Міністерство освіти і науки України

Національний аерокосмічний університет імені М.Є. Жуковського
«Харківський авіаційний університет»

«ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ КРИТИЧНИХ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ»

ХАРЧЕНКО Вячеслав Сергійович – Заслужений винахідник України, доктор технічних наук, професор, завідувач кафедри Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ»

ЯКОВЛЕВ Сергій Всеволодович – Заслужений діяч науки і техніки України, доктор фізико-математичних наук, професор, професор Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ»

ЛУКІН Володимир Васильович – доктор технічних наук, професор, завідувач кафедри Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ»

ГОРБАЧИК Олена Семенівна – кандидат технічних наук, старший науковий співробітник, старший науковий співробітник Інституту проблем реєстрації інформації НАН України

ЛЕТИЧЕВСЬКИЙ Олександр Олександрович – доктор фізико-математичних наук, старший науковий співробітник, провідний науковий співробітник Інституту кібернетики ім. В.М. Глушкова НАН України

СІОРА Олександр Андрійович – кандидат технічних наук, генеральний директор ПАТ «Науково-виробниче підприємство «Радій»

СИДОРЕНКО Микола Федорович – Заслужений винахідник України, кандидат технічних наук, доцент, головний конструктор ДНВП «Об'єднання Комунар» - начальник НТ СКБ «ПОЛІСВІТ»

УРИВСЬКИЙ Леонід Олександрович – Заслужений діяч науки і техніки України, доктор технічних наук, професор, завідувач кафедри Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського»

РЕФЕРАТ

Харків – 2019

Робота охоплює дослідження та розробки зі створення наукових основ безпечних інформаційно-керуючих систем (ІКС), оцінювання та забезпечення функціональної безпеки критичних ІКС, їх компонентів і підсистем на різних етапах життєвого циклу, які виконано за останні 30 років у Національному аерокосмічному університеті імені М.Є. Жуковського «ХАІ» (м. Харків), Національному технічному університеті України "Київський політехнічний інститут імені Ігоря Сікорського", Інституті кібернетики імені В. М. Глушкова НАН України, Інституті проблем реєстрації інформації НАН України (м. Київ), Науково-технічному спеціалізованому конструкторському бюро «ПОЛІСВІТ» Державного науково-виробничого підприємства «Об'єднання Комунар» (м. Харків), Публічному акціонерному товаристві «Науково-виробниче підприємство «Радій» (м. Кропивницький).

Актуальність дослідження. Вартість відмов апаратних, програмних і комунікаційних (мережних) засобів критичних інформаційно-керуючих систем (ІКС), які є ключовим інструментом забезпечення надійності, безпеки та живучості критичних об'єктів та інфраструктур, зокрема аерокосмічних, енергетичних, медичних тощо, є надзвичайно високою. Це зумовлює необхідність: по-перше, гарантованого виконання вимог до рівня стійкості до відмов системних засобів, збурень різної природи та змін характеристик середовища; по-друге, забезпечення якості розроблення і точності відтворення реальних потреб використання ІКС за призначенням; по-третє, мінімізації часових, енергетичних та інших ресурсів, які використовуються.

Найважливішою характеристикою критичних ІКС є функціональна безпека, яка відповідно до міжнародних і національних стандартів визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та/або його наслідки. Для України актуальність нормування, моніторингу, оцінювання та забезпечення функціональної безпеки підтверджується наявністю великої кількості аварійно небезпечних об'єктів, перш за все АЕС, енергетичних систем і комунікацій, авіаційних і ракетно-космічних комплексів. Вона зростає внаслідок поглиблення рівня інформатизації об'єктів, важливих з точки зору безпеки, ускладнення програмних і апаратних засобів, збільшення інтенсивності можливих утручань і кібератак. Таким чином, важливість забезпечення функціональної безпеки критичних ІКС є одним із визначальних чинників безпеки України в цілому.

Метою роботи є забезпечення функціональної безпеки інформаційно-керуючих систем у критичних галузях, де відмови, зумовлені фізичними і проектними дефектами, атаками на вразливості, можуть призвести до значних матеріальних втрат, аварій, загрози життю людей. Це досягається шляхом розроблення та впровадження методологічних засад, математичних моделей, методів, програмно-апаратних засобів і технологій оцінювання і зменшення ризиків переходу ІКС і керованих промислових об'єктів у небезпечний стан.

Зв'язок роботи з науковими програмами, планами, темами. Тематика робіт, що спрямовані на розроблення методологічних засад, математичних моделей, методів, програмно-апаратних засобів і технологій оцінювання і забезпе-

чення функціональної безпеки критичних інформаційно-керуючих систем, включена в галузеві та державні програми досліджень і розробок, науково-технічні плани закладів вищої освіти Міністерства освіти і науки України (Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут», Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"), інститутів Національної Академії наук України (Інституту кібернетики імені В. М. Глушкова НАН України, Інституту проблем реєстрації інформації НАН України), Державного космічного агентства (Державного науково-виробничого підприємства «Об'єднання Комунар», НТСКБ «ПОЛІСВІТ», м. Харків), Публічного акціонерного товариства «Науково-виробниче підприємство «Радій», м. Кропивницький. Роботу виконано в рамках низки державних програм, держбюджетних і договірних науково-дослідних і дослідно-конструкторських робіт, міжнародних проектів і програм (UNTC, TEMPUS, ERASMUS+, FP7, H2020).

Наукова новизна роботи полягає в наступному. В результаті досліджень сформовано концептуальні засади побудови функціонально безпечних інформаційно-керуючих систем на підставі розвитку парадигми Фон-Неймана «надійних систем із ненадійних компонентів», узагальнення понять гарантоздатності та безпеки критичних ІКС. Сформульовано та впроваджено *концепцію* створення надійних, безпечних і гарантоздатних ІКС з використанням програмно-апаратних і мережних компонент з недостатньою надійністю та безпечністю в умовах ресурсних обмежень та невизначеності, яка базується на *принципах*:

- *багатоверсійності* при розробленні та впровадженні шляхом застосування різних (диверсних) програмно-апаратних версій – продуктів і процесів створення систем для зменшення ризиків фатальних відмов за загальною причиною;
- *багатопараметричної адаптації* до негативних подій та деструктивних чинників з урахуванням змін вимог до ІКС, параметрів середовища, компонентних, системних та інфраструктурних комунікацій і забезпечення здатності еволюціонування у реальному часі та резіл'єнтності;
- *багаторівневої керованої деградації* з поступовим зменшенням якості або множини виконуваних завдань внаслідок накопичення відмов, викликаних природними і екстремальними фізичними та інформаційними впливами, в межах безпечного функціонування.

На підставі сформульованих концепції та засад:

- створено нові та розвинуто математичні методи, програмно-апаратні засоби та технології оброблення інформації, забезпечення гарантоздатності та функціональної безпеки платформ, програмно-технічних комплексів критичних ІКС за наявності обмежень, притаманних вбудованим і розподіленим, необслуговуваним і обслуговуваним системам;
- розроблено математичні методи комбінаторного аналізу, геометричного моделювання (покриття і розміщення) для задач побудови і оптимізації структур інформаційно-керуючих і комунікаційних систем з глибоким багатоешелонованим резервуванням для зменшення ризиків небезпечних відмов, а також

створення систем екологічної безпеки та моніторингу аварій для критичних об'єктів з урахуванням просторових і природних характеристик;

- розвинуто теорію та запропоновано методи інсерційного моделювання як основи для формального представлення систем, методи верифікації, тестування та підтвердження на відповідність критичних ІКС вимогам міжнародних і національних стандартів з функціональної та кібербезпеки;
- розроблено принципи та методи інтелектуального комп'ютерного оброблення великих даних у системах дистанційного зондування, мультимедіа та телекомунікацій з урахуванням їх вбудованості у комплекси критичного використання різного призначення, системи екологічного, перед- і поставарійного моніторингу;
- розроблено принципи, методи побудови і аналізу комунікаційних систем ІКС і встановлення закономірностей зміни пропускної здатності від просторово-енергетичних параметрів каналів, забезпечення їх структурної надійності та безпеки у різних середовищах з динамічною зміною фізичних та інформаційних параметрів;
- розроблено принципи, критерії оцінювання та методи підвищення живучості інформаційно-керуючих систем і систем організаційного управління критичних інфраструктур; методи та інформаційні технології прийняття рішень щодо забезпечення функціональної безпеки та живучості на різних етапах життєвого циклу.

Наукове значення роботи полягає в наступному. Запропоновано цілісну науково обґрунтовану методологію безпечного комп'ютингу і комунікацій, принципи, моделі і методи побудови та реалізації гарантоздатних інформаційно-керуючих систем для критичних з точки зору функціональної безпеки галузей. На основі теоретичних досліджень і експериментів визначено класи критичних систем, причини і наслідки відмов, зумовлених дефектами програмно-апаратних і комунікаційних засобів, атаками на їх вразливості, різними видами збурення, принципи та технології аналізу та забезпечення функціональної безпеки та її складових відповідно до вимог національних і міжнародних стандартів. Створено наукові основи розроблення безпечних інформаційно-керуючих систем, аналізу, верифікації та забезпечення функціональної безпеки критичних ІКС та їх компонентів на різних етапах життєвого циклу.

Прикладне значення роботи полягає в розробці комплексу національних і галузевих стандартів для визначення вимог до функціональної безпеки, а також методів, програмно-апаратних засобів, інструментальних систем і технологій регулювання, оцінювання, проектування, верифікації, обслуговування та забезпечення функціональної безпеки та гарантоздатності критичних інформаційно-керуючих систем, розроблених і впроваджених в індустрії впродовж двох останніх десятиліть завдяки:

- багаторічній співпраці і безпосередній участі у розробленні, виготовленні, впровадженні та супроводі інформаційно-керуючих і комунікаційних систем підприємствами аерокосмічної, енергетичної та інших галузей;

- участі у роботі національних і міжнародних експертних груп зі створення нормативної бази критичних програмно-технічних комплексів і систем;
- виконанню міжнародних наукових проектів за замовленнями компаній Motorola, Intel, Samsung, міжнародними програмами STCU, TEMPUS, ERASMUS+, FP7, H2020 під науковим керівництвом і активній участі авторів;
- виконанню багатьох національних та галузевих проектів відповідно до планів науково-дослідних робіт НАН України, МОН України, інших міністерств і відомств, приватних компаній, які працюють у сфері створення критичного програмного забезпечення, систем безпеки і екологічного моніторингу.

Зміст роботи викладений у восьми розділах.

У першому розділі сформовано концепцію, методологічні основи гарантоздатних обчислень і принципи створення функціонально безпечних ІКС. Визначено еволюційні та змістовні передумови формування концепції гарантоздатності, яка має об'єднувати надійнісну та безпекові складові. Проаналізовано кризові складові розвитку теорії надійності, зумовлені впровадженням нових технологій програмного забезпечення, хмарних і IoT систем, програмовних платформ і компонент з розширеною номенклатурою причин, природи і наслідків відмов. Досліджено статистику відмов, які призвели до аварій ракетно-космічних та інших критичних систем, зроблено висновки про зростання впливу проектних дефектів і дефектів взаємодії із середовищем на виникнення фатальних відмов. Обґрунтовано напрями комплексного захисту таких систем від різних типів дефектів і відмов. Розроблено таксономію (сукупність причин відмов, інформаційно-технічних станів, механізмів толерування, первинних і вторинних властивостей), концепцію та загальні моделі гарантоздатних і резіл'єнтних обчислень, які інтегрують надійність, функціональну та інформаційну безпеку, живучість і здатність до еволюції при зміні вимог, середовища і виникненні неспецифікованих вимог.

Визначено сталу і динамічну складові еволюції критичних систем у контексті гарантоздатності та багатоверсійності. Перша полягає у суттєвих і поступових змінах технологій, які впливають на різні системи, друга – у змінах, які стосуються конкретної системи протягом її життєвого циклу. Відзначено, що стала складова еволюції технологій для гарантоздатних систем має цікаві прояви, які стосуються компонент COTS (комерційних компонент, Commercial-Of-The- Shelf) і CrOTS (критичних компонент, Critical-Of-The-Shelf) і реалізації принципу диверсності у критичних застосуваннях. Для COTS і CrOTS досліджено закономірність, яку названо «колообігом компонент», пов'язану з систематизацією особливостей і обмежень та процедурами, необхідними для використання комерційних компонент (програмних продуктів і апаратних засобів), та використання критичних IT-компонент для комерційних застосувань. Для другого випадку визначено клас динамічно еволюціонуючих гарантоздатних систем (самоеволюціонуючих систем реального часу, які здатні ураховувати зміни вимог і характеристик середовища та використовують власні або зовнішні ресурси за визначеними правилами).

Розроблено моделі операційних циклів забезпечення гарантоздатності, функціональної безпеки та резил'єнтності. Узагальнено підхід до формування операційного циклу відмовостійкості для різних типів дефектів і рівнів ієрархії, на яких забезпечується стійкість до різних типів дефектів. Аналогічний операційний цикл сформовано для урахування змін вимог і середовища. Запропоновано і удосконалено таксономію, принципи багатоверсійних обчислень і методів оцінювання диверсності, зроблено висновок про необхідність їх комплексного застосування, тобто розроблення технології «багатоверсійної» оцінки багатоверсійності. Визначено поняття версійної надмірності, багатоверсійних процесів, продуктів і проектів у контексті розроблення критичних ІКС для різних галузей. Запропоновано модель «куба диверсності» як узагальненого простору рішень для створення функціонально безпечних систем. На базі куба багатоверсійності розроблено двовимірні матриці проектних рішень для різних рівнів (концептуального, системного, програмного, апаратного) та етапів життєвого циклу системи. Досліджено закономірності еволюції самих багатоверсійних систем і технологій на прикладі розвитку та реалізації принципу диверсності в інформаційно-керуючих системах АЕС (зокрема, систем аварійного захисту), які описуються законом «заперечення заперечення». Узагальнено парадигму «гарантоздатних/безпечних систем із негарантоздатних/недостатньо безпечних компонент» з використанням різних видів багатоверсійності.

Другий розділ надає стислий огляд розроблених методів та технологій забезпечення якості процесів і продуктів при створенні інформаційно-керуючих систем, важливих для безпеки, кейс-орієнтованих методів та засобів оцінювання відповідності програмного забезпечення, апаратно-програмних і програмовних платформ та ІКС у цілому вимогам національних і міжнародних стандартів до надійності та функціональної безпеки на різних етапах життєвого циклу. Узагальнено V-моделі життєвого циклу для функціонально та інформаційно безпечних систем для АЕС, які розробляються відповідно до цих моделей. Запропоновано методи проведення валідаційних випробувань ІКС при їх впровадженні та модернізації. Запропоновано методи оцінювання готовності та функціональної безпеки ІКС з урахуванням змінних параметрів потоків відмов, зумовлених проектними дефектами програмних засобів і атаками на вразливості з можливістю їх патчеризації, які базуються на багатофрагментних марковських моделях. Запропоновано методи вибору інструментальних засобів і параметрів їх налаштування для чисельного вирішення систем диференціальних рівнянь Колмогорова-Чепмена, які забезпечують мінімізацію ризиків неточних і нестабільних рішень внаслідок великої жорсткості і розрідженості матриць коефіцієнтів. Розроблено та досліджено моделі й методи систем з версійно-інформаційною та версійно-структурною надмірністю, іншими варіантами комбінованої надмірності, використання яких надає можливість мінімізувати ризики відмов за загальною причиною. Проаналізовано автоматні моделі таких систем різних класів, визначено їх властивості. У рамках реалізації принципу багатопараметричної адаптації запропоновано комплекс методів із різними видами адаптації: порогової, ярусної, версійної та їх комбінацій, які використовують залежно від вихідних і поточних значень параметрів. Для систем на програмній логіці розробле-

но методи структурно-просторової адаптації, які ураховують розташування дефектних і працездатних логічних комірок на кристалі, і забезпечують можливість завантаження найкращого за показниками надійності варіанта відмовостійкої структури.

Третій розділ присвячено опису методів і засобів інтелектуальної обробки великих даних у безпечних системах дистанційного зондування (ДЗ), мультимедіа та комунікацій, що використовуються для моніторингу критичних об'єктів і територій та вбудовуються в інформаційно-керуючі системи та інфраструктури екологічної безпеки. Для успішного використання таких даних розроблено інтелектуальні методи ефективної обробки та зберігання з урахуванням високої розрізнювальної здатності та великої кількості каналів. Запропоновано методи оброблення даних на борту носія або у центрі оброблення інформації з наступною передачею їх користувачам. При цьому забезпечується адаптація методів й алгоритмів до властивостей сигнальної та завадової складових, що можуть змінюватися, а також стійкість обробки до різних чинників і похибок вимірювань параметрів і здатність приймати рішення про доцільність застосування різних етапів оброблення.

Розроблено методи, які дозволяють визначати: корельованість або некорельованість завад; їх просторовий спектр, статистичні характеристики адитивних або сигнально-залежних завад. Отримані результати мають суттєве значення для прогнозування ефективності фільтрації, прийняття рішення щодо доцільності застосування фільтрації, для вибору методу фільтрації та встановлення параметрів фільтра. Запропоновано шляхи підвищення точності прогнозування, що включають вибір найбільш інформативних вхідних параметрів, спільне використання двох чи більшої кількості параметрів, застосування нейромереж або машин опорних векторів. Показано, що характеристики завад доцільно враховувати під час стиснення зображень із втратами. Розроблено алгоритми варіаційно-стабілізуючого перетворення для гіперспектральних даних ДЗ, які дозволяють досягати стиснення в околі оптимальної робочої точки для групи каналів (зон). Доведено, що використання тривимірних кодерів дозволяє суттєво покращити показники стиснення. Запропоновано алгоритми прогнозування рівня втрат згідно з різними критеріями. Показано, що точність прогнозування можна підвищити за рахунок машин опорних векторів і використання кількох вхідних параметрів. Розроблено методи і алгоритми стиснення із втратами попередньо фільтрованих зображень. Комплекс запропонованих операцій попереднього оброблення забезпечує надійну класифікацію даних багатоканального ДЗ з високим рівнем завад у вхідних зображеннях, виявленню ділянок, що можуть бути забрудненими, детектуванню змін у сценах, що можуть бути наслідками критичних явищ і аварій.

У четвертому розділі описано методи та засоби забезпечення пропускної здатності та безпеки підсистем ІКС, а саме інфокомунікаційних систем, які працюють в умовах динамічного середовища. На основі аналізу призначення, існуючої класифікації та досвіду застосування сучасних інфокомунікаційних систем запропоновано нові ефективні рішення щодо побудови функціонально безпечних підсистем управління для інтелектуальних мереж зв'язку. Основні

переваги полягають в адаптації архітектури, що надає можливість оптимізації параметрів передачі даних із заданою якістю. Завдяки цьому автоматизується процес керування умовах динамічного середовища та впливу різних деструктивних чинників.

Запропоновані рішення базуються на цифровізації інформаційної інфраструктури та використанні пакетних засобів передавання інформації. Для визначальних показників – пропускної здатності та продуктивності дискретного каналу зв'язку розроблено аналітичні методи розрахунку. Розвинуто концепцію прийняття рішення щодо використання сигнально-кодових конструкцій за ознакою типу модуляції та завадостійкого кодування для підвищення безпеки і гарантоздатності. Проаналізовано якість зв'язку в безпровідному каналі, що створено на основі найновішого стандарту 802.11ac, призначеного для розроблення і застосування безпечних засобів зв'язку для ІКМС в умовах динамічного середовища. Ефективність зв'язку в створеному безпровідному каналі оцінено на основі результатів, отриманих теоретично, в лабораторії та в ході натурних випробувань. Показано, що застосування запропонованих рішень в абонентських радіостанціях забезпечує суттєве підвищення структурної надійності мережі, її живучості та безпеки, зокрема, показника ефективності (ймовірності своєчасної передачі повідомлень з необхідною достовірністю) 35% порівняно з неавтоматизованою системою зв'язку.

В п'ятому розділі в рамках теорії живучості комп'ютерних та інформаційно-керуючих систем сформульовано поняття, показники та критерії функціональної, структурної та інформаційної живучості як складової загальної гарантоздатності. Визначено складність досліджень, яка зумовлена, перш за все, збільшенням кількості варіантів функціональної поведінки системи залежно від зовнішнього середовища. Проведено комп'ютерне моделювання з урахуванням надвеликою кількістю можливих станів зовнішнього середовища під час функціонування системи, семантичної різноманітності вихідної структурованої чи неструктурованої інформації, яка потребує опрацювання засобами ІКС, багатоваріантності функцій опрацювання інформації, та неможливості побудови вичерпного критерію оцінювання якості функціонування таких систем.

На функціональному рівні запропоновано аналітичні та імітаційні моделі систем, виокремлено стани живучості системи, побудовано оцінки і показники функціональної живучості. На структурному рівні у рамках графових і мережевих моделей визначено критерії та оцінки структурної живучості, необхідні для розв'язання прикладних задач. Досліджено можливості сучасних комунікаційних технологій щодо підтримки необхідних структур мобільних об'єктів, які мають спільну «колективну» мету. На інформаційному рівні досліджено можливості систем захисту і показано недостатність їх для гарантування безпеки функціонування критичних інформаційно-керуючих систем, оскільки ці системи мають не лише техніко-технологічну, а й соціальну складову, що активно взаємодіє із зовнішнім середовищем.

Теоретично обґрунтовано і підтверджено на практиці, що впровадження спеціальних механізмів забезпечення живучості, зокрема, механізмів розпізнавання, компенсації, відновлення, адаптації, реконструкції, реконфігурації та ре-

організації, які не дозволять системі раптово припинити функціонування і спрямовані на збереження функціональності системи, поступову деградацію і безпечну зупинку, підвищує функціональну безпеку критичних інформаційно-керуючих систем. Запропоновано для відпрацювання базових системних, конструкторських, програмних і технологічних рішень щодо впровадження тих чи інших механізмів забезпечення живучості інформаційно-керуючих систем на етапі їх розроблення використовувати спеціалізовані комп'ютерні моделюючі комплекси, засоби яких дозволяють вивчати й удосконалювати технологічні процеси на об'єктах критичної інфраструктури, процеси управління ними, раціоналізувати організаційну структуру об'єкта управління, прискорити процеси взаємодії, покращити показники якості функціонування.

Шостий розділ присвячено розробленню конструктивних засобів математичного і комп'ютерного моделювання критичних систем засобами геометричного проектування. Показано та обґрунтовано, що при проектуванні широкого класу систем моніторингу, діагностування та контролю доцільно здійснювати перетворення інформації про різні за своєю природою об'єкти в єдиний вид геометричної інформації. Запропоновано спеціальний математичний апарат, що дозволяє враховувати як реальні геометричні особливості елементів систем (їх тип, кількість, форму, розміри, параметри розміщення), так і властивості перетворення фізичної інформації в геометричну. Математичні моделі та методи їх розв'язання стали основою створення інтелектуальних інформаційно-аналітичних систем геометричного проектування, розрахунку показників підсистем контролю стану небезпечних об'єктів, розташованих у різних місцях. Їх математичне забезпечення базується на моделях і методах розв'язання задач розміщення та покриття геометричних об'єктів, а також оригінальних методах комбінаторної оптимізації, що враховують властивості критичних ІКС.

Для побудови спеціальних класів математичних моделей задач моніторингу стану критичних об'єктів, створення та супроводу систем спостереження та контролю здійснено перетворення інформації, що описує фізичні процеси та об'єкти, в геометричну, у зв'язку з чим формалізовано поняття геометричної інформації, пов'язаної з матеріальними об'єктами або їх сукупністю. Формалізація задач розміщення та покриття базується на теорії конфігураційних просторів, розроблення якої дозволила досліджувати об'єкти, що мають довільну просторову форму, метричні характеристики та відповідне взаємне розташування з урахуванням технологічних обмежень критичних ІКС.

Досліджено нові комбінаторні моделі задач синтезу дискретних структур. На основі відображення комбінаторних множин у евклідовий простір розроблено теоретичні засади побудови нового класу задач дискретної оптимізації – задач евклідової комбінаторної оптимізації, які застосовують при пошуку надійних і безпечних конфігурацій критичних ІКС. Отримано фундаментальні результати в напряму теорії глобальної оптимізації, що дозволило гарантувати оптимальні рішення для побудови та модернізації підсистем контролю небезпечних станів критичних ІКС.

У сьомому розділі наведено технологію використання формальних методів розроблення програмного та апаратного забезпечення критичних ІКС, яке

інтегрується у стандартний процес у вигляді верифікації та валідації властивостей функціональної та кібербезпеки на кожному етапі життєвого циклу. Для кожного етапу створено сукупність методів, що дозволяє підвищити якість та ефективність розробки, уникнути критичних помилок на подальших етапах, таких як інтеграція або валідація. На етапі формування і аналізу вимог верифікуються класичні властивості несуперечливості і повноти вимог, безпеки та життєздатності, локальні властивості (інваріанти, контракти) та властивості, що визначають відповідність вимогам, властивості, специфічні для певних класів систем, а саме, такі як конкуруючі процеси, взаємне виключення, когерентність станів, динамічне взаємне блокування. На етапах проектування та кодування для артефактів етапів (модель дизайну або код), запропоновано процедуру верифікації властивостей моделі, перш за все, властивостей безпеки.

Розроблено методи модельного тестування на основі технік інсерційного моделювання та символьного виконання, методи генерування тестів із заданим критерієм покриття, методи символьного виконання тестів на основі технік «чорної» та «білої» скриньки, методи інтеграційного та регресивного тестування, що суттєво підвищують ефективність процесу тестування з точки зору критерію покриття. Методи реалізовано в системах алгебраїчного програмування, інсерційного моделювання, що дозволили сформувати алгоритмічну основу системи верифікації та тестування вимог VRS, системи модельного тестування GTG, системи ре-інжинірингу Uniquesoft, алгебраїчної платформи garuda.ai, які використовувалися в телекомунікаційних областях, автопромисловості, верифікації мережних протоколів, мікропроцесорній індустрії. Важливо, що це дало можливість використання інженерних специфікацій в рамках мови алгебри поведінок та як наслідок - розширити використання формального підходу та методів верифікації програмного забезпечення критичних ІКС.

У восьмому розділі систематизовано результати впровадження наукових положень роботи. Дано перелік найважливіших НДР і НДДКР, у рамках яких отримано основні результати досліджень та розробок, що виконувались за замовленням Міністерств освіти і науки, оборони, енергетики України, Національної Академії наук України, індустріальних підприємств і приватних організацій, замовників з Аргентини, Болгарії, Бразилії, Канади, Китаю, Мексики, Франції, інших країн, міжнародних програм і фондів.

Показано, що результати всебічно впроваджено в окремих пристроях, програмному забезпеченні, інформаційно-керуючих системах різних галузей, насамперед атомної енергетики, космічних комплексів, авіації, медицини, а також державного будівництва, освіти, мультимедіа, телекомунікацій. Серед підприємств, де результати досліджень і розробок знайшли впровадження, відзначимо НВП «Радій», НВП «Радікс», АЕС України, Козлодуйська АЕС Болгарії, дослідницькі реактори Інституту ядерної енергії НАН України, Аргентини і Бразилії, ДП «Івченко-Прогрес» та АТ «Мотор Січ», «Хартрон-Аркос», ПАТ НПО «ЕЛМІЗ», ПАТ «НВП Сатурн» та інші. Розробки використано в рамках міжнародного космічного проекту МКС за участю NASA, ESA, JAXA та інших. Описано переваги й позитивні наслідки впроваджень.

Результати використано при створенні Концепції інформаційної безпеки України (1998р.), Концепції державної інформаційної політики України (2001р.), Концепції створення системи забезпечення інформаційної безпеки ДПС України (2002р.), Концепції інформаційної політики з питань євроатлантичної інтеграції України (2004р.), Концепції розвитку інформаційного суспільства в Україні (2005), Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій. Наведено огляд впроваджень у медицині та навчальному процесі провідних університетів України.

Світовий рівень результатів підтверджується: публікацією авторами роботи наукових статей за напрямами досліджень у міжнародних англомовних профільних журналах з високими рейтингами, а також великою кількістю посилань на них фахівцями понад 50 країн; виданням серії монографій, науковими редакторами та співавторами яких є автори роботи, у провідних світових наукових видавництвах Springer (Великобританія, ФРН), River Publishers (Данія), IGI Global (США), які індексовано науково-метричними базами Web of Science Scopus; запрошенням авторів роботи на міжнародні конференції та семінари у Болгарії, Великобританії, Естонії, Італії, Польщі, Словаччини, США, Швеції та інших країн як пленарних доповідачів і лекторів. Результати наукових досліджень, рівень їх впровадження перевершує світові аналоги за показниками функціональної безпеки (імовірності/ризики небезпечних відмов і відмов за загальною причиною), гарантоздатності, відносних витрат на забезпечення відмово- та атакостійкості, завадостійкості та пропускної здатності і т. ін.

Результати досліджень і розробок впроваджено у понад 20 провідних високотехнологічних підприємствах України, що дозволило підвищити функціональну безпеку, надійність і зменшити витрати на реалізацію процесів життєвого циклу програмно-технічних комплексів, інформаційно-керуючих і комунікаційних систем у різних критичних галузях (атомна і теплова енергетика, авіаційні системи та ракетно-космічні комплекси, медичні системи, тощо). Дослідження проводилися в рамках міжнародного співробітництва та виконання спільних проектів у США, Канаді, Фінляндії, Мексиці, КНР, Аргентині, Болгарії, Південній Кореї та інших країнах. Економічний ефект від впровадження полягає у зменшенні потенційних витрат на відновлення критичних об'єктів внаслідок небезпечних відмов та аварійних ситуацій, а також витрат на створення та забезпечення функціональної інформаційно-керуючих систем шляхом розроблення та впровадження методів і технологій оптимізації структур і характеристик програмно-технічних комплексів та стратегій застосування і обслуговування критичних ІКС.

Кількість публікацій: 60 монографій (з них 30 – у зарубіжних виданнях), 9 підручників, 19 навчальних посібників, 240 статей (з них 150 – у зарубіжних виданнях). Загальна кількість посилань на публікації авторів / h-індекс роботи згідно з базами даних становить відповідно: Scopus – 2216/27; Web of Science 780/16; Google Scholar – 5295/38. Отримано 41 патент на винахід, понад 500 патентів на корисну модель та авторських свідоцтв на твір, розроблено 7 галузевих стандартів. За даною тематикою захищено 11 докторських і 71 кандидатських дисертацій.