https://orcid.org/0000-0002-9639-3544

УДК 004.457

О.Є. КОВАЛЕНКО[*, **]

КОНВЕРГЕНЦІЯ ІНТЕРНЕТУ РЕЧЕЙ ТА СИСТЕМ СИТУАЦІЙНОГО УПРАВЛІННЯ

[*]Національний університет біоресурсів і природокористування України, м. Київ, Україна
[**]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *Особливе значення оперативного і точного інформування у процесах ситуаційного управління у критичних сферах застосування набуває запобігання та усунення наслідків катастрофічних явищ, управління військовими операціями, медична діяльність, управління енергетичними системами тощо. Цілі та задачі діяльності в цих сферах визначають і специфіку побудови відповідних систем ситуаційного управління для них. Функціонування систем ситуаційного управління засноване на отриманні точної та оперативної інформації про середовище, в якому здійснюється ситуаційне управління. Конвергенція систем ситуаційного управління з засобами бездротових сенсорних мереж (Wireless Sensor Networks, WSN) та інтернету речей (Internet of Things, IoT) забезпечує отримання такої інформації. У статті проведено аналіз засобів інтернету речей із точки зору здатності поєднання в системах ситуаційного управління для вирішення проблем управління в різних сферах діяльності. Розглянуто особливості побудови та переваги використання ситуаційних систем на основі IoT у різних сферах діяльності. Конвергенція IoT у ситуаційних системах різного типу вимагає розв'язання типових для IoT задач, пов'язаних з організацією гетерогенного мережевого середовища з контрольованим енергоспоживанням і необхідністю обробки великих об'ємів даних. Показано, що сфера застосування визначає специфічні вимоги до побудови систем ситуаційного управління і в кожному конкретному випадку система вимог орієнтована на підтримку критичної вимоги. Однією з основних проблем конвергенції IoT та систем ситуаційного управління є складність стандартизації середовища функціонування. Множинність та різноманіття варіантів можливих рішень при розробці таких систем обумовлює необхідність застосування інтелектуальних технологій розробки систем із застосуванням штучного інтелекту і моделей знань цільової предметної сфери.*

Ключові слова: *ситуаційна система, інтернет речей, кіберконвергентна система, гетерогенні мережі.*

Abstract. *Quick and accurate provision of information in the processes of situational management acquires special importance in the critical areas of application – the prevention and elimination of the consequences of catastrophic events, the management of military operations, medical activities, the management of energy systems, etc. The goals and objectives of activities in these areas also determine the specifics of building appropriate situation management systems for them. The functioning of such systems is based on obtaining accurate and current information about the environment in which situational management is carried out. The convergence of situation management systems with the means of wireless sensor networks (Wireless Sensor Networks, WSN) and the Internet of Things (IoT) ensures obtaining such information. The article analyzes the means of the Internet of Things from the point of view of their ability to be combined in situation management systems to solve management problems in various spheres of activity. The construction features and advantages of using situational systems based on IoT in various spheres of activity are considered. The convergence of IoT in situational systems of various types requires the solution of IoT-typical tasks related to the organization of a heterogeneous network environment with controlled energy consumption and the need to process large volumes of data. The paper demonstrates that the scope of application determines the specific requirements for the construction of situation management systems, and in each specific case the system of requirements is focused on the support of a critical requirement. One of the main problems of the convergence of IoT and situation management systems is the difficulty of standardizing the operating environment. The multiplicity and variety of options for*

possible solutions in the development of such systems determine the need for the use of intelligent technologies for the development of systems with the use of artificial intelligence and knowledge models of the target subject area.
Keywords: *situational system, Internet of Things, cyber-convergent system, heterogeneous networks.*

DOI: 10.34121/1028-9763-2023-3-89-103

1. Вступ

Використання інформаційних технологій у різних галузях діяльності людства забезпечує зростання їх ефективності на основі поєднання передових досягнень предметної галузі з можливостями цифрової обробки інформації. Переважна більшість проблем управління в різних галузях залишається неформалізованими і розв'язуються на основі ситуаційного підходу. Ситуація розглядається як усвідомлене знання суб'єкта про динаміку навколишнього середовища, представленого певними типами інформаційних повідомлень, що є основою для побудови обґрунтованої інтерпретації послідовності зміни станів (динаміки) світу (предметної області) з певної точки зору [1]. Ситуаційне управління – це метод управління, заснований на використанні сімейства концепцій, моделей та наявних технологій для розпізнавання, пояснення, впливу та прогнозування ситуацій, які виникли або можуть виникнути в динамічній комплексній системі за визначений час роботи [2]. Таким чином, ситуаційне управління являє собою цілеспрямовану індивідуальну або колективну діяльність, пов'язану з розпізнаванням, поясненням і прогнозуванням ситуацій, які виникли або можуть виникнути в динамічних системах, та впливом на них із використанням відповідних концепцій, моделей і технологій. Представлення об'єктів предметної сфери у вигляді віртуалізованих кіберсутностей (Cyber Entities, CE) дозволяє застосувати до управління цими об'єктами модельно-орієнтований підхід у середовищі кіберконвергентних систем [3, 4].

Кіберконвергентна система фокусується головним чином на кіберсутностях, які існують у кіберсвіті та можуть бути пов'язані з об'єктом у кіберпов'язаних світах для розв'язування відповідних задач управління цими об'єктами. Таким чином, у кіберконвергентних системах поєднуються компоненти двох основних категорій: категорії кіберсвіту та категоріях, пов'язаних із кібернетичною інформацією. Ці дві категорії природно представляються ситуаційними агентами [5]. Загалом кібероб'єкт (кіберсутність) можна визначити як такий, що існує в кіберпросторі або є чисто комп'ютерним синтезом, або тісно пов'язаний із реальним об'єктом у фізичному, соціальному та психічному просторах [6, 7]. Функціонування систем ситуаційного управління засноване на отриманні точної та оперативної інформації про середовище, в якому здійснюється ситуаційне управління. Конвергенція систем ситуаційного управління з засобами бездротових сенсорних мереж (Wireless Sensor Networks, WSN) та інтернету речей (Internet of Things, IoT) забезпечує отримання такої інформації.

Метою дослідження є аналіз засобів інтернету речей із точки зору здатності поєднання в системах ситуаційного управління для вирішення проблем управління в різних сферах діяльності.

2. Особливості ситуаційного управління в кіберконвергентних системах

Ситуаційне управління здійснюється в межах ситуаційних систем різного типу [8]. Особливе значення оперативного і точного інформування у процесах ситуаційного управління у критичних сферах застосування набуває запобігання та усунення наслідків катастрофічних явищ, управління військовими операціями, медична діяльність, управління енергетичними системами тощо. Цілі та задачі діяльності в цих сферах визначають і специфіку побудови відповідних систем ситуаційного управління для них. Розглянемо ці особливості.

Ситуаційний аналіз

Основою адекватного ситуаційного управління є ситуаційний аналіз, який допомагає розробити основу для розуміння середовища, в якому виконується план. Він забезпечує загальну точку відліку для процесу планування та визначає пріоритетність дій.

Ситуаційний аналіз може забезпечити оцінку ризиків і переваг для проєкту та залучених організацій від того, як реалізується процес комунікації. Це миттєвий знімок організації чи ситуації або стану речей на певний момент часу. Іноді це здійснюється за допомогою SWOT-аналізу (сильні сторони, слабкі сторони, можливості та загрози), який вивчає всі аспекти щодо успіху або результатів відповідного проєкту. Зрозуміло, що якщо комунікаційна діяльність буде погано підготовлена та реалізована через погане розуміння конкретної ситуації, проєкт може мати фатальне завершення через брак інформованості та довіри суспільства. Ситуаційний аналіз може допомогти визначити потенційно слабкі сторони проєкту, дозволяючи передбачити необхідні зміни до того, як буде завдано непоправні шкодливі дії. Ситуаційний аналіз також допоможе визначити, де можуть існувати можливості для розвитку стратегічних альянсів із групами зацікавлених сторін підтримки і покаже де можна докласти додаткових зусиль для їх розвитку. Ситуаційний аналіз також може допомогти визначити спроможності в середині організації з точки зору виконання вимог комунікаційного плану до його розробки для реалізації стратегії. Він також слугує для того, щоб висвітлити ті сфери стратегії, які, можливо, потребують покращення, щоб врахувати поточну ситуацію або ситуацію, що розвивається. Підтримка актуального ситуаційного аналізу також допоможе визначити можливі розриви і неточності у очікуваному плані впровадження.

Визначення бачення-місії-цілей

При розробці стратегії необхідно визначити та зрозуміти основну мету і цілі стратегії. Це може бути настільки просто, як інформування якомога більшої кількості зацікавлених сторін, або це може включати конкретні цілі, такі як охоплення певних груп зацікавлених сторін, проведення певної кількості зустрічей або навіть отримання підтримки для просування проєкту. Хоча можна мати кілька цілей для комунікаційної діяльності. Важливо встановити цілі, яких можна практично досягти.

Для забезпечення належного рівня участі громадськості планування стратегії має починатися на ранній стадії (на етапі ініціації проєкту), щоб спілкування та участь могли бути інтегровані у процес прийняття рішень у проекті. Ключовою є чітко визначена мета, яка не є надто розпливчастою чи широкою. Якщо мета надто розпливчаста, тоді повідомлення не буде помітним для зацікавлених сторін у процесі прийняття рішень. Якщо мета надто широка, повідомлення втратить будь-який вплив, і в будь-якому випадку успіх буде неможливо виміряти.

Ключ до розробки адекватних цілей ґрунтується на моделі SMART [9]:

***S**pecific* (конкретність) – мета чітко визначає, що планується робити і як саме це можна зробити. Серед запитань, які варто поставити, є: «Що планується робити? Чому це важливо? Хто збирається це робити?»

***M**easurable* (вимірність) – потрібно визначити вимірники мети, наприклад, відсоток залучених осіб, кількість завершених процесів (операцій) тощо.

***A**chievable* (досяжність) – мета має бути досяжною з урахуванням місцевих умов, періоду часу, виділених ресурсів тощо.

***R**ealistic* (реалістичність) – цілі мають бути досягнуті з урахуванням наявних часових, матеріальних та людських ресурсів.

***T**ime-bound* (прив'язаність до часу) – мета має бути чітко визначена з урахуванням обмежень часу, потрібного для її досягнення.

3. Сенсорні мережі та інтернет речей

Отримання інформації про стан середовища управління здійснюється з використанням сенсорних мереж. Бездротові сенсорні мережі (WSN) забезпечують універсальність, масштабованість та всепроникність сенсорних мереж у середовищі управління [10].

WSN є стандартизованим сервісом, який реалізується в комерційних і промислових проєктах на основі використання вбудованих мікроконтролерів із низьким енергоспоживанням та засобів телекомунікацій. Архітектура бездротової сенсорної мережі складається з вузлів, які використовуються для спостереження за навколишнім середовищем: температура, вологість, тиск, положення, вібрація, звук тощо. Ці вузли можна використовувати в різних програмах реального часу для виконання різноманітних завдань, таких як інтелектуальне виявлення, виявлення сусідніх вузлів, обробка та зберігання даних, збір даних, відстеження цілей, моніторинг та контроль, синхронізація, локалізація вузлів та ефективна маршрутизація між базовою станцією та вузлами.

Інтернет речей (Internet of Things, IoT) – концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини. Незважаючи на багато спільних рис, між IoT та WSN є відмінні, які представлені у табл. 1.

Таблиця 1 – Відмінності між технологіями інтернету речей та сенсорними мережами

Інтернет речей	Бездротові сенсорні мережі
Технологія, яка підключає обладнання до Інтернету, щоб воно могло спілкуватися з іншими пристроями та обмінюватися даними	Використовується для відстеження та збору інформації про фізичні та навколишні умови
Складається з меншої кількості пристроїв, підключених до Інтернету через дротове або бездротове з’єднання	Складається з великої кількості маленьких малопотужних датчиків, які бездротовим способом передають дані на центральну базову станцію
Більш загальний і універсальний	Створено для роботи в певних налаштуваннях для певних потреб
Покладається на галузеві стандартні протоколи, наприклад, TCP/IP	Використовуйте запатентовані технології та протоколи
Більш децентралізований і включає багато організацій і людей	Розгортається в межах окремої організації
Відкрита система	Закриті системи
Більш динамічний, із пристроями та речами, які переміщуються та підключаються до кількох мереж	Статичні, з датчиками, розміщеними в певному місці і залишаються у цьому місці
Використовується для збору даних, моніторингу, керування та комунікацій	Включає збір даних і моніторинг

4. Конвергенція IoT у кібермедичних системах

Охорона здоров'я є однією із сфер застосування IoT. Портативні пристрої моніторингу стану здоров'я на основі IoT можуть значно скоротити відстань між пацієнтом і лікарем. IoT дозволяє підійти індивідуально до кожного пацієнта, проаналізувати стан його здоров'я та розрахувати індивідуальний метод лікування. За допомогою портативних датчиків лікарі можуть віддалено контролювати стан здоров'я пацієнтів і реагувати в режимі реального часу. Однак метрики в реальному часі потребують безперервного підключення до Інтернету, незважаючи на те, що IoT в охороні здоров'я швидко розвивається, але все ще не в повній мірі використовується в деяких галузях медицини [11].

Сучасні медичні працівники стикаються з необхідністю збору великої кількості даних, їх аналізом та інтерпретацією для прийняття обґрунтованих та персоналізованих рішень. Все це вимагає чималих зусиль і часу. Нові технології IoT можуть прискорити та полегшити даний процес. У зв'язку з масовим впровадженням електронних медичних систем спостерігається зростання кількості оцифрованих медичних даних. Повний перегляд і оцінка всієї цієї інформації займає багато часу. Крім того, потрібне також навчання медичного персоналу технології, заснованій на ШІ, яка дуже пов'язана з IoT [12].

Завдяки скоординованим діям таких цифрових технологій, як IoT та ШІ, лікарі можуть краще адаптувати лікування до потреб пацієнтів. Завдяки цим технологіям можна обробляти значно більший обсяг інформації, зберігати та аналізувати її, щоб уважно стежити за перебігом певної хвороби чи процесу. Уміле поєднання практичного особистого досвіду з можливостями нових методів діагностики, збору та аналізу приведе до позитивних змін в управлінні охороною здоров'я [13]. Рис. 1 представляє концепцію IoT в охороні здоров'я.

Рисунок 1 – Концепція IoT в охороні здоров'я

Згодом IoT представляє мережеві технології, що включають портативні пристрої, які можуть запускати, виявляти, синергізувати та з'єднуватися з іншими порівнянними медіа в Інтернеті [14]. IoT глибоко змінює виробництво, використання та розповсюдження даних. Пересічні суб'єкти часто використовують ці системи, щоб стежити за своєю дієтою,

сном, життєвими показниками, фізичними вправами та іншими фізичними станами, тоді як технології IoT періодично збирають і обробляють екологічні дані, які впливають на здоров'я людини. Зрештою ця сумісність поклала початок новому виробництву медичних альтернатив.

5. Конвергенція IoT у системах управління ризиками катастроф

Необхідність оперативного усвідомлення ситуації в управлінні ризиками катастроф породжує проблему швидкої підготовки даних про катастрофи [15]. Управління ризиками катастроф вимагає особливого втручання з точки зору протоколів, тому що кожен тип катастрофи має своє поняття виникнення, час аварії, здатність до шкоди. Наприклад, зсуви часто локалізовані, тоді як землетруси впливають на великий географічний регіон. Крім того, ці катастрофи мають різний вплив на життя людей та інфраструктуру. Таким чином, необхідно розглянути декілька питань при виборі інфраструктури та багаторівневих каркасних протоколів. Крім того, легкі та енергоефективні протоколи на основі IoT корисні для виявлення локальних сенсорних пристроїв і шлюзів для безпечного запуску зв'язку. Оскільки катастрофічні ситуації завжди відключають постраждалий регіон від зовнішнього середовища, використовуючи дротові лінії зв'язку, наприклад, повітряні дроти, антени та оптичні канали, дуже важливо враховувати можливості мережі. На рис. 2 показано підтримувані IoT протоколи зв'язку, придатні для управління катастрофами.

Рисунок 2 – Еталонна модель стека протоколів для управління ризиками катастроф на основі IoT

Еталонна модель стека протоколів описує, як сім рівнів протоколів узгоджено взаємопов'язані один з одним для обробки катастрофічних подій із точки зору швидкого з'єднання, гетерогенних зв'язків між об'єктами, доступу до захищеної інформації та виявлення об'єкта (наприклад, людей та інших джерел існування). Хоча подання цих рівнів відповідає певній цілісності щодо управління катастрофічними подіями, воно зовсім не стандартизоване. Цей узагальнюючий аспект базується на спеціалізації його шарів. Більшість протоколів зазвичай використовуються в типових моделях OSI або TCP/IP. Деякі з них нещодавно включені до цієї тимчасової та нової еталонної моделі [16]. Під час розробки даної еталонної моделі узгодженість обмежена, тобто від найнижчого рівня пристроїв до найвищого рівня додатків IoT. Повна модель вертикально захищена за допомогою рівня безпеки, який підтримують відкритий торговий протокол (OTP) і протокол X.509, придатний для додатків на основі Інтернету речей.

6. Конвергенція IoT у військових системах

Інтернет військових/бойових речей (Internet of Military/Battlefield Things, IoM/BT) – це мережа датчиків, переносних пристроїв і пристроїв Інтернету речей, які використовують хмарні та граничні обчислення для створення згуртованої бойової сили. Майбутнє військових операцій стає високотехнологічним, і все більше значення в них набуває Інтернет речей для бойового спорядження із вбудованими біометричними переносними пристроями, що допомагає солдатам ідентифікувати ворога, підвищити ефективність у бою та отримати доступ до засобів і систем зброї з використанням швидкісних граничних обчислень. Інтернет речей має потужні військові застосунки, які об'єднують кораблі, літаки, танки, безпілотники, солдатів і операційні бази в єдину мережу, яка підвищує ситуаційну обізнаність, забезпечує оцінку ризиків і зменшує час реагування.

Використання IoM/BT приводить до революційних змін у веденні сучасної війни, застосовуючи дані для підвищення ефективності бою, а також зменшення збитків і втрат за допомогою автоматизованих дій, одночасно зменшуючи навантаження на бійців-людей. Наразі системи командування, управління, зв'язку, комп'ютерів, розвідки, спостереження та дослідження (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, C4ISR) використовують мільйони датчиків, розгорнутих на ряді платформ, щоб надати ситуаційну обізнаність військовим командирам і військам на землі, на морі та в повітрі. Однак справжня сила полягає у взаємозв'язку пристроїв і обміні сенсорною інформацією, яка дозволить людям зрозуміти величезний, складний, заплутаний і потенційно оманливий океан інформації. У сценаріях на полі бою зв'язок між стратегічними військовими засобами, такими як літаки, військові кораблі, бронетехніка, наземні станції та солдати, може привести до покращеної координації, яку може забезпечити IoM/BT. Однак, щоб стати реальністю, це бачення має подолати кілька технічних обмежень поточних інформаційних систем і мереж. На рис. 3 показано типове поле бою, яке складається з різнорідних об'єктів, таких як солдати, бронетехніка та літаки, які обмінюються інформацією під час кіберфізичних атак противника [17].

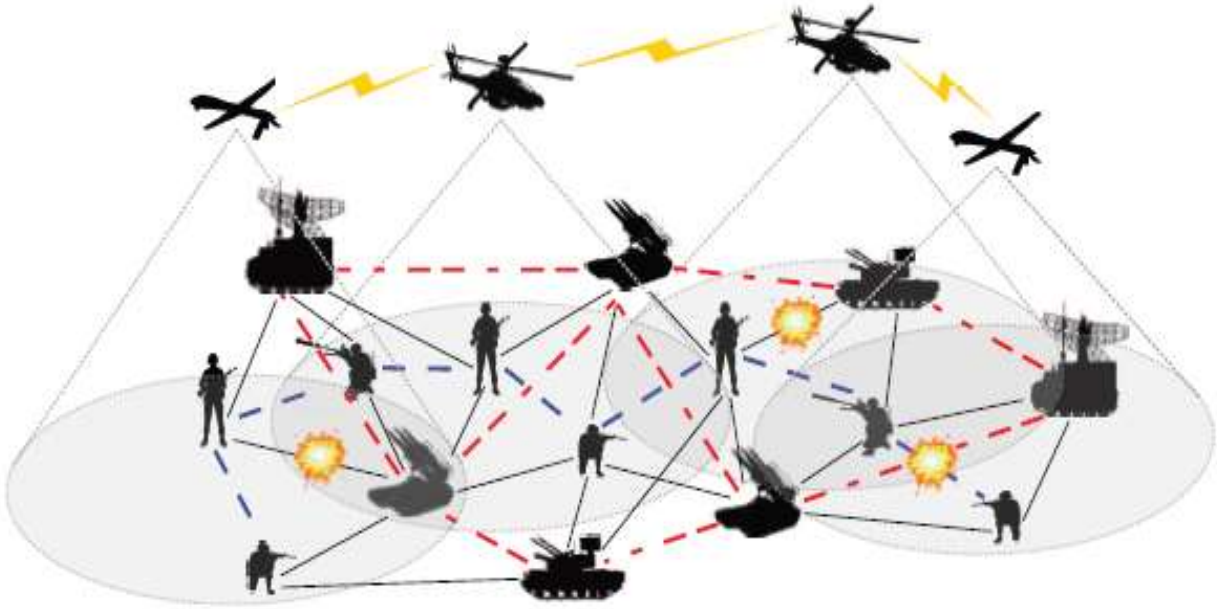

Рисунок 3 – Приклад гетерогенної мережі IoBT із випадковими атаками противника [17]

Речам IoBT на полі бою потрібно використовувати зв'язок між пристроями (D2D), щоб обмінюватися інформацією з іншими речами. Таким чином, на обмін інформацією можуть впливати такі фізичні параметри мережі, як потужність передавачів речей,

кількість розгорнутих речей, їх розташування та гнучкість зв'язку з іншими типами речей. На додаток до цих факторів, ще однією перешкодою для підключення речей на полі бою є чутливість до кіберфізичних атак. На обмін інформацією між об'єктами може впливати декілька факторів, таких як глушіння радіочастотних (РЧ) каналів, фізичні атаки на інфраструктуру, збої вузлів через атаки на джерела живлення або відсутність живлення тощо. Оскільки аналітика та автоматизовані рішення в мережі IoBT покладаються на дані в реальному часі, які надають датчики, розгорнуті на полі бою, то потрібно забезпечити поширення інформації в мережах із певним рівнем надійності та безпеки, щоб приймати правильні рішення.

Незважаючи на те, що IoBT поширюється за межі комунікацій на полі бою у такі системи, як цифрова аналітика та автоматичне реагування, що забезпечує більш швидке та точне реагування систем у порівнянні з людьми, але однак аспект зв'язності є життєво важливим, щоб дозволити системам IoBT повністю розкрити свій потенціал. Ідеальним є досягнення повної обізнаності про ситуацію та поширення інформації мережею. Притаманна IoBT обмеженість доступних ресурсів, супутні витрати (капітальні та операційні) і вразливість до атак вимагає побудови економічно ефективної, безпечної та реконфігурованої мережі в кожному конкретному випадку застосування.

7. Конвергенція IoT у системах управління біоресурсами та природокористування

Із зростанням впровадження Інтернету речей (IoT) підключені пристрої проникли в усі аспекти нашого життя, від здоров'я та фітнесу, домашньої автоматизації, автомобільної промисловості та логістики до розумних міст і промислового Інтернету речей [18]. Таким чином, цілком логічно, що IoT, підключені пристрої та автоматизація знайдуть своє застосування в сільському господарстві і значно покращать майже кожен його аспект.

Протягом останніх десятиліть сільське господарство зазнало низки технологічних трансформацій, стало більш індустріалізованим і технологічним. Використовуючи різноманітні розумні сільськогосподарські гаджети, фермери отримали кращий контроль над процесом вирощування худоби та вирощування сільськогосподарських культур, зробивши його більш передбачуваним та підвищивши ефективність.

Технології та Інтернет речей мають потенціал трансформувати сільське господарство в багатьох аспектах. Можна виділити 6 напрямів, у яких IoT може покращити сільське господарство:

1. Big Data. Величезні об'єми даних, зібраних розумними датчиками у сільському господарстві, наприклад, про погодні умови, якість ґрунту, процес росту культур або здоров'я худоби, можуть бути використані для відстеження стану фермерського бізнесу в цілому, а також продуктивності персоналу, ефективності обладнання тощо.

2. Контроль. Покращення контролю за внутрішніми процесами і, як наслідок, зниження виробничих ризиків. Здатність передбачити випуск вашого виробництва дозволяє планувати кращий розподіл продукції. Якщо точно спрогнозувати об'єми врожаю, то можна завчасно забезпечити реалізацію всієї товарної продукції.

3. Ризики. Зменшення ризиків втрати врожаю шляхом управління витратами та зменшення відходів на основі посиленого контролю над виробництвом. Завдяки можливості оперативно виявляти аномалії в рості сільськогосподарських культур або здоров'ї худоби, можна зменшити ризики втрати продукції.

4. Ефективність. Підвищення ефективності бізнесу завдяки автоматизації процесів. Використовуючи інтелектуальні пристрої, можна автоматизувати численні процеси виробничого циклу, наприклад, зрошення, внесення добрив або боротьбу із шкідниками.

5. Якість. Підвищення якості та обсягів продукції на основі кращого контролю над виробничим процесом і підтримка стандартів якості врожаю та здатності до росту шляхом автоматизації.

6. Екологія. Зменшення екологічного сліду на основі застосування автоматизованих технологій розумного землеробства, які можуть скоротити використання пестицидів і добрив, пропонуючи більш точне покриття, і, таким чином, зменшити викиди парникових газів.

Компаніями, що працюють у сфері розумного природокористування, пропонується цілий спектр різноманітних рішень [19]. Розглянемо деякі приклади.

1. Моніторинг кліматичних умов. Одними з найпопулярніших пристроїв для розумного сільського господарства є метеостанції, що поєднують у собі різноманітні розумні фермерські датчики. Розташовані у полях, вони збирають різні дані з навколишнього середовища та надсилають їх у хмару. Надані вимірювання можна використовувати для картографування кліматичних умов, вибору відповідних культур і вжиття необхідних заходів для покращення їх продуктивності (тобто точного землеробства).

2. Автоматизація парників. Як правило, фермери використовують ручне втручання для контролю тепличного середовища. Використання пристроїв IoT дозволяє отримувати точну інформацію в режимі реального часу про стан середовища у теплиці, такі як освітлення, температура, стан ґрунту, вологість та керувати ними. Крім отримання даних про навколишнє середовище, метеостанції можуть подавати сигнали для автоматичного регулювання умов відповідно до заданих параметрів.

3. Управління рослинництвом. Ще один вид продукту IoT у сільському господарстві та ще один елемент точного землеробства – це пристрої для керування врожаєм. Як і метеостанції, їх слід розміщувати в полі. Вони надають дані, що стосуються землеробства; від температури й опадів до водного потенціалу листя та загального здоров'я врожаю. Таким чином, можна стежити за ростом врожаю та будь-якими аномаліями, щоб ефективно запобігати будь-яким хворобам або інвазіям, які можуть зашкодити врожаю.

4. Моніторинг та догляд за худобою. Подібно до моніторингу врожаю, існують сільськогосподарські датчики IoT, які можна прикріпити до тварин на фермі, щоб стежити за їх здоров'ям і продуктивністю. Відстеження худоби та моніторинг допомагають збирати дані про здоров'я худоби, самопочуття та фізичне місцезнаходження. Наприклад, такі датчики можуть ідентифікувати хворих тварин, щоб фермери могли відокремити їх від стада та уникнути зараження. Використання дронів для відстеження худоби в реальному часі також допомагає фермерам скоротити витрати на персонал.

5. Точне землеробство. Полягає в ефективності та прийнятті точних рішень на основі об'єктивних даних. Це також одне з найпоширеніших і найефективніших застосувань IoT у сільському господарстві. Використовуючи датчики IoT, фермери можуть збирати широкий спектр показників щодо кожного аспекту мікроклімату та екосистеми поля: освітлення, температура, стан ґрунту, вологість, рівень CO2 та зараження шкідниками. Ці дані дозволяють фермерам оцінити оптимальну кількість води, добрив і пестицидів, які потрібні їхнім посівам, зменшити витрати та виростити кращі й здоровіші врожаї.

6. Сільськогосподарські дрони. Можливо, одним із найперспективніших досягнень агротехніки є використання сільськогосподарських дронів у розумному землеробстві. Також відомі як БПЛА (безпілотні літальні апарати) дрони краще оснащені для збору сільськогосподарських даних, ніж літаки та супутники. Крім можливостей спостереження, безпілотники також можуть виконувати величезну кількість завдань, які раніше вимагали людської праці: посадка культур, боротьба зі шкідниками та інфекціями, обприскування сільськогосподарських культур, моніторинг посівів тощо.

7. Прогнозна аналітика для розумного землеробства. Точне землеробство базується на прогнозній аналітиці даних. Завдяки тому, що технології IoT та інтелектуальних WSN надають високорелевантні дані у режимі реального часу, використання аналітики даних допомагає фермерам зрозуміти тенденції та зробити важливі прогнози: час збирання врожаю, ризики хвороб і інвазій, обсяг врожаю тощо. Інструменти аналізу даних допомагають

зробити сільське господарство, яке за своєю суттю є ризикованою діяльністю і сильно залежить від погодних умов, більш керованим і передбачуваним.

8. Наскрізні системи управління фермерським господарством. Більш комплексний підхід до продуктів IoT у сільському господарстві можна представити так званими системами управління продуктивністю ферм. Зазвичай вони включають низку сільськогосподарських пристроїв Інтернету речей і датчиків, встановлених на території, а також потужну інформаційну панель з аналітичними можливостями та вбудованими функціями обліку/звітності. Це надає можливості дистанційного моніторингу процесів фермерського господарства та дозволяє оптимізувати більшість бізнес-операцій.

9. Роботи та автономні машини. Робототехнічні інновації також пропонують багатообіцяюче майбутнє в області автономних машин для сільськогосподарських цілей. Деякі фермери вже використовують автоматизовані комбайни, трактори та інші машини і транспортні засоби, які можуть працювати без контролю людини. Такі роботи можуть виконувати повторювані, складні та трудомісткі завдання. Наприклад, до сучасних агророботів відносяться автоматизовані трактори, які можуть працювати за заданими маршрутами, надсилати сповіщення, починати роботу в запланований час тощо. Такі трактори без водіїв скорочують витрати на оплату праці фермерів.

Різноманітність застосування IoT у природокористуванні обумовлює різноманітність можливих архітектур та технічних рішень для кожного конкретного випадку.

8. Конвергенція IoT у системах кіберенергетики

Сьогодні енергетичний сектор сильно залежить від викопного палива, що становить майже 80 % кінцевої енергії в усьому світі. Надмірний видобуток і спалювання викопного палива має негативний вплив на навколишнє середовище, здоров’я та економіку через забруднення повітря та зміну клімату. Енергоефективність, тобто споживання менше енергії для надання тієї самої послуги і використання відновлюваних джерел енергії, є двома основними альтернативами для зменшення негативного впливу використання викопного палива [20].

Автоматизація промислових процесів і систем диспетчерського керування та збору даних стали популярними в енергетиці в 1990-х роках. Завдяки моніторингу, контролю обладнання та процесам ранні етапи IoT почали сприяти енергетичному сектору, зменшуючи ризик втрати виробництва або знеструмлення. Надійність, ефективність, вплив на навколишнє середовище та проблеми з обслуговуванням є основними проблемами старих електростанцій. Вік обладнання в енергетичному секторі та проблеми з поганим обслуговуванням можуть призвести до високого рівня втрат енергії та ненадійності. Активам іноді більше 40 років, вони дуже дорогі, але не можуть бути легко замінені. IoT може сприяти зменшенню деяких із цих проблем в управлінні електростанціями. Застосовуючи датчики Інтернету речей, пристрої, підключені до Інтернету, здатні розпізнавати будь-який збій у роботі або аномальне зниження енергоефективності, що сигналізує про необхідність обслуговування. Це підвищує надійність і ефективність системи на додаток до зниження вартості обслуговування. В табл. 2 і 3 наведено опис сфер застосування IoT в енергетичних системах.

Головною проблемою конвергенції IoT в енергетиці є інтеграція систем IoT у підсистеми енергетичної системи. Оскільки підсистеми енергетики є унікальними і в них використовуються різноманітні сенсорні та комунікаційні технології, то потрібні рішення для управління обміном даними між підсистемами енергетичної системи з підтримкою IoT. Підхід до пошуку рішень для інтеграційної проблеми, враховуючи вимоги IoT до підсистеми, відноситься до моделювання інтегрованої структури для енергетичної системи. Інші рішення пропонують розробку моделей спільного моделювання для енергетичних систем для інтеграції системи та мінімізації помилки затримки синхронізації між підсистемами.

Таблиця 2 – Застосування IoT в енергетичному секторі. Регулювання, ринок та енергопостачання [21]

	Застосунок	Сектор	Опис	Переваги
Регулювання і ринок	Демократизація енергетики	Регулювання	Надання доступу до мережі для багатьох дрібних кінцевих користувачів для однорангової торгівлі електроенергією та вільного вибору постачальника	Пом'якшення ієрархії в ланцюгу енергопостачання, ринкової влади та централізованого постачання; ліквідація енергетичного ринку та зниження цін для споживачів; підвищення обізнаності щодо використання та ефективності енергії
	Агрегація дрібних просьюмерів (віртуальні електростанції)	Енергетичний ринок	Агрегування навантаження та генерування групи кінцевих споживачів для пропозиції на ринках електроенергії, балансування чи резерву	Мобілізація невеликих вантажів для участі в конкурентних ринках; допомога мережі шляхом зменшення навантаження в години пік; відмежування ризику високих рахунків за електроенергію в години пік; підвищення гнучкості мережі та зменшення потреби в балансуючих активах, пропонуючи прибутковість споживачам
Постачання енергії	Профілактичне обслуговування	Видобуток нафтогазової промисловості/ комунальні підприємства	Моніторинг несправностей, витоків і втоми шляхом аналізу великих даних, зібраних за допомогою статичних і мобільних датчиків або камер	Зменшення ризику збою, втрати виробництва та простою технічного обслуговування; зниження вартості O&M; запобігання нещасних випадків і підвищення безпеки
	Обслуговування несправностей	Видобуток нафтогазової промисловості/комунальні підприємства	Виявлення збоїв і проблем в енергетичних мережах і, можливо, їх віртуальне усунення	Підвищення надійності послуги; підвищення швидкості усунення витоків у системі централізованого теплопостачання або збоїв в електромережах, а також скорочення часу на технічне обслуговування та зниження ризику для здоров'я/безпеки
	Зберігання енергії і аналітика	Промислові постачальники або комунальні компанії	Аналіз ринкових даних і можливостей для активації опцій гнучкості, таких як зберігання енергії в системі	Зниження ризику дисбалансу попиту та пропозиції; підвищення рентабельності торгівлі енергоносіями за рахунок оптимального використання гнучких опцій та опцій зберігання; забезпечення оптимальної стратегії зберігання активів

Продовж. табл. 2

	Цифрове виробництво електроенергії	Комунальні підприємства та системний оператор	Аналіз великих даних та керування багатьма генеруючими установками в різних часових масштабах	Підвищення безпеки постачання; покращення використання та управління активами; зниження витрат на забезпечення резервної потужності; прискорення реакції на втрату навантаження; зниження ризику знеструмлення

Таблиця 3 – Застосування IoT в енергетичному секторі. Енергетичні мережі та споживачі [21]

	Застосунок	Сектор	Опис	Переваги
Мережа передачі та розподілу	Розумні мережі	Управління електромережами	Платформа для керування мережею з використанням великих даних та ІКТ-технологій на відміну від традиційних мереж	Підвищення енергоефективності та інтеграція розподіленої генерації і навантаження; підвищення безпеки постачання; а також зменшення потреби в резервних ресурсах і витратах
	Управління мережею	Експлуатація та управління електричною мережею	Використання великих даних у різних точках сітки для більш оптимального керування сіткою	Виявлення слабких місць і відповідне посилення мережі та зменшення ризику знеструмлення
	Інтегрований контроль парку електромобілів	Експлуатація та управління електричною мережею	Аналіз даних зарядних станцій і циклів заряду/розряду електромобілів	Покращення реакції на попит на зарядку в години пік; аналіз та прогнозування впливу електромобілів на навантаження; визначення зон для встановлення нових зарядних станцій та посилення розподільчої мережі
	Контроль і управління транспортним засобом до мережі (V2G)	Експлуатація та управління електричною мережею	Аналіз навантаження та схеми заряду/розряду електромобілів для підтримки мережі, коли це необхідно	Підвищення гнучкості системи шляхом активації електромобілів у постачанні електроенергії в мережу, зменшення потреби в резервному копіюванні, пропускна здатність у години пік. Контроль і управління парком електромобілів для забезпечення оптимальної взаємодії між мережею та електромобілем
	Мікромережі	Електромережі	Платформи для управління мережею, незалежною від центральної мережі	Підвищення безпеки постачання; створення взаємодії та гнучкості між мікрогрідами та основною мережею; пропонування стабільних цін на електроенергію для споживачів, підключених до

Продовж. табл. 3

				мікромережі
	Контроль та управління теплопостачанням	Мережа теплопостачання	Аналіз великих даних температури та навантаження в мережі і підключених споживачів	Підвищення ефективності мережі для задоволення попиту; зниження температури гарячого водопостачання та економія електроенергії, коли це можливо; визначення точок сітки з потребою у посиленні
Сторона споживання	Реагування на попит	Житловий/комерційний та промисловий	Центральне керування шляхом опускання, зміщення або вирівнювання	Зниження попиту в час пік, що саме по собі зменшує перевантаження мережі
	Реагування на попит (управління попитом)	Житловий/комерційний і промисловий	Централізований контроль (тобто шляхом проливання, зміщення або вирівнювання; навантаження багатьох споживачів шляхом аналізу навантаження та роботи приладів	Зниження попиту в час пік, що саме по собі зменшує перевантаження мережі; зменшення рахунків споживачів за електроенергію; а також зменшення потреби в інвестиціях у резервну потужність мережі
	Розширена інфраструктура вимірювання	Кінцеві споживачі	Використання датчиків і пристроїв для збору та аналізу даних про навантаження і температуру на місці споживача	Наявність доступу до детальних змін навантаження в різних часових масштабах; визначення областей для покращення енергоефективності (наприклад, кімнати з надмірним кондиціонуванням або додаткове освітлення, коли немає мешканців); зниження вартості використання енергії
	Управління енергією батареї	Кінцеві споживачі	Аналітика даних для активації батареї в найбільш підходящий час	Оптимальна стратегія заряду/розряду акумулятора в різних часових масштабах; підвищення енергоефективності та допомога мережі в години пік; зниження вартості використання енергії
	Розумні будівлі	Кінцеві споживачі	Централізоване та дистанційне керування приладами	Підвищення комфорту завдяки оптимальному контролю приладів і систем ОВК; зменшення ручного втручання, економія часу та енергії; підвищення рівня знань про використання енергії та вплив на навколишнє середовище; підвищення готовності до приєднання до розумної мережі або віртуаль-

Продовж. табл. 3

				ної електростанції; покращення інтеграції розподілених систем генерації та зберігання

8. Висновки

Конвергенція IoT у ситуаційних системах різного типу вимагає розв'язання типових для IoT задач, пов'язаних з організацією гетерогенного мережевого середовища з контрольованим енергоспоживанням і необхідністю обробки великих об'ємів даних. Отже, для вироблення базових вимог до побудови конкретної кіберконвергентної IoT системи застосовні загальні оптимізаційні підходи зі зваженими пріоритетами.

З іншого боку, особливості використання ситуаційних систем різного призначення накладає специфічні вимоги і обмеження при визначенні архітектури і технічних рішень для таких систем. Наприклад, для кібермедичних систем однією із ключових вимог є безпека пацієнта і персоналу. Отже, всі рішення повинні забезпечувати цю вимогу. В військових ситуаційних системах на основі IoT ключовою вимогою є швидка адаптивність в умовах витрат ресурсів і зміни топології. В кожному конкретному випадку система вимог орієнтована на підтримку критичної вимоги. Множинність та різноманіття варіантів можливих рішень при розробці таких систем обумовлює необхідність застосування інтелектуальних технологій розробки систем із застосуванням штучного інтелекту і моделей знань цільової предметної сфери.

СПИСОК ДЖЕРЕЛ

1. Kovalenko O. Information Taxonomy and Ontology for Situational Management. *IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies. CSIT 2018 Proc*. 2018. Vol. 2, N 8526723. P. 94–97. DOI: 10.1109/STC-CSIT.2018.8526723.
2. Jakobson G., Buford J., Lewis L. Situation Management: Basic Concepts and Approaches / eds. V.V. Popovich, M. Schrenk, K.V. Korolenko. *Information Fusion and Geographic Information Systems*. LNG&C. Heidelberg: Springer, 2007. Vol. XIV. P. 18–33.
3. Kovalenko O. Systems Convergence for Situational Control and Decision Making in Distributed Environments. *IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022. P. 344–347. DOI: 10.1109/TCSET55632.2022.9767006.
4. Kovalenko O. Knowledge Driven Cyber-Convergent Systems Based on Situational Agents. *IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT)*. 2022. P. 243–246. DOI: 10.1109/CSIT56902.2022.10000762.
5. Коваленко О.Є. Онтологія та модель трансформації інформації в ситуаційних агентних системах. *Електронне моделювання*. 2020. Т. 42, № 5. С. 3–23. DOI: https://doi.org/10.15407/emodel.42.05.005.
6. Ma J., Ning H., Huang R., Liu H., Yang L.T., Chen J., Min G. Cybermatics: A holistic field for systematic study of cyber-enabled new worlds. *IEEE Access*. 2015. Vol. 3. P. 2270–2280.
7. Zhou X., Zomaya A.Y., Li W., Ruchkin I. Cybermatics: Advanced Strategy and Technology for Cyber-Enabled Systems and Applications. *Future Generation Computer Systems*. 2018. Vol. 79. P. 350–353.
8. Коваленко О.Є. Принципи інженерії ситуаційних систем. *Математичні машини і системи*. 2019. № 4. С. 65–78. DOI: 10.34121/1028-9763-2019-4-65-78.
9. Situational Analysis. URL: https://www.iaea.org/resources/nuclear-communicators-toolbox/methods/planning/situational-analysis.
10. Wireless Sensor Network Architecture and Its Applications. URL: https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/.
11. Sadoughi F., Behmanesh A., Sayfouri N. Internet of things in medicine: a systematic mapping study. *J. Biomed. Inform.* 2020. Vol. 103. P. 103383. URL: https://doi.org/10.1016/j.jbi.2020.103383.

12. Paranjape K., Schinkel M., Nanayakkara P. Short keynote paper:mainstreaming personalized healthcare-transforming healthcare through new era of artificial intelligence. *IEEE J. Biomed. Health Inform*. 2020. N 1. URL: https://doi.org/10.1109/JBHI.2020.2970807.
13. Ergen O., Belcastro K.D. AI Driven Advanced Internet Of Things (Iotx2): The Future Seems Irreversibly Connected in Medicine. *Anatol. J. Cardiol*. 2019. N 22. P. 15–17. URL: https://doi.org/10.14744/AnatolJCardiol.2019.73466.
14. Kumar B., Al Ismaili M. Incorporating Internet of Things Applications in Healthcare. *Current Overview on Science and Technology Research*. 2022. Vol. 1. P. 37–49. URL: https://doi.org/10.9734/bpi/costr/v1/3485A.
15. Kovalenko O., Velev D. Big data aggregation in disasters risk management systems. *2020 6th International Conference on Advances in Environment Research. IOP Conf. Series: Earth and Environmental Science*. 2021. Vol. 776. P. 012007. IOP Publishing. DOI: 10.1088/1755-1315/776/1/012007.
16. Ray P.P., Mukherjee M., Shu L. Internet of Things for Disaster Management: State-of-the-Art and Prospects. *IEEE Access*. 2017. Vol. 5. P. 18818–18835. DOI: 10.1109/ACCESS.2017.2752174.
17. Farooq M.J., Zhu Q. On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT). *IEEE Transactions on Wireless Communications*. 2018. Vol. 17, N 4. P. 2618–2632. DOI: 10.1109/TWC.2018.2799860.
18. Tao W., Zhao L., Wang G., Liang R. Review of the internet of things communication technologies in smart agriculture and challenges. *Computers and Electronics in Agriculture*. 2021. N 189. P. 106352.
19. IOT in Agriculture: 9 Technology Use Cases for Smart Farming (and Challenges to Consider). URL: https://easternpeak.com/blog/iot-in-agriculture-technology-use-cases-for-smart-farming-and-challenges-to-consider/.
20. Connolly D., Lund H., Mathiesen B. Smart Energy Europe: The technical and economic impact of one potential 100% renewable energy scenario for the European Union. *Renew. Sustain. Energy Rev*. 2016. Vol. 60. P. 1634–1653.
21. Hossein Motlagh N, Mohammadrezaei M, Hunt J, Zakeri B. Internet of Things (IoT) and the Energy Sector. *Energies.* 2020. Vol. 13 (2). P. 494. URL: https://doi.org/10.3390/en13020494.

Стаття надійшла до редакції 13.08.2023