УДК 681.3: 004.415.5

В.С. Харченко

Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»

ГАРАНТОЗДАТНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ: ПРОБЛЕМИ І РЕЗУЛЬТАТИ

Аналізуються проблеми гарантоздатності комп'ютерних систем, пов'язані із комплексним забезпеченням надійності та безпечності (аварійної – safety та інформаційної – security). Надається огляд основних задач, теоретичних і практичних результатів, отриманих науковцями кафедри комп'ютерних систем і мереж Національного аерокосмічного університету «ХАІ», напрямків подальших досліджень.

комп'ютерні системи та мережі, критичні застосування, гарантоздатність, надійність, безпечність, багатоверсійні технології, багатопараметрична адаптація, багатоступенева деградація, верифікація

Вступ

Надійність та безпека авіаційних, космічних комплексів, АЕС, інших комплексів критичного використання (ККВ) залежить від надійності комп'ютерних інформаційно-управляючих систем (КІС) та їх компонент – програмних, апаратних, мережних, а також стійкості до дії факторів зовнішнього середовища. Надійність КІС ККВ повинна розглядатися у більш широкому контексті як комплексна властивість, що включає не тільки традиційні складові, перед усім, безвідмовність і готовність, але й безпечність (інформаційну та аварійну). За міжнародною практикою така властивість має назву "dependability" (на відміну від "reliability"), якій у найбільшій мірі відповідає україномовний варіант "гарантоздатність" (надійність у широкому сенсі).

Проблеми забезпечення найбільш суттєвих складових гарантоздатності КІС – безвідмовності (або готовності), відмовостійкості та інформаційної безпеки у більшості наукових досліджень і розробок розглядалися різними (у першу чергу, вітчизняними) фахівцями окремо, хоча ці та інші власти-

вості, безперечно, взаємопов'язані і впливають одна на одну. Це підтверджують публікації останніх років у провідних міжнародних журналах, технічних звітах наукових центрів та університетів, працях конференцій щодо проблеми гарантоздатності [1]. Зважаючи на тісний зв'язок означених складових для КІС, їх визначальний вплив на надійність і безпеку ККВ в цілому та певну обмеженість результатів досліджень з цього питання, *актуальними* є розробка основ теорії гарантоздатних систем, комплексних методів забезпечення гарантоздатності КІС. Ураховуючи статус КІС ККВ (та їх програмного забезпечення) як важливого об'єкту нормативного регулювання, *актуальною* є також розробка інструментальних методів достовірної оцінки (експертизи та верифікації) їх відповідності регулюючим вимогам.

В статті надається аналіз основних проблем в цій галузі, проводиться стислий опис теоретичних і практичних результатів, отриманих науковцями кафедри комп'ютерних систем і мереж Національного аерокосмічного університету «ХАІ» за останні роки, характеризується їх рівень, визначаються напрямки подальших досліджень.

1. Стан проблеми гарантоздатності

В Україні, провідних країнах Європи, США, Китаї, Японії та Росії проводяться інтенсивні наукові дослідження, практичні розробки та накопичено значний досвід використання комп'ютерних інформаційно-управляючих систем для авіаційних та ракетно-космічних комплексів Це стосується також КІС, важливих для безпеки АЕС, залізничного транспорту, інших ККВ. *Факти* засвідчують, *по-перше*, про зростання кількості інцидентів, аварій ККВ, обумовлених відмовами програмних, апаратних і мережних компонент КІС, що викликано обмеженою безвідмовністю, готовністю, безпечністю компонент, інтенсифікацією зовнішніх впливів активного та пасивного характеру на працездатність, складністю та унікальністю проектів КІС, недосконалістю технологій їх розробки, верифікації та експертизи; *по-друге*, про динамічний розвиток окремих складових теорії та інформаційних технологій створення відмовостійких комп'ютерних

систем, які забезпечують конкурентноздатне середовище як для критичних, так і для комерційних застосувань.

Беручи до уваги їх велику відповідальність, статистику інцидентів, аварій та катастроф, спричинених у майже у кожному п'ятому випадку відмовами КІС, зростання інтенсивності впливу пасивних і активних факторів зовнішнього середовища, фахівцями науково-технічних центрів LAAS (Франція), SRC та CSR (Великобританія), відомих фірм Siemens (ФРН), Schneider Electric (Франція), Boing, Westinghouse (США) та інш. інтенсифікуються дослідження і розробки, спрямовані на розробку нових технологій створення відмовостійких апаратних, програмних, мережних компонент і КІС в цілому. Для регулювання питань забезпечення надійності та безпеки цих систем розроблені стандарти Європейським космічним агентством, Європейською кооперацією з стандартизації у космічній галузі, IAC, ISO, IEC, IAEA та інш. щодо вимог до таких систем та їх компонент.

Слід зазначити, що аналогічні задачі мають місце і для бізнес-критичних застосувань, зокрема, банківських та інших комерційних систем з великим обігом коштів, що функціонують в умовах жорсткого конкурентного середовища та впливів через мережу Інтернет. Забезпечення гарантоздатності бізнес-критичних КІС – задача, яка інтенсивно вирішується науковцями та інженерами-розробниками та користувачами таких систем.

У останні роки дослідження та розробки щодо надійності та безпеки КІС набувають більш комплексного характеру. Це підтверджується розробкою концепції Dependable Computing (Systems, Networks) – DSN, що базується на розширеному понятті надійності – гарантоздатності, яка включає безвідмовність (reliability), готовність (availability), пристосованість до обслуговування або ремонтопридатність (maintainability) та безпеку, як інформаційну (security) та її складові – конфіденціальність (confidentiality) і цілісність (integrity), так і аварійну безпеку (safety).

У роботах відомих спеціалістів А.Авіженіса, Ж.-К.Лапрі, Б.Рендела, що представляють відповідно американські, французькі та англійські наукові центри у цій предметній галузі, властивість гарантоздатності та її складові визначаються через поняття послуг (сервісів - services), що надаються системою [1]. Ця робота підсумовує двадцятирічний шлях формування

базових понять, що почався з редакційної статті А.Авіженіса, Ж.-К.Лапрі у спецвипуску корпорації IEEE, який був перекладений на російську мову у 1986 році [2]. Перші роботи в російськомовній літературі, де використовувався термін у тому ж сенсі були опубліковані у [3, 4], але не знайшли подальшого розвитку, у першу чергу, через деякий термінологічний консерватизм серед спеціалістів з надійності, а також внаслідок певного відторгнення можливості комплексування питань щодо забезпечення безвідмовності (відмовостійкості) апаратних і програмних засобів у єдиній системі.

Гарантоздатність у [1] визначається як властивість системи надавати заплановані (коректні) послуги; безвідмовність – здатність надавати їх *безперервно*, готовність – властивість знаходитися у стані, коли такі послуги *можуть бути надані*, обслуговуваність – пристосованість до *відновлення* надання послуг після відмов, конфіденціальність – захищеність від *несанкціонованого доступу* до інформації, цілісність – властивість зберігати інформацію без *несанкціонованих перекручень* при наданні послуг, безпека (safety) - властивість не створювати *небезпеку для середовища* (людей, навколишнього середовища, інших систем) при наданні послуг.

При цьому відмовостійкість (fault-tolerance) – здатність автоматично, за обмежений час прогнозувати, попереджувати, парирувати та відновлювати працездатність після відмов) – визначається як засіб або механізм підтримки усіх складових гарантоздатності, а не як окрема її складова. Такий підхід до відмовостійкості має рацію, оскільки забезпечення певного рівня усіх складових гарантоздатності в умовах розширення множини причин, що можуть викликати відмову (тобто ненадання послуг), потребує реалізації відповідних засобів відмовостійкості.

Системи або процеси (наприклад, обчислення), які мають таку комплексну властивість, можуть називатися гарантоздатними. Питання розробки та використання гарантоздатних систем обговорюються на спеціалізованих національних і міжнародних форумах і конференціях (DSN, SAFECOM, ESREL, PSAM та інш.) вже більш 20 років. З 2004 року всесвітньо відомою науково-технічною корпорацією IEEE, яка відслідковує найбільш важливі тенденції у інформаційних технологіях видається журнал “Dependable and Security Computing”. Означені напрямки науково-

технічних розробок щодо створення гарантоздатних комп'ютерних систем і мереж підтримуються оборонними департаментами США, НАТО і поширюються у бізнес-критичних застосуваннях, а саме е-комерції (Dependable e-services, Internet-commerce) і банківських технологіях високої, продовженої та гарантованої готовності (High, Continuous, Dependable Availability Technologies) [5, 6].

Протягом кількох десятиріч розробка надійних комп'ютерних систем управління для аерокосмічної та інших критичних галузей проводилась підприємствами України, зокрема, такими науково-виробничими об'єднаннями і конструкторськими бюро Харкова як Хартрон, Комунар, НДІРВ, Авіаконтроль та інш. Наукові дослідження і розробки, що підтримували ці проекти, здійснювались спеціалістами кафедри комп'ютерних систем і мереж, інших кафедр Національного аерокосмічного університету «ХАІ».

За останні роки кафедрою комп'ютерних систем і мереж ХАІ разом з спеціалістами НТСКБ «Полісвіт», ЗАТ «Радій», організацій та підприємств Державного комітету ядерного регулювання України – НТЦ ядерної та радіаційної безпеки, Сертцентру АСУ та інш. проведені розробки проектів КІС для авіаційної техніки та АЕС, галузевих стандартів для Національного космічного агентства України, атомної енергетики, методик проектування та верифікації відмовостійких систем на програмованих інтегральних схемах над великої інтеграції (ПЛІС), а також інструментальних засобів оцінки критичного програмного забезпечення. Але аналіз вітчизняних та закордонних публікацій показує, що розвиток комп'ютерної та програмної інженерії, пов'язані з їх впровадженням ризики для ККВ, жорсткі умови зовнішнього середовища, зростаючі вимоги до надійності, живучості та безпечності (тобто гарантоздатності взагалі), *актуалізують вирішення комплексної проблеми аналізу та синтезу гарантоздатних систем, розробки методів та інструментальних засобів оцінки та забезпечення складових гарантоздатності КІС ККВ.*

Це обумовлено тим, що більшість розробок з цього питання вирішують *окремі задачі* як для *властивостей* КІС (складових гарантоздатності), так і для *їх компонент* (програмних, апаратних, мережних) і *процесів* життєво-

го циклу, включаючи незалежну *верифікацію та експертизу*, що є обов'язковими для критичних застосувань.

2. Мета та етапи досліджень

Мета досліджень, які проводились і проводяться на кафедрі комп'ютерних систем і мереж з розглянутої проблеми, є розробка *теоретичних основ* оцінки та забезпечення, гарантоздатності комп'ютерних систем обробки інформації, управління та контролю критичного застосування, *методів, інструментальних засобів та технологій* проектування, моделювання, оцінки, верифікації та експертизи гарантоздатних аерокосмічних комп'ютерних систем, АЕС, інших систем критичного та бізнес-критичного застосування з урахуванням обмежень, які пов'язані з особливостями їх призначення та побудови (бортових і наземних, відновлюваних і невідновлюваних, розподілених і зосереджених, вбудованих і мобільних), а також факторів зовнішнього середовища (активного або пасивного).

Дослідження проводяться за трьома напрямками, у три етапи.

Перший етап – теоретичні дослідження, спрямовані на створення науково-методичних засад гарантоздатних КІС, загальних методів їх аналізу та синтезу. Необхідність таких досліджень пов'язана з необхідністю формування системних моделей гарантоздатних КІС, комплексних показників їх оцінки, формулювання та вирішення оптимізаційних задач їх створення та реінжинірінгу. *Другий етап* – комплексні дослідження щодо розробки методів оцінки (моделювання, верифікації експертизи) та забезпечення гарантоздатності та її складових апаратних, програмних і мережних компонент КІС. *Третій етап* – дослідження та практичні розробки, пов'язані зі створенням інструментальних засобів та інформаційних технологій підтримки прийняття рішень на різних етапах життєвого циклу КІС ККВ з урахуванням вимог до надійності та безпеки (гарантоздатності).

3. Базові ідеї та принципи

Базові ідеї досліджень фундуються на парадигмі побудови *гарантоздатних систем із негарантоздатних компонент* (dependable systems out of undependable components – DSoUC). Вона була сформульована у роботах

кафедри [7, 8] у контексті еволюційного аналізу розвитку проблеми надійності (гарантоздатності) комп'ютерних систем, починаючи з базової праці Джона фон-Неймана [9], де були розроблені принципи побудови "надійних організмів із ненадійних компонент". Парадигма DSoUC була розвинута та частково реалізована стосовно створення гарантоздатних web-систем та систем захисту інформації науковцями кафедри при виконанні проекту "On Developing a General Approach to Analysis and Synthesis of Multiversion Software Systems and Applying it in Emerging Application Domains" за грантом Британського Королівського наукового товариства RS № 16114, 2003-2004рр. та дослідженнях що проводяться разом з спеціалістами університетів Ньюкасла та Лондона [10 – 12]. Вона реалізується через такі принципи.

1. Комплексний аналіз та урахування усіх можливих внутрішніх і зовнішніх факторів, що впливають на гарантоздатність КІС ККВ, а саме:

– *відмов апаратних засобів*, що виникають внаслідок процесів старіння, пасивних та активних екстремальних впливів середовища – космічного простору, сейсміки та ін.;

– *відмов програмних компонент* через дефекти, що вносяться при розробці, не виявляються при тестуванні та проявляються при використанні, а також через інші аномалії;

– активних і пасивних *інформаційних втручань* різного характеру – вірусів, закладок, спаму, цілеспрямованих та випадкових атак та ін.;

– *відмов внаслідок помилок обслуговуючого персоналу* систем.

2. Визначення системних зв'язків між складовими гарантоздатності КІС. Проведений аналіз показує, що вони знаходяться у складних суперечливих відносинах, оскільки підсилення однієї складової може призвести до зменшення показників іншої [10]. Наприклад, це стосується пари "готовність – безпечність (security)", оскільки підвищення інформаційної захищеності КІС, з одного боку, підвищує готовність до надання послуг внаслідок зменшення імовірності відмов при зовнішніх втручаннях, з іншого, - зменшує її через необхідність періодичного проведення моніторингу та обновлення системи захисту, що потребує додаткових непродуктивних витрат часу.

3. Впровадження технологій її забезпечення на базі принципів, об'єднаних концепцією "ЗБ" [13]:

– *багатоверсійності*, тобто створення резервованих систем, в яких резервні канали реалізують різні за математичними моделями, архітектурою, програмно-апаратними засобами, але адекватні за функціями, що виконуються, версії. Системи, в яких реалізується цей принцип, називаються багатоверсійними системами, а технології створення (розробки, виробництва, випробувань) та застосування за призначенням, в яких застосовують різні види диверсності (версійної надмірності) процесів та продуктів, – багатоверсійними технологіями. Принцип N-версійного програмування для зменшення рівня залишкових дефектів у програмному забезпеченні та надання йому у такий спосіб відмовостійкості було запропоновано у [14]. Далі він був поширений у принцип проектного різновиду і зафіксований у нормативних національних і міжнародних нормативних документах щодо вимог до систем безпеки АЕС. Основи теорії багатоверсійних систем та методи їх розробки надані в монографіях [15, 16];

– *багатопараметричної адаптації*, що базується на методах управління динамічною реконфігурацією архітектури системи за кількома параметрами залежно від кількості, виду відмов апаратних та програмних компонент, режимів функціонування та наявності ресурсів для відновлення працездатності. Прикладами такої адаптації є версійно-структурна (версійно-порогова), ярусно-порогова, структурно-просторова та інші види адаптації [15, 17-19], які надають можливість змінювати поріг спрацьовування відновлювальних органів, кількість версій, що реалізуються, ярусну та логічну структуру систем залежно від номенклатури відмов та умов функціонування і таким чином підвищувати безвідмовність та інші складові гарантоздатності;

– *багатоступеневої керованої деградації та відновлення*. Цей принцип реалізується у системах, що припускають можливість зниження якості функціонування при накопиченні одно- та багатократних відмов внаслідок внутрішніх та зовнішніх екстремальних факторів. Він полягає у динамічному перерозподілі ресурсів системи для мінімізації рівня деградації при відмовах компонент, що дозволяє максимізувати показники живучості при певних обмеженнях. У [20, 21] розроблені математичні моделі, методи та

програмно-технічні засоби реалізації багатоступеневої керованої деградації та відновлення.

Таким чином, означені принципи надали змогу сформулювати та перевірити *наукову гіпотезу* щодо можливості побудови гарантоздатних (надійних і безпечних) систем з програмних, апаратних, мережних компонент і підсистем з обмеженою надійністю та безпечністю шляхом використання процесно-продуктної диверсності при розробці, моделюванні та оцінці (верифікації та експертизі), багатопараметричної адаптації архітектурних параметрів до кількості і номенклатури відмов і динаміки зовнішнього середовища та мінімізації (керування) деградації за рахунок перерозподілу системних ресурсів та гнучких стратегій відновлення. Ця гіпотеза знайшла своє певне підтвердження на попередніх етапах досліджень та розробок і дозволяє обґрунтувати їх подальші напрями.

4. Основні наукові результати

1. Проведено аналіз впливу надійності комп'ютерних систем та їх компонент на безпеку ракетно-космічних комплексів. На підставі аналізу причин аварій та катастроф ракетно-космічної техніки за останні 40 років створена база даних і визначені головні ризики, пов'язані з використанням комп'ютерних технологій у цій галузі. Показано, що кожний сотий пуск закінчується аварією внаслідок дефектів програмного забезпечення, а кожна п'ята аварія викликана відмовою комп'ютерних систем управління [22, 23].

2. Запропоновані принципи еволюційного такого аналізу проблеми надійності КІС у системі координат "властивості компонент – властивості систем" [7]. Проведений аналіз розвитку принципів методів і засобів побудови надійних систем із ненадійних елементів на основі фон-неймановської парадигми та її модифікацій (дефектостійких систем з дефектних апаратних та програмних компонент, безпечних систем із небезпечних елементів та інш). Обгрунтовано і сформульовано її сучасне представлення щодо комп'ютерних систем як парадигми гарантоздатних систем із негарантоздатних компонент. Проведене її пророблення для web-систем. Запропоновані гарантоздатні (надійні, безпечні, відмовостійкі) архітектури web-сервісів та проведено їх моделювання з урахуванням типів

відмов web-компонент [24].

3. Проведено класифікацію та аналіз видів процесної та продуктної диверсності при створенні КІС для критичних застосувань. Запропоновані багатоверсійні технології проектування програмного забезпечення, що базуються на моделі життєвого циклу багатоверсійного ПЗ, метриках диверсності та моделях генерації розповсюдження появу та усунення дефектів. Досліджені моделі багатоверсійних систем з урахуванням значень метрик диверсності [25, 26]. Розроблені інструментальні засоби імітаційного моделювання та підтримки розробки багатоверсійного ПЗ [27].

4. Розроблено графо-подійні моделі одно- та багатоверсійних систем аварійного захисту АЕС та досліджено вплив відносних, групових і абсолютних дефектів програмного забезпечення на їх надійність та безпеку. Запропоновано комплексний метод оцінки надійності та верифікації багатоверсійних ІУС важливого для безпеки АЕС [28]. Розроблені елементи теорії багатоверсійних цифрових автоматів (БЦА), що мають підвищені властивості самоперевірки та відмовостійкості за умов фізичних дефектів та дефектів проектування [16]. Запропоновано абстрактні моделі БЦА, варіанти їх реалізації при структурно-аналітичній диверсності. Проведено експериментальні дослідження БЦА в умовах одиничних і кратних відмов.

5. Надано системний аналіз, запропоновані базові моделі та архітектури гарантоздатних комп'ютерних систем на основі дослідження варіантів комплексування принципів багатоверсійності, захисту інформації (security) та відмовостійкості. Проведено теоретичні та експериментальні дослідження систем захисту (забезпечення) конфіденційності та цілісності. Зокрема, експериментально доведено доцільність використання двохверсійних цифрових підписів [29].

6. Розроблено клас відмовостійких FPGA-систем (на основі програмованих логічних схем) з гібридним резервуванням. Досліджені аналітичні та імітаційні моделі систем на кристалі (systems on chip ? SOC) при кластерних відмовах логічних комірок. Запропоновано структурно-просторовий підхід до моделювання, розробки та адаптації FPGA-SOC до відмов [30]. Розроблено алгоритмічні та програмні засоби генерації кластерних відмов, конфігурування структур та їх дослідження. Отримано два сертіфікати Фонду алгоритмів і програм [31, 32].

7. Розроблені методи профілювання та надійного проектування комп'ютерних мереж для критичних застосувань при використанні відкритих мережних технологій. Побудовані мережні профілі для інфомаційно-управляючих систем критичного застосування (АЕС), методики оцінки та забезпечення відповідності профілям на рівні структурованих кабельних систем, розроблені моделі життєвого циклу комп'ютерних мереж та інструментальні засоби їх проектування з урахуванням вимог до надійності та живучості [33 – 35].

8. Розвинуто компонентно-орієнтований підхід до проектування та оцінки ризиків КІС для критичних застосувань з використанням раніше розроблених (Of-The-Shelf) компонент, у тому числі комерційних апаратних та програмних засобів (COTS-компонент) [36]. Надано їх класифікацію і аналіз варіантів обміну та перетворення таких компонент між комерційними (COTS) та критичними (CrOTS) застосуваннями [37]. Проаналізовані можливості і доведена доцільність забезпечення безвідмовності та стійкості до факторів космічного середовища бортових КІС для комерційних проектів на базі IOTS-підходу, тобто використання компонент класу Industry, що дозволяє мінімізувати витрати при виконанні вимог до надійності та безпеки [38]. Проведено порівняльний аналіз аварій та інцидентів у ракетно-космічній галузі та у атомній енергетиці внаслідок недостатньої верифікації проектів при використанні OTS-компонент [39].

9. Розроблено моделі стійких до зовнішніх втручань (intrusion-tolerant) інформаційно-пошукових систем (ІПС), що функціонують в умовах впливів на різні алгоритмічні компоненти ІПС [40] та реалізують багатоверсійні технології.

10. Проведена систематизація імовірнісних моделей надійності програмних засобів і запропоновано графові-матричний метод її оцінки [41]. Розроблено метрико-імовірносний метод оцінки якості та надійності програмного забезпечення та інструментальні засоби його підтримки [42]. Подано заявку на патент України на систему оцінки якості ієрархічних об'єктів. Проведено практичне відпрацювання цього методу при оцінці надійності бортових операційних систем, програмного забезпечення КІС АЕС, комерційних телекомунікаційних систем. Запропоновано комплекс

багатофрагментних марковських моделей оцінки надійності відновлюваних ПЗ з урахуванням зміни параметрів потоків відмов і відновлень [20].

11. Розроблено теоретичні та нормативно-методичні засади побудови інструментальної системи підтримки незалежної верифікації та експертизи критичного програмного забезпечення (систем профілювання та оцінювання) [43]. Проведено прототипування та розроблені інструментальні засоби побудови та аналізу профілів і метричного оцінювання [44]. Розроблені галузеві стандарти і стандарт підприємства щодо методів оцінки якості програмного забезпечення аерокосмічних систем.

12. Розроблено аналітичні (комбінаторно-імовірнісні та марковські) та імітаційні моделі живучих систем обробки інформації та управління з багатоступеневою деградацією [20, 45, 46]. З урахуванням специфіки авіаційних комплексів проведені розробка та дослідження потенційно живучих систем на основі моделей номінальних функціональніх структур. Запропоновано методику оцінки потенційної живучості бортових інформаційно-управляючих систем шляхом аналізу критичності функцій підсистем і можливості перерозподілу ресурсів при відмовах [47].

13. Проведена розробка, моделювання та дослідження класу багатоканальних дубльованих систем (БДС), що базуються на STRATUS-технологіях. Розроблені структурно-компонентні моделі, доведені твердження та теоремі щодо властивостей контролездатності, діагоностованості та відмовостійкості одно- та багатоверсійних БДС. Досліджені марковські моделі готовності БДС при різних стратегіях відновлення. Запропоновано інформаційну технологію (технологію гарантованої готовності) побудови гарантоздатних систем на принципах адаптації, багатоверсійності та гнучкого відновлення [48]. Доведені переваги розроблених архітектур відносно штатних ІУС, важливих для безпеки АЕС. Отримано патент України на винахід “Резервована система” [49].

14. Розроблено моделі станів, подій та оцінки відмовобезпечних інформаційно-управляючих систем. Визначені та досліджені класи похибок першого-четвертого роду для відмовобезпечних КІС. Запропоновані алгоритмічні методи оперативного відновлення їх працездатності та проведено імітаційне моделювання за допомогою розробленого програмного комплексу [50].

15. Розроблені та досліджені моделі та методи комбінованого структурно-версійно-часового резервування систем, важливих для безпеки, при кратних і парних відмовах апаратних і програмних засобів. Запропоновано метод вибору відмовостійких структур на основі побудови та аналізу пріоритетних рядів з використанням методів детермінованого, імовірнісного та експертного аналізу [51, 52].

16. Проведено аналіз доцільності використання принципу диверсності для систем захисту інформації. Сформовано клас так званих SDOD (Security-Diversity Oriented Decisions)-рішень, в яких завдяки його використанню забезпечується відмовостійкість та безпека (security). Надано варіанти та експериментально підтверджена доцільність впровадження структур, що реалізують двохверсійний цифровий підпис [29].

17. Одержані моделі, що базуються на принципі багатоверсійності, за допомогою яких є можливим підвищити криптографічну стійкість систем захисту інформації з точки зору забезпечення її конфіденційності. Запропоновані підходи базуються на сумісному використанні симетричних та несиметричних криптоалгоритмів для криптографічних перетворень повідомлень та ключових параметрів за різними способами [29].

Означені результати були отримані при виконанні держбюджетних та госпдоговірних НДР, договорів про науково-технічну співпрацю з підприємствами та організаціями м. Харкова, України та інших країн.

5. Забезпечення рівня наукових результатів

Світовий рівень отриманих результатів досліджень підтверджується тим, що вони:

– пройшли експертизу та включені до програм Європейських і всесвітніх конференцій з питань розробки комп'ютерних систем і технологій, забезпечення їх надійності та безпеки COMPSAC-2002 (Оксфорд, Англія), PSAM-2000 (Осака, Японія), 2002 (Пуерто-Ріко, США), MAPLD-2001-2003 (Меріленд, США), ESREL-1999 (Мюнхен, ФРН), 2001 (Флоренція, Італія), 2004 (Берлін, ФРН) 2004 (Гданськ, Польща), DSN-2004 (Флоренція, Італія) та ін.;

– опубліковані у збірках праць означених конференцій, рейтингових

журналах, а також у колективній монографії “Dependable Architectures of Computing Systems”, що прийнята до видання у видавництві "Шпрингер", ФРН. Отримано Сертифікат визнання журналу “Systems and Software”, Elsevier Publishing- Amsterdam – New-York, 2003р.);

– увійшли складовою до проекту «Багатоверсійний підхід до створення програмних систем і його розвиток для нових застосувань", виконаного у 2003-2004 за грантом, наданим Британським королівським науковим товариством;

– опубліковані у 2004 – 2005 роках у науково-технічних звітах сумісно з університетами Ньюкасла та Лондона (Великобританія) [10, 11];

– використані при підготовці у 2003 – 2005 роках проектів 2 галузевих стандартів за замовленням Національного космічного агентства України, в яких надаються вимоги та методи оцінки якості програмного забезпечення для КІС космічних комплексів і стандарту підприємства, що регламентує процеси розробки, верифікації та сертифікації програмного забезпечення бортових авіаційних систем;

– реалізовані у вигляді технічних і програмних рішень, захищених патентами і сертифікатами [31, 32, 49].

Наукові і практичні результати досліджень обговорюються на протязі 2001 – 2005 років на постійно діючому науково-технічному семінарі "Критичні комп’ютерні системи та технології" (http://k503.xai.edu.ua/), який має статус Всеукраїнського. На 30 засіданнях було заслухано понад 60 доповідей фахівців з України (Києва, Харкова, Донецька, Севастополя, Кіровограда, Полтави, Черкас, інших міст), Росії, Молдови, що представляють університети, науково-технічні центри, конструкторські бюро, приватні фірми –розробники інформаційних технологій.

6. Практичне використання наукових результатів

Практична цінність отриманих результатів полягає в тому, що вони забезпечили розробку інформаційних технологій та конкретних програмно-технічних рішень та підвищення достовірності оцінки верифікації та експертизи програмних засобів, комп’ютерних систем і мереж для аерокосмічних комплексів АЕС, інших критичних застосувань, їх гарантоздатності (безвідмовності, готовності та безпеки) у контексті виконання держав-

них планів і національних програм розвитку космічної галузі, транспорту, атомної енергетики. Їх подальше впровадження забезпечить зниження ризиків аварій ті катастроф критичних систем внаслідок зменшення імовірності невиявлених дефектів програмних засобів, можливості оперативного парирування відмов апаратних і програмних засобів, відмов внаслідок зовнішнього втручання та дії екстремальних факторів середовища. Розроблені технології, технічні рішення та інструментальні засоби є конкурентноздатними і можуть забезпечити пріоритетність України у наукоємних інформаційних галузях, пов'язаних з критичними застосуваннями та їх комерційними аналогами.

Результати досліджень реалізовані у 2001 – 2005 роках на підприємствах і конструкторських бюро авіаційно-космічної, енергетичної та інших галузей, організаціях і установах, які спеціалізуються на розробці, виробництві, випробуваннях, нормуванні безпеки та проведенні експертизи критичного програмного забезпечення, комп'ютерних систем і мереж, а саме при: створенні інтегрованого інструментального середовища підтримки експертизи та незалежної верифікації ПЗ систем критичного застосування (Сертифікаційний центр АСУ Держцентрякості ДКЯРУ, 2002-2005рр.); розробці галузевих нормативних вимог до якості програмного забезпечення й програмно-технічних комплексів критичного застосування для ракетно-космічної техніки, гармонізованих з нормативною базою Європейської кооперації по стандартизації космічної діяльності (ECSS) (Сертцентр АСУ Держцентрякості ДКЯРУ, 2003 – 2005рр.); розробці методів і засобів забезпечення відмовобезпеки цифрових систем контролю та управління АЕС при використанні програмованих ВІС (ЗАТ "Радій", 2003-2005рр.); розробці авіаційних відмовостійких систем з використанням ПЛІС-технологій (НТСКБ "Полісвіт", 2001 – 2005рр.) та ін.

Відповідно до договору про науково-технічну співпрацю з представництвом фірми "General Electric Fanuc"(м. Москва) та Хартеп (м. Харків) створена експериментальна база для навчання студентів та науково-технічних розробок сучасних вбудованих мікроконтролерних систем для енергетики та інших галузей.

Результати досліджень реалізовані *у навчальному процесі* при підготовці фахівців за спеціальностями «Комп'ютерні системи та мережі", «Сис-

темне програмування», “Спеціалізовані комп’ютерні системи” у вигляді монографій [16, 53 – 54] підручників [20, 55, 56], конспектів лекцій, навчально-методичних посібників [57 – 59], у спецкурсах і лабораторно-дослідницьких заняттях, курсових, бакалаврських і магістерських кваліфікаційних роботах і дипломних проектах, при розробці планів і програм післядипломної освіти.

Крім того, у монографіях [60, 61] опубліковані результати, пов'язані з проблематикою управління проектами для критичних застосувань, що базуються на принципах, які апробовані для задач оцінки та управління якістю програмного забезпечення [53, 58, 62, 63].

За результатами досліджень у 2003 – 2005 роках захищено 7 кандидатських дисертацій, 12 магістерських робіт. У 2005 – 2007 роках планується *підготувати та захистити* 2 докторські, 8 кандидатських дисертацій, 15 магістерських робіт.

7. Напрямки подальших досліджень

Подальші дослідження планується проводити за такими напрямками.

1. *Розробка теоретичних основ гарантоздатних комп’ютерних систем*, а саме: системний аналіз властивості гарантоздатності комп’ютерних систем і мереж та взаємовпливу її складових; аналіз шляхів зменшення ризиків аварій аерокосмічної техніки, пов’язаних з відмовами комп’ютерних систем та шляхів підвищення їх гарантоздатності; розробка узагальнених моделей гарантоздатних систем та показників гарантоздатності.

2. *Розробка методів оцінки та забезпечення якості та надійності, інструментальної підтримки верифікації та експертизи критичного програмного забезпечення*: удосконалення методів і технологій профілювання програмного забезпечення і комп’ютерних систем для аерокосмічних, енергетичних та інших застосувань; розробка та дослідження методів метричної оцінки та управління якістю критичного програмного забезпечення, моделей якості вимог до програмного забезпечення; удосконалення методів та інструментальних засобів метрико-ймовірнісної оцінки надійності програмного забезпечення та їх експериментальне дослідження; розробка моделей багатоверсійного життєвого циклу, дослідження метрик

диверсності реальних проектів, технологій створення відмовостійкого програмного забезпечення з використанням процесно-продуктної версійної надмірності.

3. *Розробка методів і засобів оцінки та забезпечення відмовостійкості та живучості конфігурованих апаратних засобів для вбудованих (бортових) комп'ютерних систем управління реального часу з програмованою логікою (ПЛІС, систолічних процесорних матриць та ін.)*: систематизація та аналіз варіантів побудови відмовостійких комп'ютерних систем управління за технологіями CPLD, FPGA, мікроконтролерними технологіями та їх сумісними рішеннями; моделювання відмов ПЛІС-структур в умовах зовнішніх факторів космічного простору; розвиток теорії та експериментальне дослідження багатоверсійних цифрових пристроїв з програмованою логікою та технологій їх проектування; розробка методів верифікації ПЛІС-проектів для критичних застосувань.

4. *Розробка та дослідження принципів створення гарантоздатних комп'ютерних систем і технологій гарантованої готовності*: аналіз варіантів розвитку та комплексування принципів багатоверсійності, багатопараметричної адаптації та керованої багатоступеневого відновлення; дослідження шляхів, методів оцінки та зниження ризиків використання Of-The-Shelf - компонент для критичних застосувань; аналіз HA-, CA- технологій та розробка технологій гарантованої готовності.

5. *Розробка методів інструментальної підтримки проектування та модернізації комп'ютерних мереж для критичних застосувань*: удосконалення моделей життєвого циклу комп'ютерних мереж для критичного застосування, що будуються з використанням відкритих мережних технологій та стандартів; систематизація варіантів та розробка моделей функціонального, просторового та надійнісного реінжинірингу комп'ютерних мереж; розробка методів профілювання та інформаційної технології оцінки та вибору профілів комп'ютерних мереж для критичних застосувань; дослідження методів оцінки та забезпечення надійності та живучості комп'ютерних мереж для критичного застосування.

6. *Розробка та дослідження гарантоздатних Web-систем*: моделювання Web-додатків, побудованих з використанням інтегрованих Web-сервісів, що функціонують в умовах відмов апаратних, програмних ком-

понент та зовнішніх втручань; розробка методів оцінки та забезпечення гарантоздатності інтегрованих Web-сервісів з використанням принципів диверсності; розробка та експериментальне дослідження гарантоздатних архітектур Web-систем; розробка моделей та дослідження гарантоздатних інформаційно-пошукових систем.

7. *Розробка та дослідження моделей та засобів забезпечення захисту інформації на основі багатоверсійних технологій*: систематизація та аналіз можливих варіантів застосування багатоверсійних технологій в системах захисту інформації; розробка методів забезпечення цілісності та конфіденціальності з використанням принципу диверсності; програмно-апаратна реалізація засобів забезпечення захисту інформації на основі багатоверсійних технологій; експериментальне дослідження моделей та засобів забезпечення захисту інформації на основі багатоверсійних технологій.

Закінчення

1. Проблема розробки та дослідження гарантоздатних комп'ютерних систем є однією з ключових проблем розвитку сучасних інформаційних технологій, оскільки її вирішення є визначальним для безпеки аерокосмічних, енергетичних, інших критичних застосувань та конкурентоспроможності комерційних рішень, що базуються на використанні складних інформаційних, інформаційно-управляючих системах розподілених обчисленнях, мережі Інтернет.

2. Наукові та практичні результати, отримані на протязі останніх років фахівцями кафедри комп'ютерних систем і мереж у співдружності з науковцями інших країн та вітчизняними розробниками КІС для авіаційних, космічних систем, інформаційно-управляючих систем АЕС, дозволили підвищити надійність та безпеку КІС та ККВ, повноту та достовірність оцінки якості програмного забезпечення і таким чином зменшити ризики аварій та катастроф. Вони створили підґрунтя для подальших досліджень та впровадження їх результатів.

3. Напрямки проведення подальших досліджень та очікувані результати: *теоретичні основи, моделі та методи* оцінки та забезпечення гарантоздатності комп'ютерних систем; *методики, алгоритми, програмні та ін-*

струментальні засоби моделювання, розробки, верифікації та експертизи програмного та апаратного забезпечення гарантоздатних аерокосмічних КІС, інших КІС ККВ з урахуванням обмежень, які пов'язані з особливостями їх використання (бортових або наземних, відновлюваних або невідновлюваних, розподілених або зосереджених, факторів агресивного активного або пасивного середовища); *патентоздатні технічні рішення* засобів забезпечення гарантоздатності (безвідмовності, готовності та безпеки) КІС; *нормативно-методичні документи* для авіаційної, ракетно-космічної та енергетичної галузей, стандартів підприємств; *навчальні програми, підручники, посібники* для відповідних навчальних дисциплін підготовки бакалаврів, магістрів, аспірантів, докторантів.

Література

1. Avizienis A., Laprie J.-C., Randoll B. Fundamental Concepts of Dependability //Technical Report: UCLACSD Report no. 010028, LAAS Report no. 01-145, Newcastle University Report no.CS-TR-739. – 2002. – 31 p.

2. Avizienis A., Laprie J.-C. Dependability Computing: From Concepts to Design Diversity // Proceeding of the IEEE. – 1986. - № 5. – P. 629 – 638.

3. Харченко В.С. Многоальтернативные системы и обеспечение гарантоспособности. – Х.: Ин-т проблем машиностроения АН Украины, 1989 – 33 с.

4. Харченко В.С. Модели и свойства отказоустойчивых многоальтернативных систем // Автоматика и телемеханика. – 1992. – № 12. – С. 140 – 147.

5. Barlett W., Spainhower L. Commercial Fault Tolerance: A Tale of Two Systems // IEEE Transactions on Dependable and Security Computing. – 2004. – Vol. 1, № 3. – P. 87 – 96.

6. Харченко В.С., Асидех Ф.А. STRATUS-системы для энергетических комплексов гарантированной готовности: компонентная модель, свойства и метод адаптации // Вісник Харківського державного технічного університету сільського господарства. – Х.: Міністерство аграрної політики України. – Вип. 27, том 2. –С. 207 – 210.

7. Харченко В.С. От безотказных цифровых устройств к гарантоспособным Веб-системам: эволюция парадигм, методов и средств // Труды Международной конференции «СИЭТ-2004», Одесса. – 2004. – С. 15 – 17.

8. Харченко В.С. От безотказности электронных устройств к гарантоспособности web-систем // Контрольно-измерительные приборы и автоматика. – 2004. – № 9. – С. 4 – 10.

9. Фон-Неман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. – М.: ИЛ, 1956. – С. 68 – 139.

10. CS-TR: 863 Development of Dependable Web Services out of Undependable Web Components / A. Gorbenko, V. Kharchenko, P. Popov, A. Romanovsky, A. Boyarchuk. School of Computing Science, University of Newcastle, Oct. 2004. – 36 p.

11. CS-TR: 879 Dependable Composite Web Services with Components Upgraded Outline: Solutions, Model and Implemenmtation / A. Gorbenko, V. Kharchenko, P. Popov, A. Romanovsky. School of Computing Science, University of Newcastle, Dec. 2004. – 25 p.

12. V. Kharchenko, P. Popov, A. Romanovsky. On Dependability of Composite Web Services with Components Upgraded Online / Proceedings of Workshop on Architecting Dependable Systems (DSN), Florence, Italy, 30 June, 2004. – P. 14 – 20.

13. Харченко В.С., Токарев В.И. Проектирование отказоустойчивых и живучих компьютерных систем управления на основе концепции “3М” // Вісник Технологічного університету Поділля. – 2003. – № 3. – С. 29 – 32.

14. Avizienis A. The N-Version Approach to Fault-Tolerant Software // IEEE Trans. on Software Engineering. – 1985. – Vol. SE-11, № 12. – P. 1491 – 1501.

15. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х.: МО Украины. – 1996. – 506 с.

16. Харченко В.С. и др. Многоверсионные системы, технологии и проекты / Под ред. В.С. Харченко. – Х.: МОНУ, 2003. – 528 с.

17. Kharchenko V.S., Tarasenko V.V. The Multiversion Design Technology of an Onboard Fault-Tolerant FPGA Devices // Proceedings of Military and Aerospace Applications of Programmable Devices and Technologies Conference (MAPLD), Laurel, Maryland, USA, September, 11 – 13, 2001.

18. Kharchenko V.S., Sklyar V.V. On-Board Device and System Architectures with the Version-Threshold Adaptation to Hardware and Software Faults // Proceedings of MAPLD, Maryland, USA, September, 12 – 15, 2002.

19. Ushakov A.A., Kharchenko V.S. Fault-tolerant on-board PLD-systems: a space-structural simulation and methods of adaptation // Radioelectronics & informatics. Proceedings of East-West Design & Test Conference (EWDTC-2003). – 2003. – № 3. – P. 100 – 106.

20. Барбаш І.П., Благодарний М.П., Харченко В.С. т. ін. Основи цифрових систем. Підручник / За ред. В.С. Харченка, М.П. Благодатного. – Х.: МОНУ, Національний аерокосмічний університет ім. М.Є.Жуковського. – 2003. – 562 с.

21. Харченко В.С., Мухаметов З.Г., Токарев В.И. Метод оценки и выбора живучих структур многоярусных резервированных систем обработки информации АСУ // Моделювання та інформаційні технології. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ. – 2003. – Вип. 22. – С. 219 – 222.

22. Харченко В.С., Скляр В.В., Тарасюк О.М. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций // Радіоелектронні і комп'ютерні системи. – Х.: НАКУ «ХАІ».– 2003. – Вип. 3. – С. 135 – 149.

23. Харченко В.С., Скляр В.В., Тарасюк О.М. Надёжность компьютерных систем и безопасность аэрокосмической техники // Авиационная и ракетно-космическая техника и технология. – Х.: НАКУ «ХАИ». – 2004. – № 1. – С. 28 – 37.

24. Харченко В.С., Горбенко А.В., Боярчук А.В., Мамутов С.С., Михайличенко А.И. Инструментальная платформа для создания гарантоспособных композитных web-сервисов "INDECS" // Труды международной конференции "Информационные технологи в науке, производстве, образовании". – Х. – 2005, 24 – 26 марта. – С. 35 – 37.

25. Kharchenko V., Yastrebenetsky M., Sklyar V. Diversity Assessment of Nuclear Power Plants Instrumentation and Control Systems // Proceedings of ESREL-PSAM Conference. – Berlin. – June, 2004. – P. 1351 – 1356.

26. Скляр В.В. Анализ метрик многоверсионности программного обеспечения // Электронное моделирование. – 2004. – Т. 26. – № 4. – С. 95 – 104.

27. Волковой А.В., Скляр В.В., Харченко В.С. Метод формирования моделей многоверсионного жизненного цикла для программных проектов

// Інформаційно-керуючі системи на залізничному транспорті. – 2004. – №2 (46). – С. 40 – 44.

28. Скляр В.В., Токарев В.И. Метод оценки и выбора вариантов структур информационных и управляющих систем // Моделювання та інформаційні технології. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ. – 2004. – Вип. 26. – С. 184 – 187.

29. Лысенко И.В., Халин М.В., Харченко В.С. Анализ и разработка методов и средств защиты информации с использованием многоверсионных технологий // Отчет о НИР Г503-42/2003. – Х.: ХАИ, 2003. – С. 415 – 445.

30. Ushakov A.A., Kharchenko V.S. Methods of Modeling and Error-Tolerant Design of Dependable Embedded SOPC/FPGA-Decisions by Use of Multiversion Technology // Proceedings of East-West Design and Test Workshop (EWDTW'04). – Yalta, Alushta, Crimea, Ukrain, 2004. – P. 172 – 178.

31. Свідоцтво № 10393 про реєстрацію автор. права на комп'ютерну програму «Настраиваемый генератор кластерных отказов логических ячеек программируемых логических интегральных схем» / Ушаков А. О., Якимець Н. В. Видано Держ. департаментом інтелектуальної власності 24.06.2004.

32. Свідоцтво № 11145 про реєстрацію авторського права на комп'ютерну програму «Инструментальное средство поддержки имитационного моделирования устойчивости цифровых устройств на программируемых логических интегральных схемах к отказам различных конфигураций» / Ушаков А. О., Якимець Н. В. Видано Держ. департаментом інтелектуальної власності 23.09.2004.

33. Kharchenko V.S., Gorbenko A.V. FME(C)A Technique of Assessment and Ensuring of a Corporate Computer Network Fault-Tolerance and Safety // Proceedings of 6th Probabilistic Safety Assessment and Management Conference, Puerto Rico, 2002. – P. 96 – 102.

34. Горбенко А.В., Харченко В.С. Оценка структурной надёжности нерезервированных структурированных кабельных систем при многократных отказах // Технология приборостроения. – 2001. – № 1-2. – С. 189 – 193.

35. Gorbenko A.V., Kharchenko V.S., Hlestkov V.I. Reliability of computer networks based on open standards: requirements, methods of analysis and means of ensuring // Foreign Radioelectronics. – 2003. – № 6. – P. 22 – 41.

36. Харченко В.С., Скляр В.В., Кожемяченко В.Г. Классификация и профилирование OTS-продуктов для компьютерных систем управления // Системи обробки інформації. – Х.: ХВУ. – 2003. – Вип. 2. – С. 38 – 44.

37. Харченко В.С., Харченко К.В. COTS- и CrOTS-подходы к повышению эффективности критических и коммерческих IT-проектов // Системи обробки інформації. – Х: ХВУ. – 2002. – Вип. 2(18). – С. 252 – 258.

39. Харченко В.С., Скляр В.В. Верификация и оценка качества программных OTS компонент для информационных и управляющих систем энергетических комплексов // Вісник Харківського державного технічного університету сільського господарства. – Х.: ХДТУСГ. – 2003. – Вип. 19, Т. 2. – С. 123-128.

40. Садовский А.А. Использование многоверсионных технологий для повышения отказоустойчивости поисковых систем // Отчет о НИР Г503-42/2003. – Х.: ХАИ. – 2003. – С. 510 – 525.

41. Kharchenko V.S., Tarasyuk O.M., Sklyar V.V., Dubnitsky V.Yu. The Method of Software Reliability Growth Models Choice Using Assumptions Matrix // Proceedings of 26th Annual International Computer Software and Applications Conference “COMPSAC’2002”, Oxford, England.– 2002.– P. 541 – 546.

42. Тарасюк О.М. Метод комплексной метрико-модельной оценки качества и надежности программного обеспечения // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 2. – С. 105 – 111.

43. Konorev B.M., Kharchenko V.S., Chertkov G.N. Tool-associated system supporting expertise and independent verification of critical software: development and implementation approaches // Information technologies and safety, Proceedings of Institute of Problems in Registration of Information, NASU, Kyiv. – № 4, 2003. – P. 85 – 91.

44. Kharchenko V.S., Sklyar V.V. Monte-Carlo simulation of the unmanned multiversion systems // Proceedings of International Conference of Monte-Carlo Simulation, Monte-Carlo, Monaco, June 18-21, 2000. – P. 33 – 34.

45. Kharchenko V.S. The Probabilistic Assessment of Survivability and Safety of an Unmanned Control Systems with Multistage Degradation by Use of QD-diagrams // Proceeding of 5th International Conference on Probabilistic

Safety Assessment and Management, Osaka, Japan, 27 November, 27 - December, 1, 2000, vol.1. – P. 525 – 531.

46. Kharchenko V.S., Cherepakhin D.A. Risk Analysis of Control Systems by Use of QD-diagrams and FMECA-approach // Proceedings of 12th European Conference on Safety and Reliability, Turin, Italy, September, 16-20, 2001.

47. Харченко В.С., Бородавка Н.П. Формализованное представление номинальной функциональной структуры для анализа живучести бортовых ИУС // Моделювання та інформаційні технології. – К.: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ. – 2004. – Вип. 26.– С. 206 – 217.

48. Харченко В.С., Асидех Ф.А., Лисенко И.В. Марковские модели готовності восстанавливаемых STRATUS-систем // Системи обробки інформації. – Х.: ХВУ. – 2004.– Вип. 4.– С. 216 – 226.

49. Патент України №71083 від 16.09.2004. Пристрій для контролю та реконфігурації резервованої системи, МПК H05K10/00, G06F15/16/ Харченко В.С., Асидех Ф.А.

50. Харченко В.С., Скляр В.В., Аль-Тарази А.Х.. Теоретико-множественные модели отказоустойчивых ИУС с учетом их влияния на безопасность // Радіоелектронні і комп'ютерні системи. – Х.: НАКУ "ХАІ". – 2004. – № 2. – С. 67 – 74.

51. Kharchenko V., Shurigin O. Deterministic assessment of fault-tolerant duplicated computing structures with combined redundancy // Engineering Simulation. – 2001. – №3. – P. 31 – 38.

52. Харченко В.С., Токарев В.И., Шурыгин О.В. Анализ влияния ошибок контроля на безопасность резервированных систем управления критическими объектами // Тр. конф. «Информационно-управляющие системы на транспорте». – Алушта. – 2003. – С. 121 - 122.

53. Методы моделирования и дискретной оптимизации вычислительных систем реального времени / В.Я. Жихарев, С.В. Листровой, В.С. Харченко и др. Под ред. В.Я. Жихарева. – Житомир: Изд-во ЖГУ. – 2004. – 494 с.

54. Информационно-управляющие системы АЭС: проблемы безопасности / М.А. Ястребенецкий, В.Н. Васильченко, В.С. Харченко и др. Под ред. М.А. Ястребенецкого. – К.: Техника, 2004. – 502 с.

55. Надійність цифрових систем. Підручник / В.С. Харченко, В.М. Ілюшко, В.Я. Жихарєв та ін. За ред. В.С. Харченка, В.Я. Жихарєва. – Х.: Національний аерокосмічний університет. – 2005. – 570 с.

56. Надійність цифрових систем. Підручник / В.С. Харченко, Є.А. Артеменко, В.М. Ілюшко та ін. За ред. В.С. Марченка, В.М. Ілюшка. – Х.: Національний аерокосмічний університет. – 2005. – 654 с.

57. Лысенко И.В. Основы безопасности и защиты информации в компьютерных системах: Конспект лекцій. – Х.: Мин. образования и науки Украины. – 2004. – 110 с.

58 Харченко В.С., Скляр В.В.., Тарасюк О.М. Методы моделирования и оценки качества и надежности програмного обеспечения: Учебное пособие. – Х.: Мин. образования и науки Украины. – 2004. – 159 с.

59. Харченко В.С., Тарасенко В.В., Ушаков А.А. Встроенные отказоустойчивые цифровіе системі с программируемой логикой: Учебное пособие. – Х.: Мин.образования и науки Украины. – 2004. – 188 с.

60. Дружинин Е.А., Жихарев В.Я., Харченко В.С. и др. Научно-методическое обеспечение управления сложными проектами. – К.: Техника, 2002. – 369 с.

61. Бабынин И.М., Жихарев В.Я., Харченко В.С. и др. Применение методов искусственного интеллекта в управлении проектами / Под ред. А.Ю. Соколова. – Х.: Мин.образования и науки Украины. – 2002. – 474 с.

62. Харченко В.С., Тарасюк О.М. Использование радиальных метрических диаграмм для оценки характеристик программного обеспечения // Открытые информационные и компьютерные интегрированные технологии.– Х.: Нац. аэрокосмический ун-т “ХАИ”. – 2003. – Вып. 18. – С. 123 – 133.

63. Харченко В.С., Тарасюк О.М. Оценка экспертизы программного обеспечения: показатели, методика и инструментальные средства // Информационные технологии и безопасность.– К.: НАНУ, Институт проблем регистрации информации. – 2003. – Вып. 4. – С. 128 – 139.

Надійшла до редакції 18.04.2005