ВИМІРЮВАЛЬНІ СИСТЕМИ

АНАЛІЗ ПОТЕНЦІАЛУ КІБЕРФІЗИЧНИХ СИСТЕМ ДЛЯ ЗАСТОСУВАННЯ У АГРОСЕКТОРІ

ANALYSIS OF CYBERPHYSICAL SYSTEMS POTENTIAL FOR AGRICULTURAL APPLICATION

Бубела Т. З., д-р техн. наук, проф., Федишин Т. І., аспір.,
Національний університет "Львівська політехніка", Україна;
e-mail: paholuk@ukr.net

Tetiana Bubela, Dr. Sc., Professor, Tetiana Fedyshyn, PhD student,
Lviv Polytechnic National University, Ukraine;
e-mail: paholuk@ukr.net

https://doi.org/10.23939/istcmtm2019.04.00

Анотація. Забезпечення ефективної державної політики в галузі створення та функціонування кіберфізичних систем (КФС) в Україні вимагає детального вивчення сучасного стану та аналізу тенденцій розвитку КФС, їх видів у світі в галузі агропромисловості, особливостей механізмів державного управління ними у провідних країнах світу та особливо у ЄС, розроблення нормативного забезпечення КФС в Україні, прийняття вітчизняних і міжнародних стандартів як національних щодо різних вимог та технічних характеристик, необхідних для функціонування КФС, проведення сертифікації їх функціональної сумісності, забезпечення умов для професійного навчання кваліфікованих кадрів та підвищення їхньої кваліфікації для керування КФС, особливо у такій важливій сфері, як агровиробництво.

Ключові слова: кіберфізична система, нормативна документація, класифікація, агропромисловість.

Abstract. Ensuring an effective state policy in the field of creation and functioning of the Cyber-Physical Systems (further – CPS) in Ukraine requires a detailed study of the current state and analysis of trends in the development of CPS, their types in the world in the field of agro-industry, the peculiarities of public governance mechanisms in the leading countries of the world and especially in the EU, improvement of regulatory and legal support on CPS in Ukraine, adopting national and international standards as national, on different requirements and technical characteristics necessary for the functioning of CPS, holding certification of their interoperability, provision of conditions for vocational training of qualified personnel and improvement of their qualification to manage CPS.

The development of automation and GPS-assisted vehicle management in the agricultural sector has established the concept of precision agronomy and precision agriculture, as well as automation in the production chain. However, such systems have significant drawbacks related to the flexibility, rationing, reliability, and real-time presentation of data.

The mechanisms of control and standardization of the creation and functioning of the CPS in the field of agro-industry are analyzed. Suggestions for improving these processes have been created. In order to create appropriate regulatory, technical and metrological assurance, the classification of CPS is proposed by different criteria, namely: by industry, by type of work performed, by nature of the movement, by type of management. Taking into account the risks of CPS is particularly important for the agricultural sector. From a technical point of view, risks were identified during the construction and operation of the CPS. They relate to data heterogeneity, reliability, data management, privacy, security, and large-scale processing of large amounts of data. Based on the experience of European countries, where the term cyber-physical systems is used to describe firmware embedded systems that are connected to services available worldwide through global networks such as the Internet, and their diverse potential for development and use, the use of the term "cyber-physical system" and its definition in the national regulatory framework.

Based on the global trends in the functioning of the CPS, the need for their certification is substantiated, which must confirm the requirements for its reliability, security, stability, and confidentiality.

Key words: Cyber-Physical System, Regulatory Documentation, Classification, Agroindustry.

Вступ

Сучасні прогресивні технології в агросекторі ґрунтуються на використанні кіберфізичних систем з метою забезпечення можливості збирання даних та мережевого моніторингу і контролю [1]. Сучасне сільське господарство стикається із величезними проблемами, прагнучи створити стійке майбутнє в різних регіонах земної кулі. Прикладами таких глобальних викликів є: збільшення чисельності населення, урбанізація, зміни клімату. Глобальні економічні проблеми повинні вирішуватися так, щоб потенціал галузей сільського господарства не загрожував задоволенню світових потреб у харчових продуктах. З концепцією та потребами інновацій у сільському господарстві пов'язані різні фактори, серед яких доцільно виокремити такі: довкілля, біорізноманіття та охорона здоров'я. Зв'язок сільсь-

кого господарства та довкілля є джерелом викликів і технологічної оптимізації. За переваги інтенсивного агрокультурного виробництва людство розплачується втратою природного стану екосистем. Так, надмірне внесення добрив може спричинити загрозу забруднення навколишнього середовища, тоді як недостатня їх кількість може призвести до деградації ґрунту та втрати родючості [2–4]. У цих умовах системам сільськогосподарського виробництва необхідно більше зосередитися на ефективному збереженні та управлінні біорізноманіттям й екосистемними послугами, щоб вирішити подвійне завдання – екологічної стійкості та продовольчої безпеки, впроваджуючи такий надійний інструмент, як КФС.

Недоліки

Розвиток автоматизації та GPS-допоміжного керування транспортними засобами у агросекторі сприяли виникненню концепції точної агрономії та точного землеробства, а також автоматизації в ланцюзі виробництва. Однак такі системи мають істотні недоліки, пов'язані з гнучкістю, нормуванням, надійністю, поданням даних у режимі реального часу.

Мета роботи

Мета роботи – теоретичне обґрунтування механізмів керування та стандартизації процесів створення і функціонування КФС у галузі агропромисловості та розроблення пропозицій щодо їх удосконалення.

1. Кіберфізичні системи як засіб моніторингу, контролю та управління у сфері сільського господарства

1.1. Точне землеробство як запорука створення smart-технологій у сфері сільського господарства

Завдяки прогресу в останні десятиліття в галузі автоматизації та дистанційного зондування введено поняття точної агрономії та точного землеробства, а також автоматизації в ланцюзі виробництва продовольства. Точне землеробство та автоматизація вже встановили парадигми з метою підвищення продуктивності, якості та покращення умов праці за рахунок скорочення ручної праці. Усі ці фактори відіграють важливу роль у забезпеченні сталого розвитку агросектору. Багато сучасних фермерів уже використовують високотехнологічні рішення, наприклад, сільськогосподарське обладнання із цифровим керуванням, транспорт із підтримкою GPS, безпілотні літальні апарати для моніторингу та прогнозування. Створено частково і повністю автоматичні пристрої для більшості аспектів функціонування сільського господарства: від прищеплення до висівання та посадки, від збирання врожаю до сортування, пакування та боксу, а також для тваринництва. Незважаючи на те, що підходи до точного землеробства можуть бути ефективними та корисними для фермерів, після належного навчання вони, як правило, калібруються лише для виконання конкретного завдання, не забезпечуючи цілісного уявлення про агрокультурні процеси.

Доцільно зазначити, що сільське господарство можна розглядати як динамічну систему, в якій для кожного набору вхідних даних обов'язково отримують результат або кінцеві/проміжні продукти: однак різні умови можуть змінювати результати (наприклад, кліматичні умови, якість ґрунту, шкідники). Зовнішні фактори, які позитивно чи негативно впливають на сільськогосподарські системи, важко передбачити або контролювати. З цієї причини прогнозовані моделі не завжди можуть гарантувати очікувані результати. Тож необхідне створення кіберфізичних систем із безліччю функціональних можливостей. Фермери повинні знати стан своїх сільськогосподарських культур, а збирання даних моніторингу в реальному часі є найкращими рішеннями для упровадження інновацій та досягнення стійкої продуктивності. Отже, поєднання сучасних вимірювальних технологій з інструментарієм робототехніки є основою для концепції та методології розумного землеробства.

1.2. Класифікація кіберфізичних систем та види ризиків під час їх створення та функціонування

Аналізуючи відомі сьогодні КФС, їх метрологічне та програмне забезпечення, можна зробити висновок, що з невпинним зростанням їх кількості розширюються сфери їх застосування, а програмне та метрологічне забезпечення розвивається в напрямі підтримання роботи наявних КФС та їх придатності для конструювання нових. Тому вимогами, які ставлять, створюючи КФС, є безпека, конфіденційність, надійність, стійкість, гарантії щодо поширених взаємопов'язаних пристроїв та інфраструктур, динамічність, сумісність (можливість розмістити різні обчислювальні моделі), підтримка різних режимів комунікування у мережі, вирішення проблем складності (проблеми зондування та керування зі

зворотним зв'язком у будь-якій архітектурі КФС), синхронізація, взаємодія із експлуатаційним середовищем, можливість співпрацювати один з одним для забезпечення можливості поєднання кількох цілей.

З метою створення відповідного нормативно-технічного та метрологічного забезпечення КФС, їх доцільно класифікувати за різними критеріями. Зокрема залежно від використання КФС можна поділити так, як показано на рис. 1 [5].

Зауважимо, що в Європі одним із основних факторів використання кіберфізичних систем у сільському господарстві є оптимізування витрат на оплату праці [6]. Кіберфізичні системи можуть бути використані й використовуються практично в будь-якій галузі сільського господарства: в рослинництві, тваринництві, під час переробки сировини, транспортування, зберігання, реалізації продукції тощо. У зв'язку з цим важливе теоретичне і практичне значення має класифікація кіберфізичних систем у сфері агропромисловості (табл. 1).

Варто зазначити, що система управління сучасними промисловими кіберфізичними системами ґрунтується на повторенні запрограмованих рухів у фіксованих зонах, тоді як сільськогосподарські кіберфізичні системи використовують системи управління, що функціонують в умовах постійних змін природно-кліматичних умов. Ця система:

– забезпечує роботу з живими організмами – рослинами, тваринами, оперує з несортованими і неупорядкованими об'єктами (різними сортами рослин, чагарників, плодоносних дерев тощо);

– використовує інструменти та інше обладнання, призначені для роботи людини;

– забезпечує безпеку для людей і тварин, які працюють поруч.

З технічного погляду можна виокремити низку ризиків під час побудови та функціонування КФС, враховувати які важливо, зокрема, для агросектору (рис. 2).

1. Різнорідність даних. Різнорідність даних – це серйозна проблема, яка може негативно впливати на ефективність взаємодій і розроблення комунікаційних протоколів. Системи повинні бути здатні підтримувати велику кількість різних додатків і пристроїв.

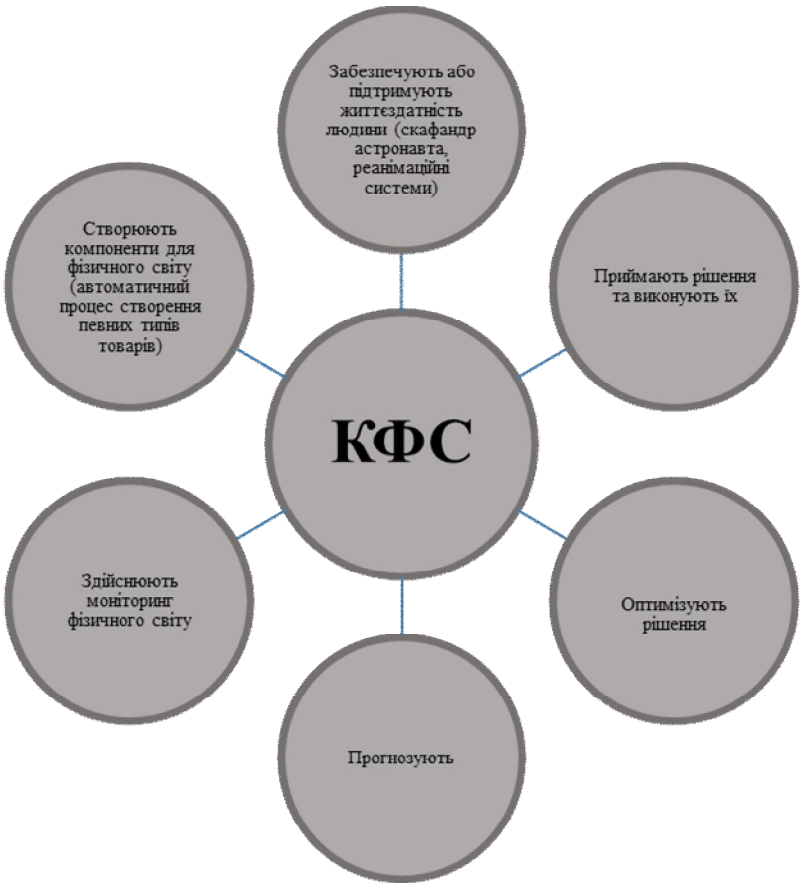

Рис. 1. Класифікація КФС за призначенням

Figure 1. CPS Classification by purpose

Класифікація КФС в агросекторі

Classification of agricultural CPS

Критерії класифікації кіберфізичних систем	Класифікація кіберфізичних систем
за галузями	– у тваринництві; – у рослинництві; – у допоміжних виробництвах
за видами виконуваних робіт	– посів сільськогосподарських культур; – обприскування рослин отрутохімікатами і добривами; – видалення, прополювання бур'янів; – контроль лабораторної схожості посівів; – збирання врожаю кормових культур; – збирання фруктів; – догляд за виноградниками та садовими деревами; – транспортування розсади в теплицях; – полив рослин у теплицях; – механізовані роботи з підготовки ґрунту, що виконуються безпілотним (автономним) транспортом – моніторинг сільськогосподарських угідь; – сортування сільськогосподарської продукції; – пакування сільськогосподарської продукції
за характером переміщення	– стаціонарні кіберфізичні системи; – мобільні кіберфізичні системи; – безпілотні кіберфізичні системи
за типом управління	– керована оператором; – автономна

Рис. 2. Ризики, пов'язані зі створенням та функціонуванням кіберфізичних систем

Figure 2. Risks of creation and operation of CPS

2. Надійність. Кіберфізичні системи можна використовувати в таких критично важливих галузях, як охорона здоров'я, інфраструктура, транспорт, агропромисловість і багато інших, основними вимогами до яких є надійність і безпека, оскільки виконавчі елементи впливають на навколишнє середовище та здоров'я людей. Крім того, кіберфізичні системи повинні бути здатні продовжувати роботу в непередбачуваних умовах і адаптуватися до будь-яких впливів.

3. Управління даними. Необхідно зберігати й аналізувати великі обсяги даних, що надходять від різних мережевих пристроїв, опрацьовувати їх і в реальному часі виводити результати. Даними можна керувати з використанням відкладеного або оперативного поточного опрацювання залежно від призначення системи. У разі використання потоків у реальному часі інформація може часто змінюватися і опрацювання повинно ґрунтуватись на адаптивних і постійних запитах.

4. Конфіденційність. Проблема полягає у підтримці балансу між збереженням конфіденційності та захистом персональних даних і доступністю даних для надання якіснішого обслуговування. Оскільки кібер-фізичні системи керують значними обсягами даних, що містять конфіденційну інформацію, виникають серйозні проблеми забезпечення їх конфіденційності.

5. Безпека. Кіберфізичні системи повинні забезпечувати безпеку комунікацій, оскільки всі дії координуються між пристроями в реальному часі. Кіберфізичні системи розширюють масштаб і обсяг взаємодії між фізичними й обчислювальними системами, що ускладнює завдання забезпечення безпеки. Для вирішення цієї проблеми недостатньо традиційних інфраструктур, тож потрібно шукати нові рішення. Необхідно захищати як поточні дані, так і збережувані дані, зібрані для використання у майбутньому. Окрім того, кіберфізичні системи використовують різні додатки і бездротові комунікації, що часто ускладнює забезпечення безпеки.

6. Реальний час. Кіберфізичні системи керують великими обсягами даних, отриманих від сенсорів, опрацювання яких повинно бути ефективним і своєчасним, оскільки фізичні процеси тривають незалежно від результатів обчислень. Щоб задовольнити цю вимогу, кіберфізичні системи повинні мати відповідно високу пропускну спроможність, оскільки несвоєчасне виконання дій може призвести до спотворення інформації.

1.3. Нормативне забезпечення створення та функціонування кіберфізичних систем

Забезпечення ефективної державної політики у галузі створення та функціонування КФС в Україні вимагає детального вивчення сучасного стану та аналізу тенденцій розвитку КФС, їх видів у світі в різних галузях економіки, особливостей механізмів управління ними у провідних країнах світу, особливо у ЄС, удосконалення нормативно забезпечення щодо КФС в Україні, прийняття вітчизняних і міжнародних стандартів як національних щодо різних вимог та технічних характеристик, необхідних для функціонування КФС, проведення сертифікації їх функціональної сумісності, забезпечення умов для професійного навчання кваліфікованих кадрів та підвищення їх кваліфікації для керування КФС. У зв'язку зі стрімким розвитком інформаційних технологій, розширенням надання послуг у кіберпросторі та розширенням сфер застосування кіберфізичних систем виникає необхідність розроблення уніфікованого загальноприйнятого визначення кіберфізичних систем. Тому доцільно детальніше розглянути особливості нормативного забезпечення функціонування КФС у провідних країнах світу.

Міжнародні організації International Electrotechnical Commission (IEC), International Organization for Standardization (ISO) та Standards Association (IEEE) створили низку стандартів для КФС [7], які можна систематизувати за рівнями їх функціонування, а саме:

рівень розумного з'єднання, який відповідає за отримання даних від фізичних об'єктів. Найпоширенішою методикою є Automatic Identification and Data Capture (AIDC) тобто використання автоматичної ідентифікації та збирання даних. ISO/IEC 19762:2016 подає терміни та визначення для AIDC. Серія ISO/IEC 15459 визначає унікальну ідентифікацію для процедур реєстрації, загальні правила, індивідуальні транспортні одиниці, індивідуальні продукти та пакети товарів, індивідуальні товари, що підлягають поверненню, транспортні товари та угруповання. Для КФС важливе використання сенсорів для автоматичного збирання даних із виробничих систем. ISO/IEC/IEEE 21450:2010 визначає основні функції, необхідні для керування системою та керування розумними сенсорами. Серія ISO/IEC/IEEE 21451 описує Network Capable Application Processor (NCAP) та інформаційну модель і протоколи зв'язку, Transducer Electronic Data Sheet (TEDS) для розумних сенсорів. Стандартні методи управління сенсорами дуже важливі. Так, серія IEC 61131 визначає основні функціональні характеристики програмованих систем управління. IEC 61499 визначає загальну модель для розподілених систем управління на основі стандарту IEC 61131, IEC 61131 і IEC 61499 дає настанови для встановлення надійного, взаємозамінного зв'язку із системами управління.

Рівень перетворення даних на інформацію охоплює опрацювання даних із погляду рівня інтелектуального з'єднання та аналізу інформації. Стандарти IEC 61804-3, IEC 61804-4, IEC 6180-5 та IEC 61804-6 (Мова електронного опису пристрою, EDDL) використовують для опису характеристик пристроїв. Серія IEC 61360 дає основу для чіткого та однозначного визначення характеристичних власти-

востей (типів елементів даних) усіх елементів електротехнічних систем – від основних компонентів до вузлів і повноцінних систем. Крім того, серія IEC 62714 забезпечує формат обміну даними, який називається автоматизованою мовною розміткою, тобто Automation Markup Language (AML). Вищезазначені стандарти забезпечують наявність уніфікованих даних. У IEC/ISO13236:1998 встановлено, що високоякісна система стосується середовища інформаційних технологій (IT). Оскільки безпека даних є важливим питанням, то у стандарті ISO 27000 містяться рекомендації щодо найкращої практики у галузі інформації та управління і контролю ризиків з метою досягнення безпеки. IEC 62443 серія (ISA99) використовується для забезпечення безпеки промислових систем автоматизації та управління і забезпечує комплексний захист і безпеку.

Рівень кіберобчислень. Комунікація є найважливішим елементом, що розглядається на рівні кіберфізичних систем та обчислень. Обмін КФС даними та інформацією потребує декількох відповідних стандартів, до яких належать стандарти дротового та бездротового зв'язку. ISO/IEC 8802 забезпечує сукупність міжнародних стандартів, які описують локальні мережі. Існує кілька стандартів дротового зв'язку. Серія IEC 61158 та IEC 61784 є стандартами для типів та профілів шин, зокрема загальних промислових протоколів, PROFIBUS і PROFINET, P-Net, WorldFIP, INTERBUS, SwiftNet, CC-Link, HART, VNET/IP, TCnet, EtherCAT, Ethernet POWERLINK Ethernet for Plant Automation (EPA), Modbus, SERCOS, Rapi Net, SafetyNet p та MECHATROLINK. Ці протоколи містять розподілене управління у реальному часі в КФС із бездротовим зв'язком. IEC 62591 (Wireless HARTTM) та IEC 62601 (WIA-PA) доцільно використовувати для промислового бездротового зв'язку та промислових вимірювань, моніторингу та контролю. Серія ISO/IEC 14476 покращує транспортний протокол зв'язку, щоб забезпечити доброякісне обслуговування, тобто good quality of service (QoS). Якісна промислова мережа повинна використовувати вищезазначені стандарти для зв'язку сенсорної та машинної мережі. ISO/IEC 20005, ISO/IEC 29180, ISO/IEC 29182, ISO/IEC 30101 та ISO/IEC 30128 використовують для створення інтелектуальних, надійних та безпечних сенсорних мереж. Крім цього, ISO/IEC 17826 задає інтерфейс для доступу до хмарного сховища та керування даними, що зберігаються всередині. Стандарти ISO/IEC 27033 забезпечують надійність мережі. IEC 62769 використовується для інтеграції пристроїв із застосуванням комунікаційних технологій.

Рівень пізнання передбачає моніторинг та прийняття рішень. Серія ISO 13374 забезпечує основні вимоги до відкритих специфікацій програмного забезпечення, які дають машинам змогу контролювати дані, їх опрацювання та зв'язок. IEC 62453 нормує інтегрування всіх пристроїв незалежно від постачальників.

Рівень конфігурації містить стандарти загального контролю за КФС. Зокрема IEC 61512 визначає моделі контролю, терміни та моделі даних. IEC 62264, що використовується для інтеграції системи управління підприємством, підвищує одноманітність та послідовність побудови інтерфейсу. Стандарт зменшує ризик, вартість та помилки, пов'язані із реалізацією цих інтерфейсів. IEC 61508 підвищує безпеку та забезпечує надійність життєвого циклу та контроль промислового процесу.

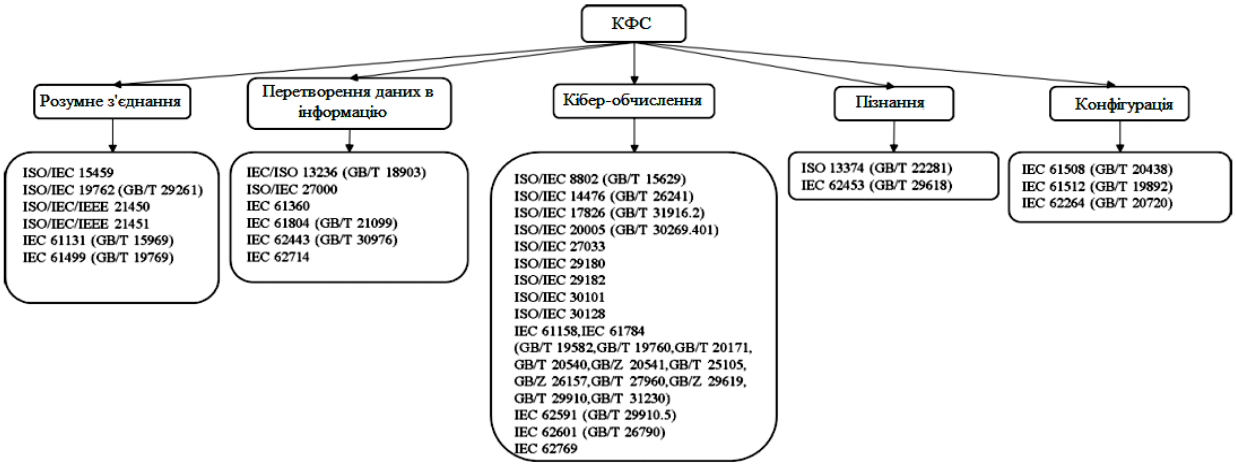

Рис. 3. Структура міжнародних стандартів для КФС

Figure 3. CPS international standard structure

Як вже зазначено вище, невід'ємною необхідною складовою функціонування кіберфізичних систем є кібербезпека. В Україні також велику увагу звертають на формування нормативної документації щодо безпеки [8–12]. Видано Указ Президента України від 15.03.2016 року "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". Також 05.10.2017 р. ухвалено Закон України "Про основні засади забезпечення кібербезпеки України", який містить поняття кібербезпеки, що є невід'ємною складовою КФС як стан безпечного, надійного, стійкого їх функціонування з урахуванням вимог конфіденційності. Натомість Стратегія кібербезпеки та Закон не містять поняття кіберфізичних систем, хоча їх дедалі ширше застосовують у світі в агропромисловості, енергетиці, охороні здоров'я, в транспортній сфері.

Результати і обговорення

Є необхідність у чіткому формулюванні поняття кіберфізичних систем та їх основних універсальних особливостей та належного нормативного врегулювання функціонування КФС. Зважаючи на це, запропоновано ввести у нормативні документи з метрології поняття "кіберфізична система" із таким її визначенням: кіберфізична система – це інтелектуальна система, що включає мережі фізичних та обчислювальних компонентів, які інженерно взаємодіють.

Можна дійти висновку, що і в рамковому документі Німеччини про КФС, і в рамковому документі США звернено увагу на необхідність відповідної сертифікації КФС, яка підтверджуватиме вимоги надійності, безпеки, стійкості, конфіденційності КФС. На необхідності сертифікації наголошено також у рамковому документі ЄС Cyber-Physical European Roadmap & Strategy Research Agenda and Recommendations for Action, відповідно до якого сучасні методи та інструменти (засоби) для сертифікації тепер вже не є абсолютно адекватними для сертифікації КФС через їх невідповідність вимогам сучасних КФС залежно від середовища КФС. Іншим питанням, на якому наголошено в рамковому документі Німеччини про КФС і у відповідному рамковому документі США, є питання прийняття та застосування уніфікованих стандартів КФС. Для того, щоб дати універсальне повноцінне визначення КФС, варто проаналізувати аспекти створення КФС. Це зроблено ґрунтовно в рамковому документі США Framework for Cyber-Physical Systems Release May 2016 Cyber Physical Systems Public Working Group.

Численні зусилля різних міжнародних організацій у сфері створення стандартів кіберфізичних систем, зокрема ISO, ITU, Industrial Internet Consortium, IoT-A тощо, досі не забезпечили повну сумісність цих стандартів щодо різнорідних КФС. Тож питання стандартизації КФС є відкритим і потребує вирішення як на міжнародному, так і на національному рівні.

Висновки

КФС – складна, розпорошена система, яка інженерно взаємодіє, що об'єднує фізичні об'єкти, хмарні обчислення, засоби зв'язку, а також сенсори та актуатори, що здійснюють моніторинг стану фізичних об'єктів у реальному часі у всіх галузях діяльності, зокрема в агросекторі, тож стандартизація КФС є необхідним та складним завданням.

Ураховуючи досвід європейських країн, де термін "кіберфізичні системи" використовують для опису програмно-апаратних вбудованих систем, які підключені до послуг, доступних в усьому світі через глобальні мережі, такі як Інтернет, і їх різноманітного потенціалу для розроблення та використання, доцільно імплементувати термін "кіберфізичні системи" та його визначення у вітчизняну нормативну базу.

Керуючись світовими тенденціями функціонування КФС, обґрунтовано необхідність їх сертифікації, яка повинна підтверджувати вимоги до її надійності, безпеки, стійкості та конфіденційності.

Подяка

Автори висловлюють вдячність колективу кафедри інформаційно-вимірювальних технологій Національного університету "Львівська політехніка" за надану допомогу та всебічне сприяння у підготовці статті.

Конфлікт інтересів

Автори заявляють про відсутність будь-якого фінансового або іншого можливого конфлікту, що стосується роботи.

Література

[1] *Cyber-Physical Systems*. Metrological Issues, Editors S. Yatsyshyn, B. Stadnyk, Spane: Barcelona, IFSA Publishing, 2016.

[2] А. О. Мельник, "Кіберфізичні системи: проблеми створення та напрями розвитку", *Вісник Національного університету Львівська політехніка Комп'ютерні системи та мережі*, № 806, с. 154–161, 2014.

[3] V. Yatsuk, T. Bubela, Ye. Pokhodylo, Yu. Yatsuk, R. Kochan, "Improvement of data acquisition system of objects physic-chemical properties", *in Proc. of the 9th IEEE International Conference on "Intelligent Data Acquisition and Advanced*

Computing Systems: Technology and Applications", Bucharest, Romania, pp. 41–46, 2017.

[4] Guidance "*The key principles of vehicle cyber security for connected and automated vehicles*", 6 August 2017 [Online]. Available: www.gov.uk.

[5] О. М. Колодчак, "Універсальна структурна модель засобів прийняття рішення в кіберфізичних системах", *Моделювання та інформаційні технології*, т. 79, с. 107–113, 2017.

[6] Cyber Physical Systems Public Working Group "*Framework for Cyber-Physical Systems Release 1.0*", May 2016 [Online]. Available: www.nist.gov.

[7] J. C. Trappey, (Senior Member, IEEE), Charles V. Trappey Usharani Hareesh Govindarajan, John J. Sun, Allen C. Chuang "*A Review of Technology Standards and Patent Portfolios for Enabling Cyber-Physical Systems in Advanced Manufacturing*", 2016. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7600420.

[8] Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. [Online]. Available: http://zakon.rada.gov.ua/ laws/show/2163-19.

[9] Держспоживстандарт України ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. *Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Еталонна модель*, Київ, Україна, 2004.

[10] ДСТУ ISO 7498-2:2004 *Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура захисту інформації*; Київ, Україна, 2006.

[11] ISO/IEC 27033-1:2009. *Information technology. Security techniques. Network security. Part 1: Overview and concepts (Інформаційна технологія. Методи захисту. Захист мережі. Частина 1. Огляд та концепції)*; ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2009 [Online]. Available: https://www.iso.org/standard/51580.html

[12] ISO/IEC 27033-2:2012. *Information technology. Security techniques. Guidelines for the design and implementation of network security (Інформаційна технологія. Методи захисту. Керівництво для розробки та впровадження захисту мережі)*. Information security, cybersecurity and privacy protection, 2012 [Online]. Available: https://www.iso.org/standard/51581.html

References

[1] *Cyber-Physical Systems*. Metrological Issues, Editors S. Yatsyshyn, B. Stadnyk, Spane: Barcelona, IFSA Publishing, 2016.

[2] A. Melnyk, "Cyber-physical of the system: problems of creation and directions of development", *Computer systems and networks,* Lviv Polytech. Publ. House, Ukraine: no. 806, 2014, p. 154–161.

[3] V. Yatsuk, T. Bubela, Ye. Pokhodylo, Yu. Yatsuk, R. Kochan, "Improvement of data acquisition system of objects physic-chemical properties", *in Proc. of the 9th IEEE Int. Conf. on* "*Intel. Data Acquis. and Adv. Comp. Systems: Technology and Applications*", Bucharest, Romania, 2017, pp. 41–46.

[4] Guidance "*The key principles of vehicle cybersecurity for connected and automated vehicles*", 6 Aug. 2017, [Online]. Available: www.gov.uk.

[5] O. Kolodchak "Universal structural model of decision-making tools in cyber-physical systems", *Modelling and information technologies*, no. 79, p. 107–113, 2017.

[6] Cyber-Physical Systems Public Working Group "*Framework for Cyber-Physical Systems Release 1.0*", May 2016 [Online]. Available: www.nist.gov.

[7] J. C. Trappey, Ch. V. Trappey, U. Govindarajan, J. Sun, A. Chuang, "*A Review of Technology Standards and Patent Portfolios for Enabling Cyber-Physical Systems in Advanced Manufacturing*", 2016. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7600420.

[8] On the basic principles of ensuring the cybersecurity of Ukraine. Law of Ukraine from 05.10.2017 [Online]. Available: http://zakon.rada.gov.ua/ laws / show / 2163-19.

[9] State Consumer Standard of Ukraine DSTU ISO / IEC 7498-1: 2004. Information Technology. The interconnection of open systems. Basic reference model. Part 1. The reference model, Kyiv, Ukraine, 2004.

[10] DSTU ISO 7498-2: 2004 *Information processing systems. The interconnection of open systems. Basic reference model. Part 2. Information security architecture*; Kyiv, Ukraine, 2006.

[11] ISO/IEC 27033-1:2009. *Information technology. Security techniques. Network security. Part 1: Overview and concepts*: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, 2009 [Online]. Available: https://www.iso.org/standard/51580.html

[12] ISO / IEC 27033-2: 2012. *Information technology. Security techniques. Guidelines for the design and implementation of network security (Information Technology. Security Methods. Guidelines for Developing and Implementing Network Security)*. Information security, cybersecurity and privacy protection, 2012 [Online]. Available: https://www.iso.org/standard/51581.html