматичного майбутнього.

Наступна стаття [13] аналізує роль нанотехнологій у водному секторі. Дефіцит води та забруднення залишаються критичними глобальними проблемами, що впливають на здоров'я людей, екосистеми та економічний розвиток, і є центральними для Цілей сталого розвитку Організації Об'єднаних Націй. Це дослідження вивчає потенціал нанотехнологій у просуванні сталого управління водними ресурсами, з особливим акцентом на очищенні води. Для отримання глобальної перспективи було зібрано думки експертів від 29 учасників з Азії, Європи, Північної Америки та Близького Сходу. Найчастіше згадуваними технологіями були нанокаталізатори (34,48%), нанофільтраційні мембрани (31,03%), наноадсорбенти (27,59%) та вуглецеві нанотрубки (6,9%). Основні занепокоєння включали токсичність наноматеріалів (68,97%), високі експлуатаційні витрати (20,69%) та споживання енергії (10,34%). Понад 80% експертів наголосили на необхідності співпраці між вченими, інженерами, політиками та зацікавленими сторонами з промисловості для розробки масштабованих і стійких рішень. Результати дослідження підкреслюють такі пріоритети досліджень, як зниження витрат на матеріали, вдосконалення низькоенергетичних нанофільтраційних мембран та зменшення токсичності за допомогою біорозкладних або безпечніших за своєю конструкцією наночастинок. У висновках дослідження наголошується на важливості міждисциплінарної співпраці та нормативно-правової бази для розкриття повного потенціалу нанотехнологій для стійкого використання води.

Інша стаття [14] досліджує інтеграцію етики AI та технологічної грамотності в сучасній охороні здоров'я. Робота в галузі охорони здоров'я ґрунтується на етиці догляду, а технологічні інновації, такі як роботи та AI, повинні відповідати встановленим цінностям, нормам і практикам. Це дослідження представляє та визначає грамотність у сфері догляду за роботами (CRL) як інтегративну концепцію, яка поєднує технологічну грамотність з етикою AI в сучасній роботі з догляду. Оскільки роботизовані завдання з догляду створюють нові вимоги, CRL охоплює ресурси, навички та розуміння, необхідні практикам для ефективної та етичної роботи з роботами для догляду. Спираючись на соціотехнічну перспективу грамотності, дослідження підкреслює динамічну взаємодію між технологічним та соціальним вимірами, де успішна взаємодія між людиною та технологією залежить від обох. Використовуючи спрямований аналіз змісту та теоретичний синтез, результати дослідження визначають ключові компетенції та ситуаційну обізнаність для експлуатації роботів для догляду та спілкування про них. Запропонована концептуалізація CRL забезпечує основу для майбутніх досліджень, впровадження та розробки продуктів, підкреслюючи її значення як контекстуального доповнення до дискусії про етику ШІ в охороні здоров'я.

Шлях до загального AI в охороні здоров'я описаний в [15]. AI швидко розвивається в різних галузях, а охорона здоров'я виділяється як одна з найперспективніших сфер його застосування. Від ранніх символьних систем до сучасних фундаментальних і генеративних моделей, ШІ вже трансформував діагностику захворювань і персоналізовану медицину (Feng et al., How Far Are We From AGI, arXiv:2405.10313, 2024). У цій статті розглядається еволюція ШІ в охороні здоров'я, простежуючи прогрес від вузького AI до перспективи загального AI. На відміну від вузького AI, призначеного для виконання конкретних завдань, загальний AI розглядається як інтелект на рівні

людини, здатний адаптуватися до різних контекстів і виконувати широкий спектр інтелектуальних завдань. У статті розглядаються сильні сторони та обмеження минулих і сучасних моделей AI, а також досліджується, як загальний AI може подолати розбіжності в уніфікації, покращити узагальнення знань та сприяти глобальній медичній співпраці. У ній також розглядаються етичні, технологічні та соціальні виклики, що супроводжують цей перехід. Критично оцінюючи потенціал загального AI в обробці складних, неоднорідних даних та наданні високо персоналізованої допомоги, це дослідження сприяє поточним дебатам про трансформаційну роль AI в майбутніх системах охорони здоров'я.

Якість програмного забезпечення в IoT в [16] стосується секторів охорони здоров'я та торгівлі. Аналіз атрибутів якості є важливим етапом у визначенні функціональних можливостей та властивостей, якими повинна володіти програмна система від моменту її створення до розробки. З інтеграцією IoT системні вимоги та можливості компонентів значно розширюються, пов'язуючи послуги в ХТ та різних наукових і бізнес-сферах. У цьому дослідженні представлено огляд літератури, що базується на стандарті ISO/IEC 25010, з метою визначення відповідних атрибутів якості у двох сферах застосування: охорона здоров'я та торгівля. Аналіз висвітлює ключові характеристики якості та особливості конкретних сфер, надаючи інформацію про вимоги до програмних продуктів. Результати дослідження слугують основою для розширення дослідження на інші сфери, підкреслюючи роль IoT та програмної інженерії у вдосконаленні аналізу вимог, планування проектів, управління складними процесами та розробки програмних послуг вищої якості.

У цій науковій роботі [17] досліджується застосування робототехнічних технологій у сфері охорони здоров'я. Інтеграція робототехніки в охорону здоров'я трансформує догляд за пацієнтами, діагностику, лікування та оперативну ефективність. Робототехнічні системи підвищують точність хірургічних втручань, зменшують кількість людських помилок і сприяють проведенню мінімально інвазивних процедур, тим самим скорочуючи час відновлення та мінімізуючи ускладнення. У реабілітації робототехніка допомагає пацієнтам відновити рухові функції та поліпшити якість життя. У цьому дослідженні вивчається вплив робототехнічної трансформації в охороні здоров'я на основі даних 103 респондентів, зібраних за допомогою випадкової вибірки. Регресійний аналіз досліджує взаємозв'язок між довірою до робототехнічних систем та кількома незалежними змінними, включаючи роль уряду, медичних працівників та громадськості. Результати показують, що такі фактори, як покращення дистанційного медичного обслуговування, зменшення кількості людських помилок, скорочення часу відновлення, клінічна ефективність та безпека, можуть негативно впливати на довіру до робототехнічних систем. Загалом, поєднання робототехніки та охорони здоров'я відкриває можливості для поліпшення результатів лікування пацієнтів, операційної ефективності та майбутнього медичного обслуговування, роблячи його більш точним, доступним та ефективним.

У дослідженні [18] розглядається трансформаційний вплив Health Care 4.0 на надання медичних послуг. У ньому досліджується інтеграція кіберфізичних систем, включаючи підключені медичні пристрої, ХТ, аналіз великих даних, AI та СППР, у більш інтелектуальну, взаємопов'язану екосистему охорони здоров'я. У розділі підкреслюється роль цифрового здоров'я в спостереженні за захворюваннями, зміцненні здоров'я, профілактиці, реабілітації та наданні послуг у всьому Азіатсько-Тихоокеанському регіоні. Приклади з практики ілюструють успішні впровадження, підкреслюючи переваги телемедицини в поліпшенні доступу, особливо у віддалених районах, та

прискорене впровадження цифрового здоров'я під час пандемії COVID-19. З оглядом на майбутнє, у тексті визначено нові технології та підкреслено необхідність співпраці між урядами, постачальниками медичних послуг та технологічним сектором для побудови надійної екосистеми цифрового здоров'я. Розглянуто ключові виклики, такі як безпека даних, К та цифрова грамотність, підкреслюючи постійні інновації та адаптацію для підвищення ефективності, Д та результатів лікування пацієнтів.

В іншій статті [19] досліджується застосування біометричних технологій у транспортних компаніях. Біометричні технології набувають все більшого значення у транспортно-логістичному секторі, пропонуючи значний потенціал для ідентифікації та автентифікації в компаніях. Їх впровадження підвищує точність ідентифікації, посилює безпеку процесів ланцюга поставок та створює можливості для інновацій та розвитку бізнесу. Однак їх впровадження також пов'язане з певними проблемами, зокрема високими витратами, технологічними помилками, труднощами з адаптацією та питаннями правового та кібербезпекового характеру. У цій роботі оцінюється застосування біометричних технологій у транспортній та логістичній галузях на основі експертної оцінки, визначаються найважливіші та найменш значущі сильні та слабкі сторони, можливості та загрози. Результати дослідження підкреслюють баланс між перевагами в плані ефективності та безпеки і практичними проблемами, які необхідно вирішити для забезпечення успішного та відповідального впровадження біометричних систем у логістичній галузі.

Нові технології для збереження К в енергетичній системі розглядаються в [20]. У цій оглядовій статті розглядається взаємозв'язок між цифровізацією та К в енергетичному секторі, висвітлюються виклики та можливості, що виникають у результаті інтеграції розподілених енергетичних ресурсів та передових технологій, таких як електромобілі та сучасна інфраструктура обліку. У міру того, як галузь рухається до більш децентралізованого, цифрового та декарбонізованого майбутнього, необхідні надійні заходи щодо захисту цифрової К.

У дослідженні розглядаються чотири технології підвищення К – гомоморфне шифрування, безпечні багатосторонні обчислення, диференціальна К та федеративне навчання – з оцінкою їх механізмів, застосувань та потенціалу для вирішення специфічних для сектора проблем К. Ці методи забезпечують безпечний аналіз даних, спільну обробку, захист індивідуальних записів та децентралізоване машинне навчання відповідно. Розглядаючи ці технології в контексті дотримання нормативних вимог, довіри споживачів та безпеки енергомереж, стаття пропонує комплексну концепцію підвищення рівня К в енергетичних системах.

В іншій статті [21] досліджується інтелектуальна система водопостачання на базі IoT. Очищення, моніторинг та розподіл питної води є життєво важливими компонентами національної КІ, що ставить все більші вимоги до мереж водопостачання (WDN). Ці системи стикаються з нагальними проблемами, такими як зміна клімату, збільшення споживання води через посуху та значні втрати, спричинені витоками під час транспортування.

Для вирішення цих проблем можна застосувати технології IoT та інтелектуальні розподільчі мережі, щоб підвищити ефективність, забезпечити безпеку та можливість раннього виявлення витоків або несанкціонованого використання. Цей підхід, який називається інтелектуальним водопостачанням на основі IoT (SW-IoT), є комплексним концептом сучасного управління водними ресурсами. У цьому огляді розглядається застосування IoT та AI у п'яти ключових сферах: сільське господарство, водоочищення, безпека, WDN та стічні води. Також розглядається відповідне законодавство в ЄС, США,

Канаді, Австралії, Китаї, Японії та Індії, з особливим акцентом на вимогах ЄС щодо обов'язкового використання інтелектуальних рішень для дистанційного збору даних у КІ. Насамкінець, у статті окреслюються поточні напрямки досліджень у сфері SW-IoT та визначаються ключові виклики для майбутніх досліджень.

Цифрова безпека ланцюгів постачання для операторів енергетичного сектору у світлі нових директив та регламентів ЄС описана в [22]. Зростаючий масштаб загроз кібербезпеці систем операційних технологій (ОТ) у КІ призвів до введення більш суворих регуляторних заходів, спрямованих на підвищення кібер- та операційної стійкості. Оскільки цифровий ланцюг поставок стає ключовою областю вразливості, нові регламенти ЄС, включаючи NIS2, Закон про кіберстійкість (CRA) та Кодекс кібербезпеки мережі для енергетичного сектору (NCCES), встановлюють конкретні вимоги для посилення безпеки ланцюга поставок.

У цій статті детально розглядаються ці законодавчі ініціативи, аналізуються їхні наслідки для компаній та працівників КІ, з особливим акцентом на енергетичному секторі. На основі цього аналізу ми пропонуємо набір передових практик для підтримки операторів критичних секторів у досягненні відповідності вимогам, а також визначаємо прогалини, які потребують подальших досліджень, щоб скерувати галузь до більш стійких цифрових ланцюгів постачання.

У дослідницькій роботі [23] досліджується кіберфізичне зміцнення цифрової водної інфраструктури. Системи водопостачання та водовідведення, як КІ, мають важливе значення для здоров'я та добробуту населення. Однак кліматичні зміни, більш суворі нормативні вимоги, демографічні зміни та старіння активів спонукають цей сектор до цифрової трансформації. У цій статті розглядається роль кіберфізичних соціальних систем (КФСС) у мережах розподілу води, що інтегрують фізичну інфраструктуру, цифрові технології та залучення зацікавлених сторін для забезпечення адаптивного та інтелектуального управління.

Основні внески статті включають огляд останніх викликів у сфері безпеки у водогосподарському секторі, підкреслюючи необхідність посилення заходів захисту; дослідження водорозподільних мереж як КФСС, що вимагають цілісного проектування системи; та аналіз сценаріїв кіберфізичних атак, підходів до управління ризиками та цінності інтегрованих знань у зменшенні ризиків. Крім того, у статті розглядається подвійне регуляторне середовище, яке регулює водну інфраструктуру, включаючи Водну рамкову директиву 2000/60/ЄС (WFD), та цифрові сфери, такі як Директива NIS, GDPR та Закон про кібербезпеку. Розглядаючи ці виклики та питання К, дослідження підкреслює, як водопостачальні підприємства можуть посилити безпеку, підвищити стійкість та забезпечити дотримання мінливого законодавства.

Тенденції в європейських дослідницьких проектах, орієнтованих на технологічну екосистему в секторі охорони здоров'я, вивчаються в [24]. Протягом останнього десятиліття сфера охорони здоров'я зазнала стрімкого зростання, а коло зацікавлених сторін розширилося за межі пацієнтів і тепер включає офіційних та неофіційних доглядачів, медичних працівників, дослідницькі установи та постачальників технологій. Це розширення призвело до виникнення різноманітних технологічних екосистем взаємопов'язаних медичних спільнот, спрямованих на впровадження найкращих практик для поліпшення самопочуття пацієнтів та результатів медичного обслуговування. З метою виявлення прогалин та можливостей у цій галузі, у цій статті представлено комплексний огляд екосистем, пов'язаних зі здоров'ям, на основі систематичного дослідження європейських дослідницьких проектів).

Огляд було проведено з використанням баз даних AAL Programme, CORDIS та KEEP. У статті викладено методологію, що застосовувалася, проаналізовано результати для отримання уявлення про евмолюцію європейських проектів у цій галузі, а наприкінці наведено основні висновки та напрямки подальшої роботи.

Наступна стаття [25] описує структуру для візуалізації транзакцій блокчейну в КІ, орієнтовану на користувача. Забезпечення надійності та Ц даних, управління та контролю в КІ стає все більш складним завданням. Нові технології, такі як 5G, загальний АІ та периферійні обчислення, розширюють поверхню атаки, викликаючи нові проблеми безпеки.

Блокчейн пропонує перспективне рішення, забезпечуючи надійний обмін інформацією між розподіленими учасниками за допомогою децентралізованої одноранговоі комунікації та криптографічних механізмів, тим самим підвищуючи Ц та автентичність даних у розумних критичних системах. Однак його псевдоанонімний характер може бути використаний супротивниками, що ускладнює відповідальність та атрибуцію зловмисних дій. Для вирішення цієї проблеми в цій статті пропонується орієнтована на користувача система візуалізації транзакцій блокчейну. На відміну від існуючих інструментів, які в основному покладаються на табличні або лінійні представлення, запропонована система інтегрує дані про транзакції, експертні знання та відгуки користувачів для виявлення аномальних або зловмисних подій. Цей підхід підтримує відстеження даних про злочини, виявлення точок порушення роботи та підвищення стійкості КІ.

Процес оптимізації кіберстійкості в мережі КІ досліджується в [26]. Розширення кіберризиків у цифрових підприємствах з КІ все більше загрожує безперервності системних процесів (SPC), оскільки такі інциденти, як викрадення даних з метою вимагання викупу, порушують взаємозалежні процеси та погіршують безперервність бізнесу.

У цій статті розглядається ключове управлінське питання щодо того, як оптимізувати кіберстійкість – здатність підтримувати SPC шляхом поглинання та адаптації до несприятливих кіберінцидентів – у складних мережевих підсистемах КІ, що складаються з декількох компонентів функціональності процесів (PFC). Ми показуємо, використовуючи алгоритмічний підхід на основі теорії графів, що проблема оптимізації або навіть наближення кіберстійкості в рамках обмеженого бюджету підприємства на кіберзахист є NP-складною. Для вирішення цієї проблеми ми пропонуємо обчислювально доступну графічну систему моделювання Монте-Карло. Ця система розподіляє обмежені ресурси кіберзахисту між PFC пропорційно до їх центральності за Кацем у мережі PFC, тим самим підвищуючи загальну стійкість. Цей підхід пропонує практичну стратегію для менеджерів щодо посилення кіберстійкості КІ в умовах реальних бюджетних обмежень.

В іншій статті [27] описується КІ на основі Індустрії 4.0. Промислова автоматизація та роботизація трансформують виробництво та пов'язані з ним промислові процеси, підвищуючи їхню ефективність та надійність. В основі цих розробок лежать промислові системи управління (ICS), які складаються зі спеціалізованих комп'ютерних компонентів, що значно відрізняються від традиційних бізнес-IT-середовищ. ICS використовуються в багатьох секторах і підпадають під дію різних нормативних рамок, причому Директива ЄС про безпеку інформаційних мереж (NIS) є основним законодавчим інструментом, що зобов'язує держави-члени вирішувати проблеми кібербезпеки. Незважаючи на ці регуляторні та технічні заходи безпеки, зловмисники продовжують атакувати ІКТ-послуги та інфраструктуру, що призводить до інцидентів безпеки, які ставлять під

загрозу К, Ц та Д. Такі інциденти можуть призвести не тільки до фінансових втрат, але й до більш широких системних та соціальних наслідків. У цій статті проводиться глибокий аналіз цих ризиків, висвітлюються вразливі місця ICS, регуляторне середовище та потенційні наслідки порушень кібербезпеки в промислових середовищах.

У статті [28] досліджуються випадки використання квантових обчислень для національної КІ. Квантові обчислення – це нова галузь на стику фізики, математики та інформатики, яка має потенціал для забезпечення обчислювальних можливостей, що значно перевищують можливості класичних систем. На відміну від традиційних комп'ютерів, квантові пристрої обробляють інформацію в квантових бітах (кубітах), які можуть існувати в декількох станах одночасно. Це дозволяє їм виконувати певні обчислення та моделювання в експоненціально швидшому темпі, ніж традиційні архітектури. Однак з точки зору уряду квантова технологія є двосічним мечем: хоча достатньо потужний квантовий комп'ютер може підірвати сучасну криптографію з відкритим ключем і поставити під загрозу конфіденційну інформацію, досягнення в галузі квантової криптографії та квантового розподілу ключів (QKD) обіцяють безпечний зв'язок, стійкий до кібератак. Визнаючи ці ризики та можливості, уряди усього світу інвестують значні кошти в квантові дослідження, щоб забезпечити національні інтереси безпеки та стимулювати економічне зростання. У цьому огляді розглядається стан досліджень і розробок у галузі квантових технологій, що мають значення для КІ, з акцентом на двох ключових сферах: квантовий зв'язок і криптографія та квантові мережі. Кожна сфера розглядається з точки зору потенційних застосувань, можливостей та викликів для безпечного урядового зв'язку. Дослідження також вивчає досягнення в області квантових супутників, квантових дронів та космічних квантових технологій як факторів, що сприяють створенню стійких квантових мереж. На основі проаналізованих досліджень ми дійшли висновку, що, незважаючи на значний прогрес, необхідні подальші дослідження для оцінки доцільності та практичної інтеграції квантових обчислень у національну інфраструктуру.

Реакція цифрових двійників на інциденти з метою підвищення безпеки КІ енергосистеми описана в [29]. Технологія цифрових двійників (ЦД) покращує цифровізацію фізичних активів, надаючи безперервні дані в режимі реального часу для аналізу, що дозволяє краще розуміти ситуацію та знаходити більш ефективні рішення. У цій статті розглядається застосування ЦД в КІ, з особливим акцентом на енергетичному секторі та промислових системах управління (ICS), включаючи сенсорні мережі та системи SCADA. Ми розглядаємо ключові особливості ЦД та їхню актуальність для захисту ICS від вразливостей, таких як семантичні атаки на польові датчики, які можуть порушити роботу. Обговорюється потенціал алгоритмів реагування на інциденти з використанням ЦД для підтримки безпеки та безперебійної роботи. У цьому огляді висвітлюються основні компоненти та напрямки досліджень щодо використання цифрових двійників для підвищення стійкості КІ енергетичного сектору.

У статті [30] досліджується AI для систем, критичних з точки зору безпеки, у промисловій та транспортній галузях. AI має значний потенціал для розробки автономних систем нового покоління, критичних з точки зору безпеки, де алгоритми машинного навчання (МН) можуть оптимізувати рішення та підтримувати інженерів з безпеки.

Однак інтеграція передових технологій ШІ з процесами та стандартами інженерії безпеки залишається серйозним викликом. Це дослідження зосереджується на промисловій та транспортній галузях, структуруючи та аналізуючи фрагментовану літературу про критично важливі для безпеки системи на основі ШІ. Воно розглядає

виклики, техніки та методи, що охоплюють традиційні функціональні системи безпеки та автономні системи, з особливим акцентом на інженерному аспекті надійності ШІ, включаючи інженерні, етичні та юридичні міркування [31-33].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У сфері КІ держави спостерігається зростаюча потреба у забезпеченні ефективності, стійкості та захищеності ТП, з одного боку, та відсутність достатньо розроблених методів, моделей та інструментів, які б інтегрували можливості ХТ у підтримку цих процесів – з іншого. Це протиріччя проявляється між:

– *практичною необхідністю* реалізації багатопараметричного моніторингу, автоматизації та кіберзахисту ТП у КІ держави;

– та *науково-методичною недостатністю* існуючих підходів, які не забезпечують комплексного використання ХТ для підтримки таких процесів.

Таким чином, *актуальність теми* визначається потребою у подоланні цього протиріччя шляхом розроблення нових методів і моделей підтримки ТП у КІ держави на основі ХТ.

У зв'язку з цим постає *завдання дослідження*, яке полягає у розробленні методів та моделей підтримки ТП у КІ держави на основі ХТ, що забезпечать:

– підвищення ефективності та гнучкості управління ТП;

– створення засобів багатопараметричного моніторингу ключових індикаторів ефективності;

– удосконалення інформаційно-комунікаційних систем і мереж для автоматизації виробничих процесів;

– належний рівень кіберзахисту даних;

– формування цілісних підходів, методологій та рекомендацій для впровадження ХТ у КІ держави.

Математична формалізація постановки завдання дослідження може виглядати наступним чином:

1. Відсутність ефективних моделей хмарної підтримки: множина рішень без застосування ХТ $\Omega_{legacy} \cap \mathrm{R} = \emptyset$, тобто існуючі моделі не дозволяють задовільнити вимоги R.

2. Відсутність ефективного багатопараметричного моніторингу: кількість контрольованих показників є меншою за необхідну $q < q_{min}$, а також відсутні ефективні моделі та алгоритми.

3. Брак спеціалізованих ІКСМ для автоматизації ТП: характеристики (у тому числі, що стосується безпеки) не відповідають рекомендованим $\mathrm{C} \neq \mathrm{C}_{req}$ або перевищують (є нижчими) граничні параметри $\ell < \ell_{min} \vee \ell > \ell_{max.}$

4. Недоліки у захищеності даних (К, Ц, Д): ймовірності порушення базових характеристик безпеки $\rho_{conf} > \varepsilon_{conf}$, $\rho_{intgr} > \varepsilon_{intgr,}$ $1 - \alpha > \varepsilon_{avlb}$.

5. Недостатнє дослідження використання ХТ для подібних задач: відсутні достовірні моделі залежностей ефективності $\ell(r)$, затримки $\alpha(r)$ та вартості ресурсів $c(r)$.

6. Відсутність цілісних стандартів та методологій: множина правил S, що визначає обмеження, є повною або суперечливою:

$$R = \bigcap_{s \in S} R_s,$$

$$S = \emptyset \text{ V } \exists s_1, s_2 : R_{s1} \cap R_{s2} \neq \emptyset.$$

Узагальнено визначене наукове протиріччя можна у формалізованому математичному вигляді представити таким чином: система підтримки ТП у КІ держави має працювати ефективно, безпечно і безперервно $(r_1, r_2, \dots, r_n) \in \text{R}$, проте на практиці (в реальних умовах) жодні рішення не задовольняють поставлених вимог $\Omega_{legacy} \cap \text{R} = \emptyset$. Необхідно розробити (удосконалити) методи, моделі та інструменти, що дозволять знайти хоча б одне рішення $\exists (r_1^*, r_2^*, \dots, r_n^*)$: $(r_1^*, r_2^*, \dots, r_n^*) \in \text{R}$.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Martynov, S., Kunytskyi, S., Shatnyi, N., Ivanchuk, O., & Galkina, O. (2022). *Optimization of the technological process of deironing groundwater in critical water supply infrastructure of settlements*. 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), 535–538. https://doi.org/10.1109/CSIT56902.2022.10000724
2. Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 directive in focus. *International Cybersecurity Law Review, 6*, 207–220. https://doi.org/10.1365/s43439-025-00154-4
3. Pastorek, A., & Tundis, A. (2024). Navigating the landscape of IoT security and associated risks in critical infrastructures. *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24)*, Article 112, 1–7. https://doi.org/10.1145/3664476.3669979
4. Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology, 1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211
5. Giannakidou, S., et al. (2022). 5G-enabled NetApp for predictive maintenance in critical infrastructures. *2022 5th World Symposium on Communication Engineering*, 129–132. https://doi.org/10.1109/WSCE56210.2022.9916037
6. Wakolbinger, C., Fickert, L., Brandauer, W., Aigner, M., & Malleck, H. (2013). A vigilant concept for smart emergency supply of critical infrastructure. *International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*, 1–4.
7. Woltjer, R., Hermelin, J., Nilsson, S., Oskarsson, P.-A., & Hallberg, N. (2018). Using requirements engineering in the development of resilience guidelines for critical infrastructure. *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, 615–622. https://doi.org/10.1109/SYSOSE.2018.8428749
8. Malik, M. Z., Nazir, S., & Khan, H. U. (2023). Artificial intelligence based system on enhancing the capabilities of transport system: A systemic literature review. *2023 IEEE Symposium on Industrial Electronics & Applications*, 1–6. https://doi.org/10.1109/ISIEA58478.2023.10212340
9. Chen, K., Zhou, X., Bao, Z., et al. (2025). Artificial intelligence in infrastructure construction: A critical review. *Frontiers in Engineering Management, 12*, 24–38. https://doi.org/10.1007/s42524-024-3128-5
10. Odeh, J. O., Yang, X., Samuel, O. W., et al. (2025). Systematic investigation of privacy preservation techniques for industrial IoT-enabled critical edge network infrastructure. *Cluster Computing, 28*, 407. https://doi.org/10.1007/s10586-025-05114-5
11. Arpagian, N. (2024). The threat of technological obsolescence for cybersecurity in the energy sector. In A. Barichella & J. Yada (Eds.), *The Palgrave handbook of cybersecurity, technologies and energy transitions*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-04196-9_6-1
12. Borah, G. (2025). Urban water stress: Climate change implications for water supply in cities. *Water Conservation Science and Engineering, 10*, 20. https://doi.org/10.1007/s41101-025-00344-5
13. Jackson, J. S., Kantamaneni, K., Ganeshu, P., et al. (2025). Assessment of the role of nanotechnology in water sector: An expert opinion. *International Journal of Energy and Water Resources*. https://doi.org/10.1007/s42108-025-00389-1
14. Turja, T., Kork, A. A., Ilomäki, S., et al. (2025). Care robot literacy: Integrating AI ethics and technological literacy in contemporary healthcare. *AI and Ethics, 5*, 2623–2640. https://doi.org/10.1007/s43681-024-00576-6
15. Ren, H., Kwok, Q., Sun, M., et al. (2025). Toward artificial general intelligence in health care. *The Visual Computer, 41*, 7341–7350. https://doi.org/10.1007/s00371-025-03808-w

16. Ojo-Gonzalez, K., Bonilla-Morales, B., & Vargas-Lombardo, M. (2024). Software quality in the IoT in health sector and commerce sector. In T. Guarda, F. Portela, & J. M. Diaz-Nafria (Eds.), *Advanced research in technologies, information, innovation and sustainability (ARTIIS 2023)* (Vol. 1935). Springer. https://doi.org/10.1007/978-3-031-48858-0_2
17. Urkude, S. V., & Sahoo, D. (2025). Adoption of robotics technology in health care: An empirical study in emerging economy. In V. Bhateja et al. (Eds.), *Innovations in information and decision sciences (FICTA 2024, Vol. 422)*. Springer. https://doi.org/10.1007/978-981-96-0147-9_24
18. Goh, J. J. K. (2025). Digital health and technology adoption in public health. In B. Y. F. Fong (Ed.), *The handbook of public health in the Asia-Pacific*. Springer. https://doi.org/10.1007/978-981-97-1788-0_32-1
19. Balevičiūtė, J., Šopaga, G., & Jarašūnienė, A. (2025). Application of biometric technologies in transport and logistics companies. In O. Prentkovskis et al. (Eds.), *TRANSBALTICA XV: Transportation science and technology*. Springer. https://doi.org/10.1007/978-3-031-85390-6_31
20. Cali, U., Gourisetti, S. N. G., Sebastian-Cardenas, D. J., et al. (2024). Emerging technologies for privacy preservation in energy systems. *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24)*, 163–170. https://doi.org/10.1145/3655693.3656546
21. Slany, V., Krcalova, E., Balej, J., Zach, M., Kucova, T., Prauzek, M., & Martinek, R. (2025). Smart Water-IoT: Harnessing IoT and AI for efficient water management. *ACM Computing Surveys*, *57*(12), Article 304. https://doi.org/10.1145/3744338
22. Nygard, A. R., & Katsikas, S. (2025). Digital supply chain security for power sector operators in the light of the new EU directives and regulation. *Proceedings of PCI '24*, 70–80. https://doi.org/10.1145/3716554.3716565
23. Cali, Ü., Catak, F. Ö., Balogh, Z. G., Ugarelli, R., & Jaatun, M. G. (2023). Cyber-physical hardening of the digital water infrastructure. *Proceedings of EICC '23*, 181–188. https://doi.org/10.1145/3590777.3591408
24. Marcos-Pablos, S., García-Holgado, A., & García-Peñalvo, F. J. (2018). Trends in European research projects focused on technological ecosystems in the health sector. *Proceedings of TEEM'18*, 495–503. https://doi.org/10.1145/3284179.3284263
25. Jeyakumar, S. T., Ko, R., & Muthukkumarasamy, V. (2023). A framework for user-centric visualisation of blockchain transactions in critical infrastructure. *Proceedings of BSCI '23*, 44–52. https://doi.org/10.1145/3594556.3594624
26. Pal, R., Sequeira, R. X., Zeijlmaker, S., & Siegel, M. (2025). Optimizing cyber-resilience in critical infrastructure networks. *Proceedings of the Winter Simulation Conference (WSC '24)*, 774–785.
27. Bederna, Z., & Szadeczky, T. (2022). Industry 4.0-based critical infrastructure and the NIS Directive. *Proceedings of CEEeGov '22*, 93–99. https://doi.org/10.1145/3551504.3551546
28. Alghamdi, M., & Alghamdi, S. (2024). Exploring quantum computing use cases for critical national infrastructures. *Proceedings of ICFNDS '23*, 25–32. https://doi.org/10.1145/3644713.3644718
29. Akerele, A., Leppert, W., Somerville, S., & Amoussou, G.-A. (2023). The digital twins incident response to improve the security of power system critical infrastructure. *Journal of Computer Science Colleges, 39*(3), 86–99.
30. Perez-Cerrolaza, J., Abella, J., Borg, M., Donzella, C., Cerquides, J., Cazorla, F. J., Englund, C., Tauber, M., Nikolakopoulos, G., & Flores, J. L. (2024). Artificial intelligence for safety-critical systems in industrial and transportation domains: A survey. *ACM Computing Surveys, 56*(7), Article 176. https://doi.org/10.1145/3626314
31. Lee, J. (2025). Narrative-based AI ethics education for emerging technologies: Leveraging 'The Monkey's Paw' for AI alignment and social justice. *2025 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, 1. https://doi.org/10.1109/ETHICS65148.2025.11098410
32. Wiese, L., Rathinam, S. S., Oschinski, M., DeWitt, B., & Schiff, D. S. (2025). AI ethics and governance in the job market: Trends, skills, and sectoral demand. *IEEE Transactions on Technology and Society*. https://doi.org/10.1109/TTS.2025.3567143
33. Potasznik, A. (2025). Press release ethics in AI: Performative ethics in for-profit AI companies. *2025 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, 1–10. https://doi.org/10.1109/ETHICS65148.2025.11098431
34. 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
35. 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

36. Al-Mudhafar Aqeel, 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 machine learning. *Advanced Information Systems, 7*(2), 49–56. https://www.scopus.com/pages/publications/85176960353
37. 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
№ 3 (31), 2025
ISSN 2663 - 4023

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 CLOUD TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE METHODS FOR THE IMPLEMENTATION OF TECHNOLOGICAL PROCESSES IN CRITICAL INFRASTRUCTURE OF THE STATE

Abstract. The paper conducted a study of scientific publications and research projects on the support of technological processes in the critical infrastructure of the state. An objective contradiction was identified (manifested between the practical need to implement multi-parameter monitoring, automation and cyber protection of technological processes in the critical infrastructure of the state and the scientific and methodological insufficiency of existing approaches that do not provide for the integrated use of cloud technologies to support such processes). The formulation of a further scientific task was formalized, which consists in developing methods and models for supporting technological processes in the critical infrastructure of the state based on cloud technologies, which will ensure: increasing the efficiency and flexibility of technological process management; creating means of multi-parameter monitoring of key performance indicators; improving information and communication systems and networks for the automation of production processes; an appropriate level of cyber protection of data; forming holistic approaches, methodologies and recommendations for the implementation of cloud technologies in the critical infrastructure of the state.

Keywords: critical infrastructure security, information technology, technological processes, cloud technologies, artificial intelligence, Internet of Things.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Martynov, S., Kunytskyi, S., Shatnyi, N., Ivanchuk, O., & Galkina, O. (2022). *Optimization of the technological process of deironing groundwater in critical water supply infrastructure of settlements*. 2022 IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT), 535–538. https://doi.org/10.1109/CSIT56902.2022.10000724
2. Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 directive in focus. *International Cybersecurity Law Review, 6*, 207–220. https://doi.org/10.1365/s43439-025-00154-4
3. Pastorek, A., & Tundis, A. (2024). Navigating the landscape of IoT security and associated risks in critical infrastructures. *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24)*, Article 112, 1–7. https://doi.org/10.1145/3664476.3669979
4. Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology, 1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211
5. Giannakidou, S., et al. (2022). 5G-enabled NetApp for predictive maintenance in critical infrastructures. *2022 5th World Symposium on Communication Engineering*, 129–132. https://doi.org/10.1109/WSCE56210.2022.9916037
6. Wakolbinger, C., Fickert, L., Brandauer, W., Aigner, M., & Malleck, H. (2013). A vigilant concept for smart emergency supply of critical infrastructure. *International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*, 1–4.
7. Woltjer, R., Hermelin, J., Nilsson, S., Oskarsson, P.-A., & Hallberg, N. (2018). Using requirements engineering in the development of resilience guidelines for critical infrastructure. *2018 13th Annual Conference on System of Systems Engineering (SoSE)*, 615–622. https://doi.org/10.1109/SYSOSE.2018.8428749

8. Malik, M. Z., Nazir, S., & Khan, H. U. (2023). Artificial intelligence based system on enhancing the capabilities of transport system: A systemic literature review. *2023 IEEE Symposium on Industrial Electronics & Applications*, 1–6. https://doi.org/10.1109/ISIEA58478.2023.10212340
9. Chen, K., Zhou, X., Bao, Z., et al. (2025). Artificial intelligence in infrastructure construction: A critical review. *Frontiers in Engineering Management, 12*, 24–38. https://doi.org/10.1007/s42524-024-3128-5
10. Odeh, J. O., Yang, X., Samuel, O. W., et al. (2025). Systematic investigation of privacy preservation techniques for industrial IoT-enabled critical edge network infrastructure. *Cluster Computing, 28*, 407. https://doi.org/10.1007/s10586-025-05114-5
11. Arpagian, N. (2024). The threat of technological obsolescence for cybersecurity in the energy sector. In A. Barichella & J. Yada (Eds.), *The Palgrave handbook of cybersecurity, technologies and energy transitions*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-04196-9_6-1
12. Borah, G. (2025). Urban water stress: Climate change implications for water supply in cities. *Water Conservation Science and Engineering, 10*, 20. https://doi.org/10.1007/s41101-025-00344-5
13. Jackson, J. S., Kantamaneni, K., Ganeshu, P., et al. (2025). Assessment of the role of nanotechnology in water sector: An expert opinion. *International Journal of Energy and Water Resources*. https://doi.org/10.1007/s42108-025-00389-1
14. Turja, T., Kork, A. A., Ilomäki, S., et al. (2025). Care robot literacy: Integrating AI ethics and technological literacy in contemporary healthcare. *AI and Ethics, 5*, 2623–2640. https://doi.org/10.1007/s43681-024-00576-6
15. Ren, H., Kwok, Q., Sun, M., et al. (2025). Toward artificial general intelligence in health care. *The Visual Computer, 41*, 7341–7350. https://doi.org/10.1007/s00371-025-03808-w
16. Ojo-Gonzalez, K., Bonilla-Morales, B., & Vargas-Lombardo, M. (2024). Software quality in the IoT in health sector and commerce sector. In T. Guarda, F. Portela, & J. M. Diaz-Nafria (Eds.), *Advanced research in technologies, information, innovation and sustainability (ARTIIS 2023)* (Vol. 1935). Springer. https://doi.org/10.1007/978-3-031-48858-0_2
17. Urkude, S. V., & Sahoo, D. (2025). Adoption of robotics technology in health care: An empirical study in emerging economy. In V. Bhateja et al. (Eds.), *Innovations in information and decision sciences (FICTA 2024, Vol. 422)*. Springer. https://doi.org/10.1007/978-981-96-0147-9_24
18. Goh, J. J. K. (2025). Digital health and technology adoption in public health. In B. Y. F. Fong (Ed.), *The handbook of public health in the Asia-Pacific*. Springer. https://doi.org/10.1007/978-981-97-1788-0_32-1
19. Balevičiūtė, J., Šopaga, G., & Jarašūnienė, A. (2025). Application of biometric technologies in transport and logistics companies. In O. Prentkovskis et al. (Eds.), *TRANSBALTICA XV: Transportation science and technology*. Springer. https://doi.org/10.1007/978-3-031-85390-6_31
20. Cali, U., Gourisetti, S. N. G., Sebastian-Cardenas, D. J., et al. (2024). Emerging technologies for privacy preservation in energy systems. *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference (EICC '24)*, 163–170. https://doi.org/10.1145/3655693.3656546
21. Slany, V., Krcalova, E., Balej, J., Zach, M., Kucova, T., Prauzek, M., & Martinek, R. (2025). Smart Water-IoT: Harnessing IoT and AI for efficient water management. *ACM Computing Surveys*, *57*(12), Article 304. https://doi.org/10.1145/3744338
22. Nygard, A. R., & Katsikas, S. (2025). Digital supply chain security for power sector operators in the light of the new EU directives and regulation. *Proceedings of PCI '24*, 70–80. https://doi.org/10.1145/3716554.3716565
23. Cali, Ü., Catak, F. Ö., Balogh, Z. G., Ugarelli, R., & Jaatun, M. G. (2023). Cyber-physical hardening of the digital water infrastructure. *Proceedings of EICC '23*, 181–188. https://doi.org/10.1145/3590777.3591408
24. Marcos-Pablos, S., García-Holgado, A., & García-Peñalvo, F. J. (2018). Trends in European research projects focused on technological ecosystems in the health sector. *Proceedings of TEEM'18*, 495–503. https://doi.org/10.1145/3284179.3284263
25. Jeyakumar, S. T., Ko, R., & Muthukkumarasamy, V. (2023). A framework for user-centric visualisation of blockchain transactions in critical infrastructure. *Proceedings of BSCI '23*, 44–52. https://doi.org/10.1145/3594556.3594624
26. Pal, R., Sequeira, R. X., Zeijlmaker, S., & Siegel, M. (2025). Optimizing cyber-resilience in critical infrastructure networks. *Proceedings of the Winter Simulation Conference (WSC '24)*, 774–785.
27. Bederna, Z., & Szadeczky, T. (2022). Industry 4.0-based critical infrastructure and the NIS Directive. *Proceedings of CEEeGov '22*, 93–99. https://doi.org/10.1145/3551504.3551546
28. Alghamdi, M., & Alghamdi, S. (2024). Exploring quantum computing use cases for critical national infrastructures. *Proceedings of ICFNDS '23*, 25–32. https://doi.org/10.1145/3644713.3644718

29. Akerele, A., Leppert, W., Somerville, S., & Amoussou, G.-A. (2023). The digital twins incident response to improve the security of power system critical infrastructure. *Journal of Computer Science Colleges, 39*(3), 86–99.
30. Perez-Cerrolaza, J., Abella, J., Borg, M., Donzella, C., Cerquides, J., Cazorla, F. J., Englund, C., Tauber, M., Nikolakopoulos, G., & Flores, J. L. (2024). Artificial intelligence for safety-critical systems in industrial and transportation domains: A survey. *ACM Computing Surveys, 56*(7), Article 176. https://doi.org/10.1145/3626314
31. Lee, J. (2025). Narrative-based AI ethics education for emerging technologies: Leveraging 'The Monkey's Paw' for AI alignment and social justice. *2025 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, 1. https://doi.org/10.1109/ETHICS65148.2025.11098410
32. Wiese, L., Rathinam, S. S., Oschinski, M., DeWitt, B., & Schiff, D. S. (2025). AI ethics and governance in the job market: Trends, skills, and sectoral demand. *IEEE Transactions on Technology and Society*. https://doi.org/10.1109/TTS.2025.3567143
33. Potasznik, A. (2025). Press release ethics in AI: Performative ethics in for-profit AI companies. *2025 IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)*, 1–10. https://doi.org/10.1109/ETHICS65148.2025.11098431
34. 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
35. 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
36. Al-Mudhafar Aqeel, 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 machine learning. *Advanced Information Systems, 7*(2), 49–56. https://www.scopus.com/pages/publications/85176960353
37. 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

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.