

## СЕКЦІЯ 4 ЕКОНОМІКА ТА УПРАВЛІННЯ ПІДПРИЄМСТВАМИ

УДК 338.984

Аталавей В.Т.  
аспірант кафедри економіки  
Сумського національного аграрного університету

### ВИКЛИКИ ІНТЕГРАЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ОПЕРАТИВНОГО УПРАВЛІННЯ ЯК РЕЗУЛЬТАТ ПОШИРЕННЯ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ В КОМПАНІЯХ НАФТОГАЗОВОЇ ІНДУСТРІЇ

#### АНОТАЦІЯ

У статті досліджено вплив все ширшого використання промислового Інтернету речей на управління компаніями нафтогазового сектору. Запропоновано модель інтеграції інформаційних технологій та оперативного управління компаніями. Наведено виклики, що стоять перед відділами інформаційних технологій та оперативного управління у зв'язку з використанням промислового Інтернету речей.

**Ключові слова:** Інтернет речей, промисловий Інтернет речей, інформаційні технології, система управління виробництвом, планування ресурсів підприємства.

#### АННОТАЦІЯ

В статье исследовано влияние все более широкого использования промышленного Интернета вещей на управление компаниями нефтегазового сектора. Предложена модель интеграции информационных технологий и оперативного управления компаниями. Приведены вызовы, стоящие перед отделами информационных технологий и оперативного управления в связи с использованием промышленного Интернета вещей.

**Ключевые слова:** Интернет вещей, промышленный Интернет вещей, информационные технологии, система управления производством, планирование ресурсов предприятия.

#### ANNOTATION

The article examines the impact of the increasing use of the Industrial Internet of things by the management of the oil and gas companies. The model of integration of information technologies and operational management of companies is offered. The challenges faced by IT departments and operational management in connection with the use of the Industrial Internet of things are presented.

**Key words:** Internet of things, industrial Internet of things, information technologies, MES, ERP.

**Постановка проблеми.** Після багатьох років високих та зростаючих цін на нафту у більш ніж 100 доларів США за барель нові технології видобутку відкрили нові джерела постачання товару на ринок, що потягнуло зниження ціни на 20–30, а потім і на 50 доларів США за барель. Така нова норма знижених цін на нафту не тільки викриває неефективність багатьох компаній нафтогазової індустрії, але й штовхає найбільш ефективні з них до подвоєння зусиль, щоб залишатись на плаву. Багато компаній вибрали для цього один з найпопулярніших напрямів, що обіцяє компаніям гарні перспективи, а саме Інтернет речей (*The Internet of Things*, далі – IoT), або індустріальний його різновид промисловий Інтернет речей (*The Industrial Internet of*

*Things*, далі – IIoT). Інтернет речей – це глобальна мережа підключених до Інтернету фізичних пристроїв, тобто «речей», оснащених сенсорами, датчиками та пристроями передачі інформації. Ці пристрої об'єднані за допомогою підключення до центрів контролю, управління й оброблення інформації. Індустріальний інтернет речей (IIoT) – термін, що стосується різних наборів апаратних складових та елементів, які працюють разом через Інтернет, щоби покращити виробничі процеси.

В нафтогазовій промисловості перспективи застосування IIoT полягають не в управлінні наявними активами, ланцюжками поставок або взаємозв'язків з клієнтами, а у створенні нової вартості в інформації про них. Інтегрована стратегія є ключовою для компаній, які прагнуть знайти нову цінність в IIoT. Одним з таких аспектів у менеджменті компаній нафтогазової індустрії, що потребує детального аналізу, є зближення та переплетення функцій сектору IT та операційного управління компаніями, як наслідок, ширшого використання IIoT. Все це зумовлює актуальність вибраної теми дослідження.

**Аналіз останніх досліджень і публікацій.** Публікації та дослідження, присвячені темі інтеграції інформаційних та операційних технологій, можна умовно поділити на кілька категорій. Перша категорія включає публікації щодо поширення й способів застосування IIoT та його різновидів, таких як IIoT та IIoTSP [2; 5; 11; 13; 14]. Основний лейтмотив цих праць передає така цитата: «Інтернет речей передбачає майбутнє, в якому цифрові і фізичні особи можуть бути пов'язані за допомогою відповідних інформаційних та комунікаційних технологій для створення цілого нового класу програм і послуг» [14, с. 1497]. Друга категорія робіт є більш наближеною до об'єкта нашого дослідження та пов'язана з управлінськими інформаційними системами в компаніях [3; 4; 6–9; 12; 17]. В цих працях розглядається еволюція управлінських інформаційних систем від *Manufacturing execution system* (MES)

[9] до ERP [8]. Третя категорія робіт поєднує перші дві з компаніями нафтогазового сектору [1; 10; 16] та вказує на специфіку, що виникає при цьому.

**Виділення невирішених раніше частин загальної проблеми.** Навіть побіжний погляд на оглянуті джерела дає змогу встановити деякі закономірності, які полягають в тому, що, по-перше, в аналізі переважає технічний аспект проблеми, а по-друге, питання впливу цих технічних змін на менеджмент компаній майже не розкриті, що й є не вирішеним сьогодні аспектом проблеми, який потребує додаткових досліджень.

**Формулювання цілей статті (постановка завдання).** Мета статті полягає в дослідженні впливу використання ПоТ на управління компаніями, насамперед вивченні того, як відбувається зближення технічної та управлінської функцій. Також одним із завдань статті є окреслення напрямів того, як мають змінюватись як управлінська, так і інформаційна служби у відповідь на ці виклики.

**Виклад основного матеріалу дослідження.** Промисловий Інтернет речей (ПоТ) – це майбутнє нафтогазової галузі, оскільки мережа пристроїв, сенсорів та програмного забезпечення Internet of Things (IoT) приводить до змін у повсякденному житті споживачів, а сьогодні у цьому галузь відстає. Правильно сказати, що Інтернет речей об'єднує реальні речі у віртуальні системи, здатні вирішувати абсолютно різні завдання. Ключова ідея концепції полягає в тому, щоби з'єднати між собою всі об'єкти, які можна з'єднати, підключити до мережі, за рахунок чого отримати синергію, щось на зразок « $2+2=5$ ».

Інтеграція підключених пристроїв до нафти й газу торкнеться практично кожного етапу ланцюга постачання нафти й газу від пошуку запасів до операцій видобутку аж до взаємодії із замовниками. Все це є полем для швидких змін індустрії та можливістю для індустрії нафти й газу конкурувати в сучасному світі.

З'єднання речей, послуг та людей через Інтернет покращує аналіз даних, підвищує продуктивність та надійність, заощаджує енергію та витрати, генерує нові можливості отримання доходів за допомогою інноваційних бізнес-моделей. Те, що починалось як інтранет речей (підключення пристроїв один до одного), перетворилось на Інтернет речей (підключення пристроїв один до одного через Інтернет), зрештою, на Інтернет речей (речі або пристрої, обладнані датчиками, обчислювальною потужністю та програмним забезпеченням). Хоча ці речі протягом багатьох років спілкувались одна з одною, ПоТ розширює зв'язок з інтрамережі в Інтернеті через такі технології, як мобільний зв'язок та хмара. Якщо хтось думає про послуги, аналітичні дані можуть стати цінними підказками для попереджувальної діагностики та обслуговування, а переваги цих послуг можуть

бути суттєвими для клієнтів [1]. Інтернет речей дає змогу побудувати нову модель для виявлення вдосконалених дій. Люди завжди будуть ключовою частиною картини.

Сектор нафтогазової індустрії стикається з викликами, що багато в чому пояснюється застарілим та неефективним підходом, який використовують багато компаній для підтримки активів та збору й обробки даних. Чому компанії нафтогазової галузі мають використовувати ПоТ? На основі аналізу літературних джерел та свіжої бізнес-аналітики наводимо п'ять причин, чому за допомогою ПоТ можна революціонізувати нафтогазову галузь.

1) Поліпшення операційної ефективності. Згідно з даними аналітиків у наступні кілька років нафтогазова промисловість зіткнеться зі збитками, коли працівники *Baby Boomer* будуть масово виходити на пенсію, залишиться мало людей, які мають відповідний досвід у галузі, щоб зайняти вакантні посади. Використання Big Data та віддалена видимість допоможуть компаніям краще керувати своїми активами та використовувати здобуті дані для оптимізації виробництва. Використання можливостей IIoT може скоротити час усунення несправностей від днів до хвилин, що залишає більше часу на інші операційні аспекти бізнесу.

2) Дохід. Ця галузь значно впливає на світовий ВВП, адже, згідно з оцінками експертів, загальне прийняття ПоТ може збільшити світовий ВВП на 0,8%, або 816 млрд. дол., у наступному десятилітті. Оскільки нижчі ціни на нафту є новою нормою, маржа прибутку знизилась, нафтові та газові компанії повинні скористатися цією можливістю, щоб інвестувати в інноваційні технології, а не проводити скорочення витрат абияк. Фінансові прибутки від скорочення витрат та заощаджуваного часу будуть безцінними, оскільки галузь стане ще більш конкурентоспроможною.

3) Дані реального часу. Великі дані не є новими для нафтової та газової промисловості, адже дані мають вирішальне значення для успіху цієї галузі. Ефективність і точність високо цінуються в нафтогазовій промисловості, навіть більше, ніж в будь-якій іншій галузі. Невеликі підвищення ефективності можуть мати значний економічний ефект. Прибуток у нафтогазовій промисловості залежить від швидких та точних даних про виробництво. Завдяки інтеграції з ПоТ видобуток нафти можна зафіксувати в режимі реального часу за допомогою вбудованих датчиків та правильної автоматизації систем передачі даних, що дасть змогу компаніям збирати інформацію з активів будь-де та приймати обґрунтовані рішення. Наприклад, компанії можуть адаптувати свої стратегії буріння після порівняння даних про буріння в реальному часі з даними з виробництва сусідніх свердловин. Згідно з даними "Bain&Company" такий рівень видимості може допомогти нафтогазовим компаніям збільшити виробництво на 6–8%.

4) Зменшений ризик безпеки. Безпека є, мабуть, найбільшою галузевою проблемою як всередині, так і зовні. ПоТ може знизити ризик, визначений потенційними проблемами, перш ніж вони стануть актуальними проблемами або серйозними викликами для безпеки. Дистанційне усунення несправностей означає більш постійне та ефективне регулювання нафтових установок. Повністю інтегрована ПоТ система також повністю зменшує кількість поїздок та потенційно небезпечну роботу для персоналу.

5) Екологічний вплив. З підвищення ефективності до зменшення ризику безпеки та зменшення подорожей прийняття ПоТ може суттєво знизити вплив на навколишнє середовище в нафтогазовій галузі. Використання меншого обсягу енергії, запобігання витокам нафти та іншим аваріям, виділення менше вуглекислого газу є досить значними факторами для сектору нафти й газу, щоб звернути увагу на ПоТ. ПоТ також дає змогу більш чітко контролювати використання енергії та ресурсів.

Навіть сьогодні сучасні промислові пристрої все ще стикаються з проблемами, які полягають в технологічних, електричних, механічних та контрольних частинах, що варіюються від відносно простого обладнання до складних машин. Загальна складність – це результат зростання безмежної різноманітності функцій, які виконує кожне обладнання. Крім того, взаємодія між системами та пристроями викликає більшу плутанину, ніж раніше.

Однак такий невпинний рух у напрямі все більшого застосування ПоТ викликає одну менш позитивну проблему подальшої глибшої взаємодії ІТ-питань з питаннями операційного управління компаніями (*Operational technology*, далі – ОТ).

Конвергенція ІТ/ОТ – це інтеграція систем інформаційних технологій (ІТ), що використовуються для обчислення даних з орієнтацією на операційні технології (ОТ), які використовуються для моніторингу подій, процесів та пристроїв, а також коректування підприємств та виробничих операцій. ОТ означає операційні технології, а саме технології, що використовуються для керування операційною стороною бізнесу, традиційно за незначної участі в цьому ІТ. Тепер ця конвергенція ОТ та ІТ не є новиною, проте останніми роками помітно, що промисловий Інтернет почав вибухати в більш загальні можливості підключення до Інтернету, на відміну від закритих систем, які більше покладались на фізичну безпеку для забезпечення цілісності. З цим переходом від закритих до відкритих систем виникають ще більша взаємозалежність і перекриття між двома аспектами та численними новими питаннями безпеки.

Нині існує багато різних поглядів на інтеграцію операційної інфраструктури (наприклад, системи управління) з ІТ-інфраструктурою (ERP, Business Intelligence тощо) для досяг-

нення цифрової трансформації. Ми вважаємо, що немає необхідності об'єднувати ІТ-відділ з комерційним відділом, відповідальним за операційну активність (ОТ-інфраструктура). Ідея повинна полягати в тому, що відділ ІТ зосереджений у своїй сфері експертизи та виконує частину ІТ-інфраструктури цифрових проектів та IoTSP-проектів, тоді як операційний відділ зберігає свою відповідальність та виконує свою частину діяльності. На рівні 3.5 ці два світи зустрічаються (рис. 1). Архітектура підприємства – це місце, де ІТ-інфраструктура підключається до операційної інфраструктури системи керування, системи безпеки, датчиків та аналізу програмного забезпечення для моніторингу стану тощо. Це також стає природною межею відповідальності між двома відділами та їх постачальниками. Дуже важливо, щоби два департаменти співпрацювали. Цілісне уявлення про такий підхід можна побачити в описі детального рівня, представленого як піраміда на рис. 1.

Більше з'єднання та інтеграція, вочевидь, є корисними для інтелектуальної аналітики та управління, але більша кількість з'єднань та мережевих пристроїв означає більше можливостей для втручання в безпеку. Незважаючи на те, що безпека завжди була пріоритетом як для ІТ, так і для ОТ в традиційних системах, ці мережеві системи є новими сценаріями та профілями ризику для обох сторін. ІТ тепер потрібно починати думати, як ОТ, і навпаки (табл. 1).

Розглянемо нові виклики для ІТ.

*Більший масштаб впливу.* Не зменшуючи очевидних згубних наслідків порушення безпеки в більш традиційному підприємстві, маємо підкреслити, що масштаби наслідків інциденту в промисловій системі значно більші. Наприклад, якими будуть наслідки, якщо мережа електроенергії виходить з ладу або якщо система керування автомобілем була зламана та більше не перебуває в повному контролі?

*Фізичні ризики та безпека.* На відміну від більш традиційних корпоративних систем, мережеві промислові системи приводять до виникнення елемента фізичного ризику, про який ІТ-команда не доводилось думати. Переривання роботи або несправність апарата може привести до завдання пошкоджень працівникам або виробництва неякісних товарів, що може завдати шкоди кінцевим споживачам.

*Застарілі або нестандартні системи.* ІТ використовується для частого та послідовного оновлення програмного забезпечення, проте промислові середовища, як правило, більш системні, де одна невелика зміна може викликати ефект доміно. Як наслідок, у багатьох застарілих системах управління заводом можуть бути запущені застарілі операційні системи, які неможливо легко замінити, або застосовуватись налаштована конфігурація, яка не сумісна зі стандартними пакетами безпеки ІТ.

Розглянемо нові виклики для ОТ.

**Фізичні ризики та безпека.** Загроза фізичній безпеці не є новим побоюванням для ОТ-команд, адже вони впроваджують заходи безпеки в промислові системи десятиліттями. Однак зараз вони стикаються із загрозами, які потенційно виходять за межі їх контролю. Захоплення машин та систем керування із замкнутої системи приводить до загрози зламаних машин, які потенційно можуть завдати шкоди працівникам (наприклад, внаслідок перегріву, аварійного відключення).

**Продуктивність та контроль якості.** Втрата контролю над виробничим процесом або будь-яким пов'язаним пристроєм – це найгірший кошмар для команди ОТ. Розглянемо сценарій, коли шкідлива сторона може вимкнути установку, припинити виробництво цілком або перепрограмувати процес збирання, щоби пропустити кілька кроків, в результаті чого несправний продукт може завдати шкоди кінцевим користувачам.

**Витік даних.** Хоча витік даних вже давно є основною турботою традиційних ІТ-команд, вони є дещо новою територією для ОТ-команд, які звикли до роботи із закритими системами. З огляду на характер типів промислових систем, що виходять онлайн, таких як комунальні послуги, авіація та автомобільне виробництво, забезпечення конфіденційності переданих даних є критичним.

**Робота з інформаційними технологіями.** Однією з найбільш несподіваних проблем, які відчуваються в ОТ-департаментах, є те, як працювати з інформаційними технологіями для вирішення вищезгаданих проблем, коли ІТ-команди, як правило, мають мало досвіду роботи в промислових системах, а їх традиційні рішення безпеки, як правило, несумісні із застарілими системами управління. Багато хто в ОТ-департаментах бачить переваги відходу від замкнених систем та збільшення з'єднання, однак брак досвіду з боку ІТ та відсутність потенційних рішень для їх проблем безпеки викликають певне відторгнення.

Незважаючи на те, що ОТ та ІТ можуть мати різні підґрунтя, що визначають їхні занепокоєння щодо трансформації, спричиненої промисловим Інтернетом речей, основним для обох сторін є збереження контролю над системами та машинами, зрештою, безпека їх працівників та клієнтів. Для того щоб обидві сторони були щасливими, ключовими компонентами будь-яких потенційних рішень з безпеки мають бути:

- визначення та автентифікація всіх пристроїв і машин всередині системи як на виробничих підприємствах, так і на місцях для забезпечення взаємодії лише перевірених пристроїв та систем; це пом'якшить ризик того, що хакер

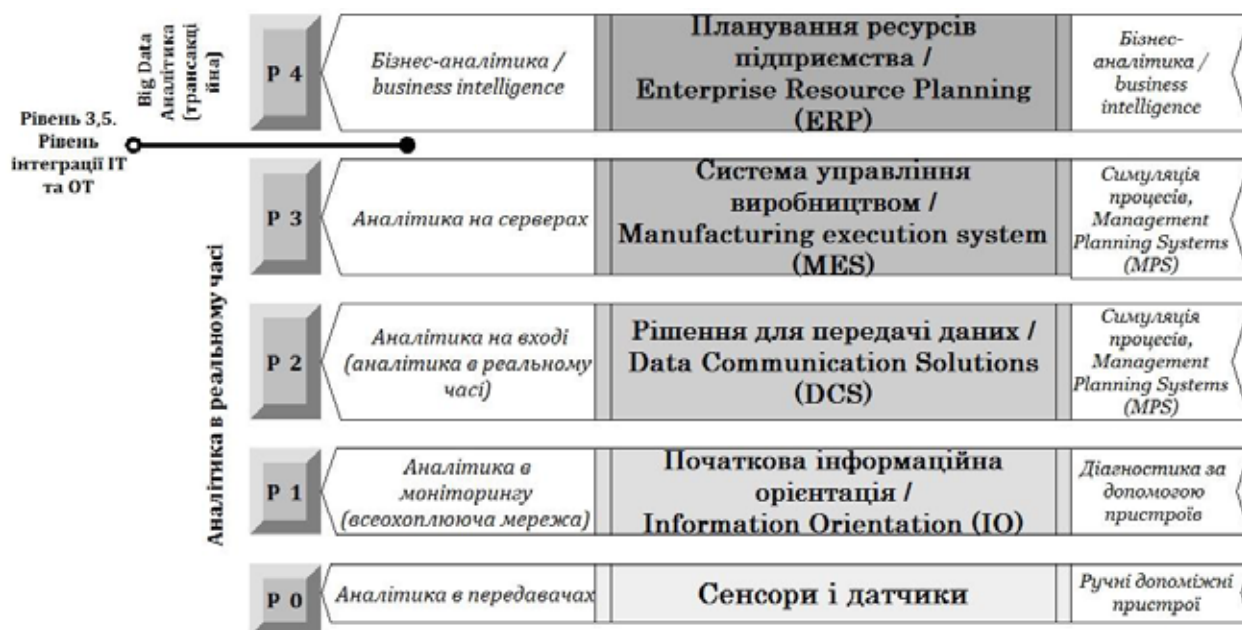


Рис. 1. Рівні інтеграції ІТ та ОТ

Таблиця 1

Нові виклики для ІТ та ОТ, пов'язані з ширшим використанням ІоТ

Нові виклики для ІТ	Нові виклики для ОТ
Більший масштаб впливу	Фізичні ризики та безпека
Фізичні ризики та безпека	Продуктивність та контроль якості
Застарілі або нестандартні системи	Витік даних
	Робота з інформаційними технологіями

увійде в систему через неналежний пристрій та контролюватиме будь-які системи та машини;

– шифрування всіх повідомлень між цими пристроями для забезпечення конфіденційності переданих даних;

– забезпечення цілісності даних, створених з цих систем; як вже згадувалось раніше, інтелектуальна аналітика є основним фактором прийняття промислового Інтернету, однак ця аналітика є марною, якщо дані неточні;

– забезпечення цілісності оновлень, якщо вироблені товари містять програмне забезпечення або прошивку, що дає змогу виконувати з ними віддалені оновлення в дорозі.

При цьому слід розуміти, що індустріальні системи управління стикаються з підвищеним ризиком загроз кібербезпеки. Мета кібербезпеки полягає в тому, щоб захистити активи, які вона вважає критичним. Тут вдаються до глибинної оборони, яка заснована на поєднанні людей, технологій, операцій та змагальній свідомості.

**Висновки.** З'єднання речей, послуг та людей через Інтернет покращує аналіз даних, підвищує продуктивність та надійність, заощаджує енергію та витрати, генерує нові можливості отримання доходів за допомогою інноваційних бізнес-моделей. Те, що починалось як інтранет речей (підключення пристроїв один до одного), перетворилось на Інтернет речей (підключення пристроїв один до одного через Інтернет), зрештою, на Інтернет речей (речі або пристрої, обладнані датчиками, обчислювальною потужністю та програмним забезпеченням). Хоча ці речі протягом багатьох років спілкувались одна з одною, IoT розширює зв'язок з інтрамережі в Інтернеті через такі технології, як мобільний зв'язок та хмара.

В роботі запропоновано спосіб інтеграції операційної інфраструктури з IT-інфраструктурою для досягнення цифрової трансформації. Ідея полягає в тому, що відділ IT зосереджений у своїй сфері експертизи та виконує частину IT-інфраструктури цифрових проектів та IoTSP-проектів, тоді як операційний відділ зберігає свою відповідальність та виконує свою частину діяльності.

Однак такий стрімкий розвиток застосування IoT у компаніях викликає зміни на рівні менеджменту, які становлять певний виклик для менеджменту компаній. Більше з'єднання та інтеграція, вочевидь, є корисними для аналітики та управління, але більша кількість з'єднань та мережевих пристроїв означає більше можливостей для втручання в безпеку. Незважаючи на те, що безпека завжди була пріоритетом як для IT, так і для OT у традиційних системах, ці мережеві системи є новими сценаріями та профілями ризику для обох сторін. IT тепер потрібно починати думати, як OT, і навпаки. Нами виділено нові виклики для IT, такі як більший масштаб впливу; фізичні ризики та безпека; застарілі або нестандартні системи, та нові ви-

клики для OT, такі як фізичні ризики та безпека; продуктивність та контроль якості; витік даних; робота з інформаційними технологіями.

Незважаючи на те, що OT та IT можуть мати різні підґрунтя, що визначають їхні занепокоєння щодо трансформації, спричиненої промисловим Інтернетом речей, основним для обох сторін є збереження контролю над системами та машинами, зрештою, безпека їх працівників та клієнтів. Вважаємо, що викладений у роботі підхід до інтеграції цих підсистем підприємств нафтогазової індустрії сприятиме подальшому вдосконаленню менеджменту у них.

#### БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Aalsalem M.Y., Khan W.Z., Gharibi W., Armi, N. An intelligent oil and gas well monitoring system based on Internet of Things. International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET). 2017. DOI: 10.1109/icramet.2017.8253159.
2. Aazam M., Khan I., Alsaffar A.A., Huh E.-N. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. Proceedings of 2014 11th International Bhurban Conference on Applied Sciences and Technology, IBCAST. 2014, art. no. 06778179. P. 414–419. DOI: 10.1109/IBCAST.2014.6778179.
3. Babiceanu R.F., Seker R. Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in Industry. 2016. № 81. P. 128–137. DOI: 10.1016/j.compind.2016.02.004.
4. Bi Z., Cochran D. Big data analytics with applications. Journal of Management Analytics. 2014. № 1 (4). P. 249–265. DOI: 10.1080/23270012.2014.992985.
5. Botta A., De Donato W., Persico V., Pescapé A. Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems. 2016. № 56. P. 684–700. DOI: 10.1016/j.future.2015.09.021.
6. Enabling condition-based maintenance decisions with proactive event-driven computing / A. Bousdekis, N. Papageorgiou, B. Magoutas, D. Apostolou, G. Mentzas. Computers in Industry. 2018. № 100. P. 173–183. DOI: 10.1016/j.compind.2018.04.019.
7. Chalal M., Boucher X., Marques G. Decision support system for servitization of industrial SMEs: a modelling and simulation approach. Journal of Decision Systems. 2015. № 24 (4). P. 355–382. DOI: 10.1080/12460125.2015.1074836.
8. Cullinan C., Sutton S.G., Arnold V. Technology monoculture: ERP systems, “techno-process diversity” and the threat to the information technology ecosystem. Advances in Accounting Behavioral Research. 2010. № 13. P. 13–30. URL: [www.emeraldinsight.com/10.1108/S1475-1488\(2010\)0000013005](http://www.emeraldinsight.com/10.1108/S1475-1488(2010)0000013005).
9. De Ugarte B.S., Artiba A., Pellerin R. Manufacturing execution system – a literature review. Production Planning and Control. 2009. № 20 (6). P. 525–539. DOI: 10.1080/09537280902938613.
10. Monitoring gas and oil fields with reliable wireless sensing and Internet of Things / W. Gharibi, M. Aalsalem, W.Z. Khan, N. Armi, W. Ghribi. International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET). 2017. DOI: 10.1109/icramet.2017.8253173.
11. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. № 29 (7). P. 1645–1660. DOI: 10.1016/j.future.2013.01.010.

12. Hao Y., Helo P., Shamsuzzoha A. Virtual factory system design and implementation: integrated sustainable manufacturing. *International Journal of Systems Science: Operations and Logistics*. 2018. № 5 (2). P. 116–132. DOI: 10.1080/23302674.2016.1242819.
13. Lewandowski D., Pareschi D., Pakos W., Ragaini E. (2018). Future of IoTSP – IT and OT Integration. *IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*. 2018. DOI: 10.1109/ficloud.2018.00037.
14. Miorandi D., Sicari S., De Pellegrinia F., Chlamtaca I. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*. 2012. № 10. P. 1497–1516.
15. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys and Tutorials*. 2014. № 16 (1). P. 414–454. DOI: 10.1109/SURV.2013.042313.00197.
16. Priyadarshy S. IoT revolution in oil and gas industry. *Internet of Things and Data Analytics Handbook*. 2016. P. 513–520. DOI: 10.1002/9781119173601.ch31.
17. Sood S.K., Sandhu R., Singla K., Chang V. IoT, big data and HPC based smart flood management framework. *Sustainable Computing: Informatics and Systems*. 2017. DOI: 10.1016/j.suscom.2017.12.001.
6. Bousdekis A., Papageorgiou N., Magoutas B., Apostolou D., Mentzas G. (2018). Enabling condition-based maintenance decisions with proactive event-driven computing. *Computers in Industry*, 100, 173–183. DOI: 10.1016/j.compind.2018.04.019.
7. Chalal M., Boucher X., Marques G. (2015) Decision support system for servitization of industrial SMEs: a modelling and simulation approach. *Journal of Decision Systems*, 24 (4), pp. 355–382. DOI: 10.1080/12460125.2015.1074836.
8. Cullinan C., Sutton S.G., Arnold V. (2010) Technology monoculture: ERP systems, “techno-process diversity” and the threat to the information technology ecosystem. *Advances in Accounting Behavioral Research*, 13, pp. 13–30. URL: www.emeraldinsight.com/10.1108/S1475-1488(2010)0000013005.
9. De Ugarte B.S., Artiba A., Pellerin R. (2009) Manufacturing execution system—A literature review. *Production Planning and Control*, 20 (6), pp. 525–539. DOI: 10.1080/09537280902938613.
10. Gharibi W., Aalsalem M., Khan W.Z., Armi N., Ghribi W. (2017). Monitoring gas and oil fields with reliable wireless sensing and Internet of Things. *2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*. DOI: 10.1109/icramet.2017.8253173.
11. Gubbi J., Buyya R., Marusic S., Palaniswami M. (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29 (7), pp. 1645–1660. DOI: 10.1016/j.future.2013.01.010.

---

#### REFERENCES:

1. Aalsalem M.Y., Khan W.Z., Gharibi W., Armi N. (2017). An intelligent oil and gas well monitoring system based on Internet of Things. *2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*. DOI: 10.1109/icramet.2017.8253159.
2. Aazam M., Khan I., Alsaffar A.A., Huh E.-N. (2014) Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2014*, art. no. 06778179, pp. 414–419. DOI: 10.1109/IBCAST.2014.6778179.
3. Babiceanu R.F., Seker R. (2016) Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. *Computers in Industry*, 81, pp. 128–137. DOI: 10.1016/j.compind.2016.02.004.
4. Bi Z., Cochran D. (2014) Big data analytics with applications. *Journal of Management Analytics*, 1 (4), pp. 249–265. DOI: 10.1080/23270012.2014.992985.
5. Botta A., De Donato W., Persico V., Pescapé A. (2016) Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, 56, pp. 684–700. DOI: 10.1016/j.future.2015.09.021.
12. Hao Y., Helo P., Shamsuzzoha A. (2018) Virtual factory system design and implementation: integrated sustainable manufacturing. *International Journal of Systems Science: Operations and Logistics*, 5 (2), pp. 116–132. DOI: 10.1080/23302674.2016.1242819.
13. Lewandowski D., Pareschi D., Pakos W., Ragaini E. (2018). Future of IoTSP – IT and OT Integration. *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*. DOI: 10.1109/ficloud.2018.00037.
14. Miorandi D., Sicari S., De Pellegrinia F., Chlamtaca I. (2012) Internet of things: Vision, applications and research challenges, *Ad Hoc Networks*, 10, p. 1497–1516.
15. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. (2014) Context aware computing for the internet of things: A survey. *IEEE Communications Surveys and Tutorials*, 16 (1), pp. 414–454. DOI: 10.1109/SURV.2013.042313.00197.
16. Priyadarshy S. (2016). IoT revolution in oil and gas industry. *Internet of Things and Data Analytics Handbook*, 513–520. DOI: 10.1002/9781119173601.ch31.
17. Sood S.K., Sandhu R., Singla K., Chang V. (2017). IoT, big data and HPC based smart flood management framework. *Sustainable Computing: Informatics and Systems*. DOI: 10.1016/j.suscom.2017.12.001.

**Atalavei V.T.**  
*Postgraduate Student at Department of Economics  
and Management,  
Sumy National Agrarian University*

## **CHALLENGES OF INFORMATION AND OPERATIONAL TECHNOLOGIES INTEGRATION AS A RESULT OF THE GROWING ROLE OF INDUSTRIAL INTERNET OF THINGS IN THE OIL AND GAS COMPANIES**

In the oil and gas industry, the prospects for using IoT are related not mainly to managing of existing assets, supply chains, or customer relationships but rather to creating a new value for information about them. An integrated strategy is crucial for companies seeking to find new value in the IIoT. One of these aspects in the management of the oil and gas industry companies, which requires a detailed analysis, is the convergence of information technology (IT) with operational technology (OT) as a consequence of the ever wider use of the IIoT.

Why do companies in the oil and gas industry use IIoT? Answering this question, the author highlights five reasons why the IIoT can revolutionize the oil and gas industry: 1) Improvement of operational efficiency; 2) Income boost potential; 3) Real-time data; 4) Reduced security risk; 5) Ecological footprint.

The author proposed the model of integration of IT and OT, in which convergence between these subsystems is divided into four levels. The author states that full integration between these subsystems begins at the level 3.5.

Greater connectivity and integration are obviously useful for intelligent analytics and management, but more connections and network devices mean more security intervention. Despite the fact that security has always been a priority for both IT and OT in traditional systems, these network systems represent new scenarios and risk profiles for both parties. Given this, the author believes that IT now needs to start thinking like OT and vice versa and spell out challenges faced by both IT and OT in that regards.