ВСТУП

Інформатизація, інтелектуалізація та безпека взаємопов'язані в Концепції Національної програми інформатизації (НПІ): розвиток сучасних ІТ – у частині завдань НПІ та у частині формування національної інфраструктури інформатизації; забезпечення інформаційної безпеки – у частині інформатизації стратегічних напрямів; розроблення і впровадження базових інтелектуальних технологій – у частині реалізації проєктів НПІ. Тенденції розвитку сегментів НПІ – інформаційних технологій, засобів інтелектуалізації, засобів апаратно-програмного захисту інформації інтегруються у міжнародний інформаційний та інтелектуальний простір рамкової програми ЄС "Горизонт – 2020", зокрема у частині цільової комплексної програми наукових досліджень Національної академії наук України "Проблеми ресурсу і безпеки експлуатації конструкцій, споруд та машин", Української стратегії Індустрії 4.0, Концепції інформаційної безпеки України.

Інформаційні технології відбирання і оброблення різнорідних даних від об'єктів дослідження (ОД) – основний інструментарій для розв'язання прикладних задач: неруйнівного контролю (НК)/технічного діагностування (ТД) матеріалів/конструкцій; моніторингу природних екосистем, які взаємодіють із техногенними. Для контролю та оцінювання параметрів технічного стану об'єктів за дії експлуатаційних факторів – механічного навантаження, температури, газоподібного водню, води як технологічного ресурсу – за критерієм "міцність – ресурс" потрібні гарантоздатні ІТ для оперативного управління станом об'єктів.

З метою комплексного вирішення проблемних завдань безпеки експлуатації техногенних об'єктів та безпеки ІТ як засобу відбирання даних та оцінювання параметрів роботоздатності у монографії сформовано єдиний підхід до забезпечення безпеки системи "об'єкт – ІТ". Підхід враховує аспекти розроблення: методологій створення ІТ відбирання і оброблення даних про фактичний стан об'єктів відповідно до структури "неруйнівний контроль – вимірювання – оцінювання" для мінімізації ресурсного ризику "дефект – руйнування – загроза – збитки"; методології безпеки автоматизованих систем контролю для мінімізації інформаційного ризику "витік – модифікація – знищення" у структурі функціонального ризику "невизначеність – відмова – аварія" згідно з концепцією "об'єкт – загроза – захист", що є новим сегментом наукового напряму цілісного вирішення завдань безпеки промислових об'єктів у контексті ІТ на рівні "роботоздатність – гарантоздатність".

Розвиток підходів до інтелектуалізації інфраструктури держави представлений технологіями побудови кіберфізичних систем та створенням методології

їх безпеки, що є актуальним напрямом у контексті вирішення завдань національної парадигми сталого розвитку України; воєнної (оборонної) доктрини України. Формування методологічних засад захисту інформації в КФС, опрацювання вимірювальної інформації вагомі у контексті досягнення безпеки системи "контроль об'єктів – оброблення інформації – управління" і дає підстави для ефективної реалізації комплексу завдань за вектором безпеки Стратегії сталого розвитку "Україна – 2020" та створення базового підходу до забезпечення інформаційної безпеки. Побудова та реалізація захищених кіберфізичних систем у предметних сферах суспільства на основі системного підходу та принципів інтеграції відповідних методів і засобів, спрямованих на забезпечення безпеки структури "об'єкт – КФС", є одним із механізмів забезпечення природно-техногенної та екологічної безпеки.

У монографії висвітлено: 1) у частині інформатизації – концепцію побудови ІТ відбирання різнорідних даних від об'єктів та методологію їх безпеки для прийняття рішення щодо управління проблемними ситуаціями: методологічний підхід до створення ІТ відбирання даних методом акустичної емісії; системний підхід до оцінювання концентрації водню у феромагнетиках магніторелаксаційним методом; комплексний підхід до визначення НДС тензометричним методом, модель оцінювання екологічного ризику на основі ІТ відбирання й оброблення параметрів води як технологічного ресурсу, методологію комплексної системи безпеки ІТ у межах структури гарантоздатності; 2) у частині інтелектуалізації – парадигму, концепцію та універсальну платформу створення комплексних систем безпеки КФС з метою забезпечення конфіденційності, цілісності, доступності інформації в багаторівневій структурі "контроль/оброблення – передавання/приймання – управління".