УДК 004.056.5

Тарасенко Ю.С., канд. фіз. - мат. наук, доцент
Клим В.Ю., канд. техн. наук
Савченко Ю.В., канд. техн. наук, доцент
Університет митної справи та фінансів, м. Дніпро, v0123klim@gmail.com

КІБЕРФІЗИЧНІ МОЖЛИВОСТІ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кіберфізичні системи (КФС) – це інтелектуальні системи, що включають в себе інженерно-взаємодіючі мережі фізичних та обчислювальних компонентів, тобто через комп'ютерні мережі і вбудовані контролери забезпечується (автономно або за участю людини) управління фізичними процесами за допомогою реалізації зворотних зв’язків [1].

Сучасні КФС мають широкий спектр призначення, зокрема для забезпечення захисту об'єктів критичної інфраструктури (ОКІ). При цьому, «не існує єдиної “мови” створення КФС, яка б інкапсулювала відмінності у підходах до розроблення компонент КФС на її різних рівнях» [2]. Однак, згідно [2], є «три основні тенденції у спробах запропонувати уніфікований підхід до побудови КФС», з яких «на найбільш базовому рівні структура КФС формується з» сіми основних компонент. Їх функціональна повнота аналогічна побудові структурно-логічної та структурно-функціональної схемам (СЛС та СФС) при реалізації радіолокаційних систем виявлення, вимірювання, дозволу та розпізнавання. Причому, основою побудови СЛС та СФС, в тому числі і для випадку оцінювання можливостей КФС по захисту ОКІ, прийнято вважати лінгвістичний опис (мовне середовище) об'єкта пізнання з відображенням його внутрішніх та зовнішніх причинно-наслідкових зв'язків та врахуванням існуючих загроз. Фактично, відмінність СЛС від СФС, головним чином полягає у тому, що перша дозволяє проводити аналіз статичної картини об'єкта пізнання із зазначенням прив'язки (локації) функціональних елементів (ланок), а друга – оцінити динамічні можливості об'єкта пізнання, оскільки крім вказівки локації задіяних елементів і вузлів кожна з них відображає їх взаємодію. Завдяки цьому, обгрунтована можливість побудови конструктивних моделей із елементами інтелектуальної кіберфізичної системи [3].

Відмітимо, що основою розроблення різних моделей кіберфізичних систем є наявність засобів вимірювання (ЗВ) та їх програмного забезпечення, де ЗВ необхідні для контролю параметрів технологічних процесів та навколишнього середовища (НС). Крім того, до особливостей сучасних КФС слід віднести функціональну автономність (як основну з точки зору призначення КФС) та мобільність, а їх реалізація «вимагає наявності всіх п’яти основних галузей інформаційної сфери: вимірювання (отримання або сприймання), зв'язок (передача), керування (вплив), обробка (опрацювання), запам’ятовування інформації» [4]. В даному випадку КФС також є системою з критичною областю застосування [5]. Тому, при проектуванні таких систем висувають підвищені зобов`язання до надійності і безпеки ЗВ з метою виконання жорстких вимог з оцінки ризиків кібербезпеки в умовах реалізації принципу невизначеності при забезпеченні метрологічної достовірності вимірювань за допомогою цих засобів вимірювання. Безпосередньо концепція принципу достовірності підтвердження відповідності ЗВ побудована на основі оцінки прийнятних ризиків і аналізу функціонування комбінованої системи підтвердження відповідності в умовах невизначеності, де підсумкові результати вимірів традиційно вимагають наявності їх достовірності, що ототожнюється з їх апостеріорною похибкою. При чому, саме поняття "похибки результату вимірів" корелює з поняттям істинного значення, чого принципово неможливо досягти. Отже, належний метрологічній контроль ЗВ необхідно реалізовувати в умовах невизначеності згідно з міжнародними стандартами, що розробляються відповідно

до Директив ISO / МЕК [6]. Саме тому, в ході сучасних подій та явищ безпосередній детальний аналіз радіоелектронних вимірів (як технічний основи КФС) з позицій їх адекватності, достовірності і надійності дозволяє констатувати, що викладене вище, аналогічно ближній або нелінійній радіолокації з отриманням та обробкою інформації, де їхня мобільна реалізація вдало використана, наприклад, у безпілотних літальних апаратах (дронах). Останні, незалежно від поставлених завдань (охорони чи розвідки з метою захисту чи заподіяння шкоди), комплектуються мобільними радіотехнічними засобами різної цілевказівки, СЛС та СФС яких фактично ідентичні «технічним і технологічним компонентам» інтелектуальної кіберфізичної системи як сукупності «технології вбудованих систем» [7] з кінцевою схемотехнічною реалізацією у вигляді взаємно-кореляційного пристрою та порогового (фільтруючого) вихідного субблоку [8]. Рівень спрацьовування останнього апріорі задає особа, яка приймає рішення, виходячи із відношення правдоподібності, що залежить від апріорної ймовірності помилкової тривоги або правильного виявлення при забезпеченні захисних заходів щодо ОКІ. Причому наявність інтелектуальних КФС тільки підвищує стійкість до кібератаки і ступінь безпеки [7].

Таким чином, виявлення атак порушників або зловмисників, які застосовують дрони, доцільно реалізовувати з використанням вбудованої КФС у радіолокаційні засоби спостереження (вимірювання) НС з використанням безперервного надвисокочастотного зондувального шумоподібного сигналу. Вибір оптимальних параметрів останнього, з одного боку, залежить від апостеріорного результату аналізу його сигнальної функції та відповідного об'ємного тіла невизначеності, а з іншого боку – дозволяє забезпечувати скритність штатного безперервного процесу забезпечення захисту ОКІ з позицій виявлення, дозволу та розпізнавання будь-яких порушень повітряного навколишнього середовища.

Список посилань

1. Чунжі Ван. Кіберфізичні системи та їх програмне забезпечення / Ван Чунжі, С.П. Яцишин, О.В. Лиса, А.В. Мідик // Вимірювальна техніка та метрологія: міжвідомчий науково-технічний збірник. Львів: вид-во НУ «Львівська політехніка». – 2018. – Т. 79. – № 1. – С. 34 – 38.

2. Голембо В. Підходи до побудови концептуальних моделей кіберфізичних систем / В. Голембо, О. Бочкарьов // Вісн. НУ "Львівська політехніка". Сер.: Комп’ютерні науки та інформаційні технології. – 2017. – № 864. – С. 168 – 178.

3. Тарасенко Ю.С. Інформаційні системи з позицій забезпечення надійності та невизначеності вимірювань / Ю.С.Тарасенко, В.Г. Соляніков // Зб. матеріалів міжнар. наук.-практич. інтерн.-конф. «Інноваційні технології, моделі управління кібербезпекою – «ІТМК-2021», УМСФ, Дніпро, 14 – 16 квітня, 2021. – С. 29 – 30.

4. Голембо В.А. Підходи до побудови концептуальних моделей кіберфізичних систем / В.А. Голембо, О Ю. Бочкарьов // Матер. Другого наук. семінару “Кіберфізичні системи: досягнення та виклики”, НУ «Львівська політехніка», Львів, 21-22 червня, 2016. – С.68 – 74.

5. Иванченко О.В. Концепция управления готовностью критических инфраструктур на основе применения информационных технологий / О.В. Иванченко, К.В. Смоктий, О.Д .Смоктий, В.С. Харченко // Системи та технології. – 2016. – Вип.1 (55). – С.5 – 23.

6. ISO/IEC Guide 98-1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT. Неопределенность измерения. Часть 1. Введение в руководства по выражению неопределенности измерения. – М.: Стандартинформ. – 2017.

7. Аулін В.В. Кіберфізичний підхід при створенні, функціонуванні та удосконаленні транспортно-виробничих систем / В.В. Аулін, А.В. Гриньків, А.О. Головатий // Центральноукраїнський науковий вісник. Технічні науки. – 2020. – Вип. 3(34). – С.331 – 343. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.32515/2664-262X.2020.3(34).331-343.

8. Тарасенко Ю.С. Фізичні основи радіолокації / Ю.С. Тарасенко. – Дніпро: Пороги, 2011. – 487с.