УДК 681.5

Б.Г. МУДЛА, Т.І. ЄФІМОВА, Р.М. РУДЬКО

ГАРАНТОЗДАТНІСТЬ ЯК ФУНДАМЕНТАЛЬНИЙ УЗАГАЛЬНЮЮЧИЙ ТА ІНТЕГРУЮЧИЙ ПІДХІД

Abstract. *The main principles and conditions of formation and stages of development of the fundamental theory and practice of the generalizing and integrating concepts of dependability were presented after the leadthrough the first joint conference of two scientific schools of J. von Neumann and N. Wiener. The basic aspects of development of theoretical principles and results of applied researches of integration processes of reliability (fail-safety), fault-tolerance and dependability of information-control computer systems (ICCS) are demonstrated.*
Key words: *critical technologies, reliability, fault-tolerance, dependability and secure, ICCS.*

Анотація. *Представлені головні принципи та умови становлення і етапи розвитку фундаментальної теорії і практики узагальнюючих та інтегруючих концепцій гарантоздатності, починаючи з першої об'єднаної конференції двох наукових шкіл Дж. фон Неймана і Н. Вінера. Приведені основні положення розвитку теоретичних засад і результатів прикладних досліджень інтеграційних процесів безвідмовності (надійності), відмовостійкості та гарантоздатності інформаційно-управляючих комп'ютерних систем (ІУКС).*
Ключові слова: *критичні технології, безвідмовність, відмовостійкість, гарантоздатність і захист, ІУКС.*

Аннотация. *Представлены главные принципы, условия становления и этапы развития фундаментальной теории и практики обобщающих и интегрирующих концепций гарантоспособности, начиная с первой объединённой конференции двух научных школ Дж. фон Неймана и Н. Винера. Приведены основные положения развития теоретических основ и результатов прикладных исследований интеграционных процессов безотказности (надёжности), отказоустойчивости и гарантоспособности информационно-управляющих компьютерных систем (ИУКС).*
Ключевые слова: *критические технологии, безотказность, отказоустойчивость, гарантоспособность и защита, ИУКС.*

1. Вступ

Створення ІУКС довгострокового безвідмовного функціонування, «здатних надавати гарантовані послуги, яким можна виправдано довіряти», на основі стійкої до відмов архітектури ІУКС, «здатної продовжувати роботу і тоді, коли в реальній системі виникають різного роду несправності, збої та відмови компонентів», є не тільки актуальною фундаментальною проблемою computer science, інформаційних технологій та кібернетики, а й важливою державною задачею. Вона пов'язана із залежністю життєдіяльності людей від сучасних ЕОМ, автономних бортових ІУКС, локальних та глобальних комунікаційних мереж, техніки зв'язку та інформаційних технологій, що інтегруються у критичні і техногенні технології та інфраструктури.

Уразливість існуючих комп'ютеризованих інфраструктур та нагальність задач щодо її подолання підтверджуються численними випадками несанкціонованих атак, здатних дистанційно дезорганізувати урядові, банківські, енергетичні мережі, оборонні системи управління. Так, за даними вчених університету Торонто, виявлено мережу електронних шпигунів, вірус – шпигун якої відслідковував вміст 1295-ти урядових комп'ютерів у 103-х країнах [1]. Найбільш показові катастрофи останніх десятиліть: аварії на ЧАЕС, ракети-носія ARIAN-5, ракети "Зеніт" з десятком супутників, збиття ізраїльського пасажирського літака, аварія на Саяно-Шушенській ГЕС та ін. Усі вони сталися при майже схожих несправностях і помилках ІУКС, що не були виявлені у процесі проектування або модифіковані без ретельної верифікації програмного забезпечення (ПЗ) після деяких, здавалося б, незначних змін в успадкованих пристроях.

Актуальність вирішення цих задач у ракетно-космічній, машинобудівній, авіаційній, енергетичній та військовій галузях зросла завдяки принципово новим вимогам глибокої модернізації автономних бортових ІУКС на основі фундаментальних досліджень у напрямку суттєвого

ISSN 1028-9763. Математичні машини і системи, 2010, № 2

підвищення перш за все їх ресурсних характеристик. Термін безвідмовного функціонування сучасних бортових автономних (замкнених – self-contained) ІУКС визначається терміном існування їх носіїв, який, наприклад, для космічних апаратів сягає тепер кількох десятків (близько 20 – 40) років. Це висунуло проблеми безвідмовності, відмовостійкості, гарантоздатності і безпеки в розряд найважливіших та стратегічних.

2. Становлення і розвиток теорії і практики узагальнюючих концепцій гарантоздатності

Гарантоздатність (безвідмовність, відмовостійкість і безпека) та живучість складних розподілених інформаційно-управляючих комп'ютерних систем і комплексів, інтегрованих у техногенні, критичні технології та інфраструктури, що управляють життєдіяльністю суспільства, у ряді розвинутих країн світу стала національним пріоритетом найвищого рівня [2], становлення і розвиток яких має досить тривалу історію [3]. Уже з появою різницевої машини Ч. Беббіджа [4] Едінбурзький огляд у 1834 році опублікував статтю доктора Д. Ларднера "Обчислювальна машина Беббіджа", у якій стверджується: "Найбільш впевнена та ефективна перевірка правильності обчислень вимагає виконання одних і тих же обчислень окремими та незалежними комп'ютерами; ця перевірка ще більш ефективна, якщо розрахунки виконуються різними методами".

Отримання правильних даних, адекватна їх переробка та доставка правильних розрахунків, надійне і безпечне обслуговування апаратури та комунікацій комп'ютерних систем і зв'язку були і є сьогодні турботою їх розробників, провайдерів та споживачів. Але висока надійність стала ґрунтовною проблемою лише у 40-х і на початку 50-х років XX століття з появою перших поколінь ЕОМ релейного типу для обслуговування телефонного зв'язку фірми Bell Telephone Laboratories та Raytheon Mfg. Co., а також ЕОМ ENIAC, EDVAC, EDSAC, JONIAC [5, 6], SEAC, DYSEAC [7] для обчислення складних високоточних задач балістики, атомної енергетики, проектування технічних засобів озброєння і військової техніки та ін. Використовували вони досить не надійні на той час компоненти: реле, електронні лампи, електронно-променеві трубки, запам'ятовуючі пристрої на лініях затримки та ін. Це змушувало розробників ЕОМ застосовувати різні методи контролю і боротьби зі збоями, помилками і відмовами, розробка та впровадження яких відставала від все нових вимог замовників щодо їх надійності. Такими, наприклад, стали принципово нові вимоги NASA (1958 р.) щодо створення комп'ютерів для понад 10-річного безвідмовного функціонування в рамках космічної місії – проект "Система самоконтролю та самовідновлення для управління і контролю космічного корабля" ("A Self–Testing – And Repairing (STAR) System for Guidance and Control") [8].

Зазначимо, що ідея самовідновлення та самоорганізації функцій кібернетичних систем належить творцям нового спрямування в науці і техніці, що виникли одночасно у 1948 році, – теорії самовідтворюючих автоматів Дж. фон Неймана[1] [6], кібернетики Н. Вінера[2] [9, 10] та нового підходу

[1] Теорія автоматів – наука про основні принципи, що є спільними для штучних автоматів (цифрові та аналогові обчислювальні машини, керуючі системи і комплекси) та для природних автоматів (нервова система людини, репродукування клітин, еволюція організмів).

[2] Кібернетика (від латино-грецького cybernetics – керманич) – наука, що вивчає системи будь-якої природи, які здатні отримувати, зберігати, переробляти і передавати інформацію та використовувати її для управління та регулювання.

до їх математизації й інтелектуалізації у фундаментальних роботах академіка В.М. Глушкова [11–17].

«У своїй роботі, стверджує А. Бйоркс [6], доктором фон Нейманом поставлено та вирішено аж ніяк не тривіальне питання про те, якого ґатунку має бути достатня логічна організація, щоб певний автомат був здатний себе відновлювати або відтворювати. Він виявив особливий інтерес до уявлення про достатньо складні автомати, такі як нервова система людини та надвеликі обчислювальні машини, появу яких він передбачив». При цьому він сконцентрував основні свої зусилля на двох суперечливих проблемах теорії автоматів – їх надійності та здатності себе відтворювати. «Надійність компонентів (складових) обмежує складність автомата, який ми можемо реалізувати, а властивість себе відтворювати вимагає досить високого рівня автомата». Але, створюючи швидкодіючі надійні EOM EDVAC (Electronic Discrete Variable Automatic Computer) [5], ENIAC (Electronic Numerical Integrator and Automatic Calculator), SEAC / DYSEAC (Standards Eastern Automatic Computer), JONIAC та інші проекти Гарвардського університету, а пізніше в Інституті перспективних досліджень (IFAS) у м. Прінстон [6], д-р Дж. фон Нейман на практиці переконався у своїх ідеях створення систематичної теорії, математичної та логічної за формою, яка б упорядкувала поняття та принципи, що стосуються структури та організації природних і штучних систем, ролі інформації та мови, програмування і управління в таких системах.

У той же час (1948 р.) професор Масачусетського технологічного інституту Н. Вінер видає свою знамениту книгу «Кібернетика або управління і зв'язок тварини та машини» [9, 10], головними тезами якої є подібність процесів управління та комунікацій в машинах, живих організмах і суспільствах (будь-то мурашиному чи людському), і перш за все це процеси передачі, збереження й перетворення інформації. Селективна теорія інформації та її кількість (як кількість вибірки), що ототожнюється з негативною ентропією, стає в ряд фундаментальних характеристик явищ природи, таких як кількість речовини або кількість енергії. Звідси його думки про кібернетику як науку загальної теорії управління і комунікацій, теорії організації і боротьби з світовим хаосом та зі згубним зростанням ентропії. При цьому професор Н. Вінер не був прихильником вузької спеціалізації, безпідставного розподілу науки на численні ізольовані галузі з їх «нічийними землями» та «прикордонними смугами» поміж окремими дисциплінами. У зв'язку з цим він пише: «…Працюючи з доктором А. Розенблютом (відомим мексиканським фізіологом), нам було абсолютно ясно, що наука має творитися згуртованими зусиллями багатьох людей. Активне та дійове вивчення білих плям на мапі науки може бути здійснене організованими колективами учених, кожен із яких, будучи спеціалістом у своїй галузі, має бути досконало ознайомленим з галузями наук своїх колег» [9, с. 45]. Так, з позиції нових понять кібернетики, професор Н. Вінер атакує проблеми техніки, фізики, біології, фізіології, медицини, психології, соціології з впевненістю, що це дасть можливість об'єднати і упорядкувати знання різних галузей, налагодити співпрацю учених різних країн, озброївши їх загальною мовою з єдиною термінологією та загальною методологією.

Керуючись такими висновками, проф. Н. Вінер та д-р Дж. фон Нейман вважали за необхідне провести зібрання всіх зацікавлених сторін для узгодження поглядів різних наукових шкіл. Така конференція відбулася у м. Прінстоні взимку 1943–1944 рр., де були присутні і інженери, і математики, і фізіологи, і психологи. «Д-р Д. фон Нейман, професор Н. Вінер та пан Вальтер Піттс

репрезентували математиків, фізіологи зробили спільне пояснення задач кібернетики під своїм кутом зору, аналогічним чином конструктори обчислювальних машин виклали свої погляди на цілі, задачі та методи. В кінці наради стало ясно, що існує суттєва ідейна спільність між фахівцями різних спеціальностей, що представники кожної групи уже можуть користуватися поняттями, відпрацьованими представниками інших груп, і при цьому треба продовжити намагання створити усіма визнану і для всіх спільну термінологію та її таксономію» [9].

Безумовно, таких же поглядів дотримувався і академік В.М. Глушков, який вважав аксіомою, що розробка масштабних напрямів сучасної науки і техніки, якою є кібернетика, до снаги лише великим колективам дослідників з різних галузей науки. Він відразу ж розгорнув роботи у трьох напрямках досліджень – апаратури, програмного забезпечення і застосування обчислювальної техніки. В.М. Глушков також побудував принципово нову теорію самоорганізації кібернетичних систем на основі геніальної ідеї розробки математичного апарата для логічного проектування обчислювальних машин та їх застосування шляхом інтелектуалізації процесів автоматизації програмування і синтезу електронної апаратури, пошуку нових принципів побудови ЕОМ та створення структур, подібних до головного мозку, програмування нових теорем у математиці та «розумних» процесорів, що «самі навчаються» та «самі налагоджуються», наукового управління виробничими процесами та економікою країни на основі загальнодержавної автоматизованої системи і багато інших [11–17].

Таким чином, уже на етапі становлення цих складних наук було запропоновано масштабну інтеграцію фахівців різних спеціальностей з різних країн для узгодження єдиної для всієї ІТ-галузі технічної мови спілкування. З того часу цей підхід еволюціонує в рамках IFIP, IEEE, ACM, ISO, IEC тощо у процесі безперервного оновлення та інтеграції фундаментальних концепцій, парадигм, термінів і понять та їх таксономічних побудов. Про аналіз цієї інтеграції та дослідження її етапів і підходів йдеться далі.

Еволюція концепції безвідмовності (надійності – reliability) ЕОМ та комп'ютеризованих систем (КС) на їх основі бере початок у перших наукових працях про методи боротьби з несправностями (physical faults), збоями (malfunctions) та відмовами (failures) у зв'язку з ненадійними їх компонентами, які характеризувались доволі високою інтенсивністю відмов та схильністю до мерехтіння (нестабільності) несправностей (transient error). Це призвело до появи оригінальних схем і методик виявлення несправностей та деяких методів автоматичного відновлення, таких як коди виявлення і виправлення помилок, дублювання з порівнянням, потроєння з голосуванням, елементи діагностики та визначення місць ушкоджень, вперше опублікованих у працях двох Гарвардських симпозіумів з проблем виявлення несправностей у ЕОМ для задач зв'язку в 1947 і 1949 рр. Аналогічним чином для усіх інших задач ці ж проблеми доповідались на перших двох Об'єднаних конференціях з розвитку ЕОМ у 1951 та 1952 рр.

Величезний інтерес до питань надійності у цей час проявився на третій Об'єднаній конференції «Системи обробки інформації: Надійність та вимоги», проведеній у грудні 1953 р. у Вашінгтоні Інститутом радіоінженерів (IRE), Американським інститутом інженерів-електриків (AIEE) та Асоціацією комп'ютерної техніки (ACM). У доповідях на конференції науково обґрунтовувались методи і засоби забезпечення надійності та відбувся обмін результатами багатьох практичних

застосувань. Симпозіум «Діагностичні програми та граничні випробування великих цифрових ЕОМ» в IRE (м. Нью-Йорк, 23–26 березня 1956 р.) був повністю присвячений безвідмовності КС. Було заслухано 5 доповідей за участю засновників цієї галузі – Г. Естрін, М. Фістер молодший, М. Уілкс. А доповідь Дж. Еккерта молодшого «Схеми контролю та діагностичні програми» і дотепер зберегла актуальність при виявленні несправностей і дублюванні [18].

У той же період Дж. фон Нейман, Е.Ф. Мур, К.Е. Шеннон та їх послідовники, досліджуючи кожен свою галузь проблем боротьби зі збоями та відмовами штучних і природних автоматів, прийшли до висновку, що безумовною перевагою останніх є передбачені ефективні способи самоконтролю і самовиправлення. Тому робота д-ра фон Неймана «Ймовірнісна логіка та синтез надійних організмів із ненадійних компонентів» (1952 р.) [19] стала першою фундаментальною науковою парадигмою[3] (відправним пунктом у теоретичному вивченні проблеми стійкості КС до відмов, «побудови надійних логічних структур із ненадійних компонентів», помилки в яких маскувались багаторазовим їх надлишком. Варіантами маскування, що найчастіше використовувались, були: чотирикратне (quadding) дублювання індивідуальних електронних компонентів і потроєння модулів з мажоритарним голосуванням. На практиці це є ефективним щодо функціональності системи, але щодо її продуктивності такий підхід веде до поступової деградації. Це й сприяло дослідженням та появі методу завбачення (method of the prediction) деградації засобів і теорії надлишковості (theory of the redundancy) комп'ютерів [19].

Теорії маскування та надлишковості компонент були узагальнені W.H. Pierce у концепцію стійкості до відмов (the concept of failure tolerance) в Академічному виданні 1965 р. Але вимога довговічності щодо проектування реальних космічних систем призвела до вивчення усіх доступних технічних рішень та теоретичних результатів. Розмаїтість існуючих теорій та методів мотивувала визначення уніфікованої концепції, що об'єднала б різноманітні підходи у єдине подання усіх системних ознак виживання у структурованій системі понять і термінів. Такі дослідження були виконані у 1967 р. під керівництвом д-ра А. Авіженіса (департамент Computer science Каліфорнійського університету Лос-Анджелеса – UCLA), який об'єднав теорію маскування з практичними технологіями виявлення помилок, діагностику несправностей і відмов та їх парирування у фундаментальне поняття – концепцію[4] відмовостійких систем (the concept of fault-tolerant systems) [20]. Це була перша наукова робота, що об'єднала два фундаментальних підходи – безвідмовність (надійність) КС та їх стійкість до відмов – у єдине поняття відмовостійкість (fault tolerance; resilience) і визначила його як «властивість архітектури цифрових систем, що дозволяє логічній машині продовжувати роботу і тоді, коли в реальній системі, що є її носієм, виникають різного роду несправності, збої та відмови компонентів». А безвідмовність є «здатність

[3] Парадигма (від грецької paradeigma – приклад, взірець, зразок) – це:
1) строга наукова теорія, що втілена у систему понять, які відображають суттєві абриси дійсності;
2) вихідна концептуальна схема, модель постановки проблем та їх вирішення; методи досліджень, що домінують протягом певного періоду у науковому товаристві.

[4] Концепція (від лат. conceptio – розуміння, система) – це змістовний спосіб розуміння або трактовки явищ; провідний задум, конструктивний принцип діяльності.
Поняття – це форма мислення, що відображає суттєві властивості, зв'язки і відношення предметів та явищ. Основною функцією П. (як у філософії, так і у логіці) є узагальнення та виділення деякого класу предметів (явищ) за визначеними загальними та у сукупності специфічними для них ознаками.

функціонального блока (системи) виконувати необхідну функцію за даних умов для заданого інтервалу часу» [21].

Головним у мотивації створення та дослідження цієї концепції було завдання NASA, що вимагало нагальної та своєчасної розробки і реалізації принципово нового «Проекту комп'ютеризованої системи управління і контролю безпілотним космічним кораблем» для міжпланетних досліджень (1958 р.). Керівником проекту був д-р А. Авіженіс, який працював тоді в Лабораторії реактивного руху (Jet Propulsion Laboratory – JPL) Каліфорнійського технологічного інституту м. Пасадена [20]. Політ планувався тривалістю понад 10 років, і надійні обчислення на борту мали стати гарантією успіху місії. Проектування відмовостійких комп'ютерів (термін введено А. Авіженісом), які б могли пережити таку тривалу подорож, а потім показати максимальну продуктивність на віддаленій планеті, було повністю непізнаною проблемою. Вивчення сутності проблеми довговічності (the long–life problem) показало, що для забезпечення необхідної надійності пропонувалася лише ідеалізована модель системи «запасна заміна», велика кількість резервних підсистем якої можуть використовуватися послідовно. Але проблема JPL полягала у тому, щоб перевести ідеалізовану модель у гідну польоту (flight – worthy) реалізацію в управляючому комп'ютері, названому «Самотестуюча та самовідновлююча система для управління і контролю (STAR)». Проект цього комп'ютера було представлено у жовтні 1961 р., а наукові та науково - технічні дослідження досягли кульмінації у конструкції та в успішній демонстрації діючої моделі комп'ютера JPL–STAR у 1971 р., що була визнана замовником придатною для 10–15-річної космічної місії [8].

Набувши неабиякого досвіду у проектуванні та реалізації одного з перших проектів діючих відмовостійких моделей КС STAR та JPL–STAR, А. Авіженіс публікує статтю «Відмовостійкі обчислення: Зверхнаміри» [22], якою започаткував нову концепцію – відмовостійкі обчислення (fault-tolerant computing). Вона стосується ролі програмного забезпечення у відмовостійкості ЕОМ і визначається як «здатність КС виконувати задані алгоритми правильно, незважаючи на відмови апаратури та помилки програм». При цьому відмовостійкі обчислення в усіх ситуативних комбінаціях негативних подій (negative evens) досягаються засобами захисної надлишковості (of protective redundancy), що визначається як така, що складається з усіх додаткових програм (програмна надлишковість), повторення операцій (надлишковість часу) і додаткових схем (апаратна надлишковість). Ідентифіковано також три головних напрями розвитку відмовостійких обчислень: 1) проектування та дослідження відмовостійких ЕОМ (W.C. Carter та W.G. Bouricius); 2) діагностування та тестування цифрових мереж (E.J. McCluskey); 3) перевірка правильності програмного забезпечення або «програмна безвідмовність» (B. Elspas та K.N. Levitt).

Ідентифікація причин «дефектних обчислень», тобто програмно-чутливих дефектів (program-sensitive faults) щодо неправильних результатів, має забезпечуватися спеціальною перевіркою «програмою доказу (program-proving) надійності». Складність такої ідентифікації полягає у тому, що вона залежить як від об'єктивних фізичних несправностей (механічне зношення і фізична деградація, внутрішні і зовнішні електромагнітні впливи та ін.), так і особливо від суб'єктивних несправностей (дефекти програми, конструкції, монтажу і наступних модифікацій, а також неправильна взаємодія людини з машиною). Тому відновлення або динамічний підхід щодо

апаратної надпишковості вимагає двох послідовних дій. Спочатку виявляється наявність несправності, а потім функція самовідновлення або ліквідує несправність, або виправляє помилку чи похибку, що була підтверджена. При цьому надлишковість вводиться селективним (вибірковим) чином, а не масово. Засобами виявлення несправностей, як уже зазначалось, є коди виявлення помилок, схеми контролю, перевірки синхронізації, дублювання і порівняння критичних функцій.

Надлишковості програмного забезпечення і часу також переймаються виявленням несправностей та самовідновленням за допомогою повторення сегмента програми, застосуванням спеціальних кодів коригування помилок і похибок, заміною дефектної частини резервом. Програмна надлишковість включає програми надзвичайних дій, які використовуються при виявленні несправності або при її підозрі. Сюди включаються також програми діагностики та тестування (що виконуються періодично або за запитом), контролюючи усі логічні схеми на присутність постійних несправностей. Повторення програми або сегмента для порівняння результатів, підключення команд-дублів та програм-перевірок достовірності також вписуються у категорію надлишковості часу.

Для порівняння ефективності методу надлишковості було досліджено також метод переконфігурації комп'ютера у нову систему без ушкодженої частини. І тут слід визнати, що обчислювальна здатність (продуктивність) його дещо знизилась, тому була допущена «часткова деградація». Такі комп'ютери можуть бути визначені як "частково відмовостійкі" (що інколи зустрічається у технічній літературі), але вони не можуть застосовуватися там, де вимагається постійна обчислювальна здатність на протязі тривалого часу або у складі комплексів управління критичними технологіями та інфраструктурами [21].

Проблема суб'єктивних несправностей (man-made faults) є загальною властивістю усіх системних відмов, спричинених помилками людей (при аналізі та синтезі, проектуванні та виготовленні, експлуатації і модернізації КС) протягом усього їх життєвого циклу (ЖЦ), тому область формального доказу або доведення правильності програм є найсучаснішим, але найменш дослідженим з усіх методів відмовостійкості. Він є найбільш стримуючим, а заодно й стимулюючим фактором щодо широкого застосування КС у критичних інфраструктурах і галузях [23].

Тут доречно зробити невелике відхилення та відзначити, що у кінці 1950-х практика розвитку принципів відмовостійкості просувалася досить мляво у зв'язку з раптовою появою напівпровідникових схем та ферит-транзисторних елементів. Надійність електронних схем зросла на декілька порядків, що дало можливість розробникам легко задовольняти практично будь-які вимоги до надійності КС без введення дорогих надлишкових засобів. У результаті поняття «відмовостійкість» почало зникати із словника і лексики розробників. Наслідки бачимо не тільки на розвитку міні- та мікро-ЕОМ, а й у таких потужних системах, як ILLIAC, CRAY, CDC та більшості сучасних вітчизняних ЕОМ. Збої та відмови, що стали менш інтенсивними, але такими ж неминучими, усувались вручну. В результаті конфлікту між реальною швидкодією і безвідмовністю такої системи, як CRAY, її середнє напрацювання до відмови (mean time to failure, MTTF) складало всього 4 год. [24, с.5], що негативно вплинуло як на її продуктивність (computer power), так і на ефективність (efficiency) в цілому та на прибутковість (profitable), зокрема [18, 25, 26].

Однак після недовготривалого, відносно повільного просування досліджень з відмовостійких обчислень уже у травні 1961р. відбулася конференція «Діагностика відмов у схемах переключення» (Conference on Diagnosis of Failures in Switching Circuits) в Мічіганському державному університеті (MSU) при спонсорстві AIEE, де мало місце широке обговорення проблеми більш ніж 50-ма провідними фахівцями під головуванням проф. R.E. Forbes. У лютому 1962р. відбувся симпозіум «Методи надлишковості для обчислювальних систем» (a Symposium on Redundancy Techniques for Computing Systems), організований Міністерством військово-морських наукових досліджень і Електрокорпорацією Вестінґхаус у м. Вашінґтон, округ Колумбія. 22 наукові доповіді відрізнялись широким світоглядом, сутністю і зрілістю поглядів та пропозицій. Деякі з них стали віхами подальшого розвитку проблеми. Разом з цим присутність близько 500 фахівців та публікація матеріалів симпозіуму [27] сприяли широкому їх розповсюдженню, що породило новий інтерес до проблеми відмовостійкості. У великій мірі цьому допомогла також сприятлива науково-технічна кон'юнктура, що спонукала до швидких і ефективних досліджень та розробок на принципах відмовостійкості у таких галузях, як:

1) електронні системи комутації (Electronic Switching System, ESS 1 – 5) фірми Bell Telephone Laboratories, нині AT&T, що прийшли на зміну електромеханічним засобам зв'язку і є найбільш численними та широко використовуваними відмовостійкими цифровими системами у світі [28]. Вони пройшли 5 етапів еволюційних змін. Але уже з появою ESS-1 [29] до них було сформульовано вимогу щодо надійності – не більше двох годин простою за 40 років служби для ручного ремонту несправності;

2) бортові процесори та ЕОМ обробки даних і управління, що створювались у зв'язку з роботами NASA у царині досліджень космічного простору: для автоматичної орбітальної астрономічної обсерваторії (ОАО) [30], для наведення ракет-носіїв Saturn 1B та Saturn V, що призначались NASA для пілотованих польотів Apollo та Skylab [31]; відмовостійкий мультипроцесор для КС управління літаками цивільної авіації FTMP [32] з універсальною для борту відмовостійкою архітектурою [33] та відповідною системою проектування і аналізу SIFT [34]. Такого типу системи віднесено до автономних або замкнутих, у яких ремонт не передбачено, і з вичерпанням ресурсів надлишковості система неминуче відмовляє. Тому для таких ІУКС основною вимогою є постійна готовність на протязі всього терміну місії без деградації функцій;

3) підвищення ефективності систем управління технологічними процесами та високоточних обчислень за рахунок високої надійності, готовності та швидкодії згаданих високопродуктивних ЕОМ типу ILLIAC-IV, IBM та міні-ЕОМ типу PDP-11 фірм DEC, H-8450 і H-700 фірми Hytati та мережевих процесорів 316 і 516 фірми Honeywell. Прикладами таких систем того часу є відмовостійка КС COMTRAC (COMputer – aided Traffic Control system) [35] для управління рухом швидкісних поїздів «Сінкан сен» на залізницях Японії та Pluribus – відмовостійкий операційний мультипроцесор [36].

Таким чином, дві попередні конференції (1961 і 1962 рр.), доповнивши одна одну, високо підняли рівень вимог щодо подальших досліджень. А у грудні 1965 р. на симпозіумі IEEE «Безвідмовність в проектуванні систем» (Reliability in System Design) у м. Фоенікс, шт. Арізона (18 наукових доповідей, голова – W.C. Carter) і відразу ж у лютому 1966р. на симпозіумі IEEE/UCLA «Організація безвідмовних автоматів» (The Organization of Reliable Automata) у м. Лос-Анджелесі (30

наукових доповідей) з усіх аспектів відмовостійкості; голова – A. Avizienis) зусиллями фахівців різних країн у галузі відмовостійкості і відмовостійких обчислень було прискорено рух до досягнення цього рівня.

На цих симпозіумах проводився ґрунтовний науковий пошук забезпечення надійності систем способами, альтернативними до відмовостійкості. Таким способом могло б стати лише повне запобігання несправностей, що вимагає створення таких фізичних компонентів і методів їх збірки, які були б максимально близькими до ідеально безвідмовних. Тобто, якщо в КС постійно відбуваються випадкові відмови з інтенсивністю λ за проміжок часу t і надійність системи визначається як $R(t) = e^{-\lambda t}$, то єдиний спосіб зробити таку систему надійнішою – зменшити λ до нуля. Але цей підхід передбачає повне екранування від усього різноманіття зовнішніх і внутрішніх завад. А це, по-перше, вимагає технологій наближення компонентів до майже ідеальних і веде до непомірного зростання їх вартості [25, 26], по-друге, такий підхід дозволяє суттєво знизити інтенсивність появи несправностей, однак на цьому шляху ще ні разу не вдавалось запобігти усім несправностям, зважаючи на природну фізику деградації конструкцій елементів, і, по-третє, оскільки при першій же відмові або збої закінчується нормальне функціонування системи, то принципово неможливе створення автономних ІУКС закритого типу.

Головним переконливим доказом на користь повсюдного використання відмовостійкості замість виключного застосування принципу повного запобігання несправностям є те, що початкові «надмірні» витрати капіталу для забезпечення стійкості до несправностей суттєво знижують загальні витрати на систему за весь термін її служби. Інші, не менш важливі та сильні аргументи, буде викладено нижче. Але в будь-якому випадку досягати цілей при створенні ІУКС з найбільшою ефективністю можливо лише зберігаючи раціональність переваг обох підходів [26].

Результати висновків і рішень симпозіумів середини 60-х жваво обговорювались у журнальних статтях, JCC та на конференціях і симпозіумах, число яких швидко зростало. Це привело до Об'єднаного комп'ютерного конгресу AFIPS '67, на якому (як уже згадувалося [20]) А. Авіженісом було започатковано нове поняття – концепцію відмостійких систем. Цьому сприяла також оцінка стану проблеми відмовостійкості в середині 1967р., наведена в головному дослідженні – огляді Р.А. Шорта «Досягнення надійності цифрових систем за допомогою надпишковості» [36]. Була оцінена також головна подія у галузі моделювання надійності – введення У.Г. Боурісіусом, У.С. Картером і П.Р. Шнайдером поняття міри покриття (охоплення) або ступеня компенсації відмов [37], визначеного як вірогідність відновлення системи при наявності відмови. Ними доведено, що ця міра є єдиним параметром у проектуванні безвідмовності ІУКС, бо зміна її від 1 до 98 є її межею. Інші методи підвищення безвідмовності за рахунок збільшення резерву є дуже слабкими перед мірою компенсації, не адекватною 99. Для поліпшення міри компенсації відмов більш ефективними є методи доповнення перевірок, тестування, діагностики і доведення причини відмови та реагування на можливі наслідки.

У галузі програмної відмовостійкості на конгресі з ініціативи Б. Ранделла була задекларована оригінальна робота «Системна структура для програмної відмовостійкості», суттєво розширена версія якої була опублікована пізніше [38, 39]. Оцінюючи показники міри компенсації щодо жорстких обмежень методу безвідмовності та проблеми із введенням надлишковості,

аргументовано викладені у працях [36, 37], Б. Ранделл спочатку сам, а згодом з П. Лі і П. Трілівном та колегами з Лабораторії обчислень Ньюкаслського університету (Англія) прискіпливо дослідили різні вимоги, що включаються для досягнення високої безвідмовності, та особливості архітектури, які дозволяють суттєво зменшити складність розподіленої ІУКС. Розглядаються співвідношення між методами структурування системи і методами відмовостійкості, що охоплюють такі теми: 1) захисна надлишковість в апаратних і програмних засобах; 2) використання елементарних операцій функціонування ІУКС та оптимізації потоків інформації; 3) методи виявлення несправностей; 4) стратегії знаходження місць несправностей та боротьби з ними і оцінка збитків; 5) методи відновлення, що ґрунтуються на концепціях: шляхи відновлення, блокування, виключення і компенсації. Досліджені методи актуальні й досі.

У подальшому розвиток концепції програмної відмовостійкості було доповнено ефективним методом N – версійного програмування, запропонованим спочатку [40] як метод багатократних обчислень для успішної боротьби з фізичними несправностями. Він став фундаментальним для досягнення відмовостійкості в цілому: багатократні обчислення N -кратним $(N \geq 2)$ дублюванням у трьох областях – часу (повторення) T, простору (апаратні засоби) H та інформації (програмне забезпечення) S. Для безвідмовної (одноканальної або симплексної) системи характерним виконанням є 1T/1H/1S (тобто симплексні: час–1T, апаратура–1H і програми–1S). І якщо в безвідмовній системі передбачено виявлення випадкових помилок, наприклад, методом повторення стану системи від «точки зворотної перемотки», то схема буде 2T/1H/1S, де додано час для відновлення роботи. В багатоканальній архітектурі [41] мають місце схеми від NT/NH/NS (наприклад, для човника NASA, де $N = 4$ [42]) до схем типу NT/YH/ZS. Наведений метод багатократних обчислень було розвинуто в один із базових підходів N -версійного програмування для забезпечення гарантоздатних обчислень як атрибута відповідних комп'ютерних систем.

Суттєве спрощення складності розподіленої ІУКС пов'язують з розвитком методів мініатюризації технічних засобів, проектуванням надвеликих інтегральних схем НВІС, МП та із структурною реалізацією складного програмного забезпечення на зразок того, як аналогічні обставини призвели до розробки діагностичних програм та теорії машинної діагностики, що стала основним засобом усунення несправностей ЕОМ при ручних методах обслуговування. У 70-х роках широкого розповсюдження набула структурна інтерпретація мови високого рівня на основі засобів мікропрограмного управління спеціальними та універсальними ЕОМ [43–47]. У ці роки на зміну діагностичним програмам прийшла мікродіагностика, яка й стала частиною системного забезпечення ЕОМ, що виконувало основні функції з виявлення і усунення несправностей та відновлення її роботи, чим ефективно підтримало відмовостійкість обчислень.

У той же час виникла нагальна потреба координації швидко зростаючих теоретичних і прикладних досліджень у наведених галузях. Вона й привела до заснування у травні 1970 р. Технічного комітету Комп'ютерних систем IEEE з відмовостійких обчислень (the IEEE-CS TC on Fault-Tolerant Computing). Усі три головні галузі – проектування і дослідження, діагностування і тестування та безвідмовність ПЗ – стали сферою інтересів цього ТК. Членство в ньому було відкрито для усіх бажаючих комп'ютерних спеціалістів. Першими результатами його діяльності є

організація спеціального видання журналу «КОМП'ЮТЕР і Симпозіум з Відмовостійких обчислень» у березні 1971 р.

Підводячи підсумок 25-річних досліджень з часу проведення Першого міжнародного симпозіуму з надійності ЕОМ (1953 р.) та аналізуючи рівень розвитку парадигми відмовостійкості у тематичному випуску збірника [18], шеф-редактор А. Авіженіс з гіркотою пише: «До цього часу створено лише декілька у повному сенсі відмовостійких систем. Більшості ж сучасних цифрових установок бракує автоматичного відновлення нормальної роботи після виникнення несправності і необхідна допомога фахівця. Традиції ручного методу обслуговування вкоренились настільки глибоко, що лише поява непомірних вимог до надійності та готовності систем змусила впроваджувати принципи відмовостійкості». До таких у США відносяться вже згадані JPL-STAR (1967–1971рр.); електронна система комутації ESS №1, №2 і №3 (1959 – 1975рр.) фірми Bell Telephone Laboratories; FTCS Raytheon Mfg Co; високонадійний відмовостійкий мультипроцесор FTMP (1965 р.) і відповідне йому ПЗ відмовостійкісних обчислень SIFT (1970 р.) для керування літальними апаратами; мультипроцесорна система високої готовності Pluribus для спеціальної міжнародної мережі (ARPA network [48]), створеної на базі відмовостійкого інтерфейного процесора повідомлень (interface message processor-IMP), який постійно контролює і керує операціями передачі даних мережі у віддалених автономних пунктах (1972 – 1975 рр.); відмовостійкі КС COMTRAC для швидкісного руху залізницями Японії, які мають постійний коефіцієнт готовності 99,99%. Багаторічна напружена робота Центру досліджень ім. Т. Дж. Уотстена фірми IBM хоча і не привела до побудови повністю відмовостійкої системи, але дала фундаментальні результати у питаннях загальних принципів архітектури [49], теорії діагностики [50], моделювання надійності [37], теорії застосування схем із самоперевіркою [51] та ін. Починаючи з 1970 р., великі експериментальні дослідження з відмовостійкості та безвідмовності багатопроцесорних систем проводяться в Університеті Карнегі-Меллона [18].

В Європі (Чехословаччина) реалізована перша у світі повністю відмовостійка 32-розрядна з плаваючою комою і пам'яттю на магнітних барабанах релейна машина SAPO (1956 р.). У ній центральний процесор має потрійне модульне резервування з голосуванням результатів. Машина розроблена у 1950 – 1954рр. під керівництвом проф. Антоніна Свободи, який повернувся у 1946 р. до Праги з Масачусетського технологічного інституту. За першою релейною ним реалізована наступна десяткова електронна машина EPOS (1962 р.) на електронних лампах з феритовою пам'яттю, в якій також широко використовувались заходи забезпечення відмовостійкості [52–54]. Крім того, в Європі реалізовані ще дві французькі розробки: MECRA [55] та COPRA [56], архітектура яких включає безвідмовний комп'ютер із самовідновлюванням за рахунок набору (сімейства) модулів рекомбінації та автоматичних методів повторних прогонів після автоматичного усунення несправностей закритих КС для авіаційних та космічних апаратів.

Таким чином, організація складних КС здійснювалась на базі відмовостійкого однопроцесорного комп'ютера (інтелектуального «ядра») з дублюванням чи резервуванням цих КС у більш складні, але громіздкі архітектури. Природно, що це давало потенційним споживачам привід для сумніву у довгоживучості таких систем і дещо стримувало їх застосування. Але накопичений досвід системного застосування методів відмовостійкості став реалізовуватися за допомогою нових

технологій мікромініатюаризації апаратури засобами мікроелектроніки, що бурхливо розвивалась [57]. Виявлення та усунення несправностей за допомогою схем із самоперевіркою легко реалізуються у надвеликих інтегральних схемах (ВІС). Це різко підвищило ступінь компенсації відмов і було сприйнято як «здіснення універсальної відмовостійкості шляхом масштабної інтеграції» [58].

Однак висновки авторів [59] та [60] з багаторічною практикою наукових і прикладних досліджень переконливо довели, що навіть з появою «всесильних» НВІС і мікропроцесорів (МП) проблему забезпечення універсальної відмовостійкості не можна вважати вирішеною ні на системному рівні, ні на рівні приладів [60]. Тут існує цілий ряд невирішених задач, а саме: 1) зростаюча складність функцій, що реалізуються НВІС у рамках одного кристалу, вимагає робити відмовостійкими самі кристали і означає, що напрацьовані механізми відмовостійкості необхідно переносити на рівень приладів; 2) така задача є принципово новою для виробників напівпровідникових приладів і не може бути вирішена простим поширенням традиційних правил і норм системного проектування на рівень приладів; 3) відмовостійкі КС ще не випускались масово і часто були вузько спеціалізованими; 4) на противагу, розробки НВІС і МП повинні мати універсальну відмовостійкість у зв'язку з їх масовістю та широким діапазоном застосування; 5) найбільш критичною є задача, яка полягає у набутті глибокого розуміння сутності всіх несправностей, що підлягають нейтралізації у відмовостійких МП. Їх класифікація і осягнення сутності та наслідків вимагають інтенсивного вивчення й аналізу нової напівпровідникової технології та, очевидно, розробки і дослідження нових підходів, методів і засобів щодо проектування їх високонадійних компонент. Так виникла ідея передачі технології створення відмовостійких КС із галузі апаратних засобів у сферу систем програмного забезпечення, яка б гарантувала високу безвідмовність проектування, виготовлення, контролю та атестації виробництва високоякісних великих інтегральних схем (ВІС), НВІС та МП широкого вжитку. Цей метод отримав назву гарантоздатних обчислень (dependable computing) як основи фундаментальної концепції гарантоздатності (dependability), введеної А. Авіженісом та Ж.-К. Лапрі в роботі [61]. В передмові до перекладу збірника [60] Є.К. Масловський звертає увагу на те, що «…статті у збірнику містять ідеї, цінні для передачі технології створення відмовостійких систем… у сферу систем програмного забезпечення, де аналогічні проблеми у нас поки що, на жаль, просто ігноруються розробниками». І тут же додає: «Основная трудность перевода данного тематического выпуска была связана именно с терминологией, поскольку авторы чётко различают, например, такие понятия, как fault-tolerance (отказоустойчивость), fault security (отказобезопасность), fault-avoidance (предотвращение неисправностей); вкладывают разный смысл в fatal failure (фатальный отказ) и catastrophic failure (катастрофический отказ); трактуют термин dependability (гарантоспособность) как более общий по отношению к reliability (безотказность, надёжность). Эта упорядоченная терминология… является полезной как для новичков в области отказоустойчивости, так и для «специалистов со стажем».

Природно, що нова галузь науково-технічної діяльності (початок її співпадає з виникненням мікроелектроніки, яка стрімко розвивається) породжує нову термінологію, що потребує певних узгоджень та стандартизації понять. Тому природним було створення у 1980 р. робочої групи (WG 10.4) «Гарантоздатні обчислення та відмовостійкість» IFIP, яка суттєво прискорила появу

несуперечливого набору атрибутів, понять і термінології концепції гарантоздатності. Ця робота була проведена у структурі підкомісії FTCS-12 «Фундаментальні поняття і термінологія» WG 10.4 IFIP та в ТК «Відмовостійкі обчислення» IEEE. Її початком були положення семи наукових доповідей на Спеціальній сесії «Фундаментальні концепції відмовостійкості» у 1982 р. На ній було розглянуто подані під різним кутом зору пропозиції концепції, розробленої кількома незалежними міжнародними колективами дослідників. Подальші їх версії детально обговорювались та розвивались на зимовій і літній сесіях WG 10.4 IFIP у 1983 та 1984 рр. У 1985р. Ж.-К. Лапрі синтезував їх у систему концептуальних властивостей, що визначають гарантоздатні та відмовостійкі обчислення, у своїй праці [61]. У ній гарантоздатність (dependability) вперше визнається глобальним поняттям з акцентом на інтеграцію системи супідрядних понять з мінімальною кількістю визначень їх сутності [62]), де відмовостійкість (fault-tolerance) є її деталізацією, а надійність (reliability) є одним із її атрибутів[5]. Були спроби розглянути поняття гарантоздатності як більш загальне щодо надійності, готовності та ін. [63], але з меншою мірою узагальнення, бо мета їх – лише визначення кількісної міри властивості.

Потреба введення терміна «гарантоздатність» як узагальненого універсального поняття пояснюється двома причинами: по-перше – усунути плутанину між поняттям надійності як загального значення (властивість надійної системи) і надійністю як математичною кількісною величиною, що характеризує міру надійності системи, і по-друге – показати, що терміни існуючого довгого списку є лише кількісними характеристиками – мірами різних проявів однієї і тієї ж властивості системи – її гарантоздатності. Звідси й її попереднє визначення як поняття, що розвивається: гарантоздатність обчислювальної системи – це «її властивість надавати споживачам постійне обслуговування та узгоджені специфікацією[6] послуги, яким можна виправдано довіряти».

Далі членами WG 10.4 IFIP під керівництвом Ж.-К. Лапрі після тривалого та інтенсивного обговорення була підготовлена і видана у 1992р. книга «Фундаментальні поняття і термінологія» [64], яка включає 34 друкованих аркуші англійського тексту та класифікатор (глосарій) на 8 сторінках з перекладами на французьку, німецьку, італійську та японську мови. Основною її новизною стало включення поняття безпеки (addition of security) як атрибута гарантоздатності, а також класу навмисних зловмисних несправностей (доступ без санкцій, злого наміру, вторгнення), введеного поряд із випадковими (фізичними, проектними та взаємодії) помилками. Наступним головним кроком було визнання атрибута безпеки комбінацією атрибутів конфіденційності, цілісності та готовності з доповненням класу навмисних незловмисних несправностей разом із аналізом проблем неадекватних системних специфікацій [65].

Зазначимо, що науково-дослідна робота з інтеграції відмовостійкості і захисту від навмисного пошкодження (загрози безпеці ІУКС) розпочата у середині 80-х років [66–68]. Тому наступною важливою віхою на шляху інтеграції існуючих понять якостей КС стала Перша робоча конференція IFIP з гарантоздатних обчислень для критичних застосувань (The first IFIP Working Conference on Dependable Computing for Critical Applications), що відбулася у 1989 р. Ця і шість

[5] Атрибут – (від лат. attributo – надаю; наділяю) необхідна, суттєва, притаманна йому властивість об'єкта.

[6] Специфікація (системна) – офіційний нормативний документ з чітким і точним перерахуванням подробиць, на які необхідно звернути особливу увагу (наприклад, при створенні та проектуванні системи).

наступних Робочих конференцій сприяли проясненню проблем взаємозв'язку гарантоздатності обчислень та захисту комунікацій, а також інтегрували захист (цілісність, конфіденційність і готовність) в інтелектуальні структури (framework – блоки даних штучного інтелекту) гарантоздатних обчислень [3]. При цьому чітко розмежовуються (структуруються) ненавмисно зловмисні несправності та зловмисно навмисні дії, де перші є результатом неприпустимої системної поведінки в результаті допущених помилок специфікаторами, проектувальниками, конструкторами або взаємодією людини і системи, а другі мають несправності двох класів: а) зловмисні логіки (malicious logics) [69] та б) вторгнення (intrusions) – як внутрішні, так і зовнішні фізичні втручання, від яких потрібний ефективний захист.

Тобто, користувачі ІУКС (і не тільки критичних галузей) потребують впевненості у гарантованому захисті систем, що використовуються ними. Вони також потребують чітких та гарантованих критеріїв оцінки для порівняння можливостей такого захисту продуктів інформаційних технологій (ІТ –продуктів), які вони збираються придбати. Щоб така оцінка була адекватною, необхідно мати незалежний сертифікаційний орган, який би міг засвідчити, що оцінка проведена відповідним чином. Цілі безпеки ІТ-системи, як і її гарантоздатність, мають бути специфічними до конкретно визначених вимог користувачів системи та умов середовища експлуатації і мають підтверджуватися методами відповідної акредитації.

У той же час концепція захисту (security&safety) до середини 80-х років розвивалася незалежно від розвитку концепції гарантоздатності (dependability), але оскільки вони тим чи іншим чином спиралися на теорію, методи і засоби одна одної, то, очевидно, що вони є ніби «дві сторони однієї медалі» і, природно, мають інтегруватися в єдине глобальне поняття. Але, як виявилось, це є досить відповідальним і тривалим процесом у зв'язку з тим, що поняття безпеки є складним і багатогранним, воно включає комбінації таких ознак як: 1) конфіденційність (попередження неправомірного розкриття інформації); 2) цілісність (попередження неправомірного видалення інформації); 3) готовність (попередження неправомірної відмови в інформації). Крім наведених, безпека визначає і вторинні ознаки. Наприклад, спеціалізація вторинної ознаки – робасність, тобто гарантоздатність відносно зовнішніх помилок, що характеризує системну реакцію на визначений клас несправностей. Термін вторинних ознак має особливий сенс для безпеки, коли розрізняють такі типи інформації, як відповідальність, справжність, невідмова та ін. А ще існують такі поняття, як життєздатність та кредитоздатність, що мають бути приведеними до показників міри гарантоздатності як категорії понять прогнозованості (performability) – ефективність, продуктивність і старанність [56] – та передбачуваності [65] і т.п.

У результаті енергійних дій, вжитих Технічними комітетами IFIP, та широкого міжнародного обговорення у червні 1991р. вийшла з друку тимчасово узгоджена версія 1.2 «Критерії оцінки безпеки Інформаційних технологій» (1.2 ITSEC) [70] для використання в експлуатації та оцінки в системах сертифікації країнами-учасницями і всіма бажаючими. Набутий практичний досвід буде використано для обговорення та подальшої розробки. Крім того, зауваження і пропозиції будуть взяті до уваги та подальшого міжнародного узгодження. Критерії, що регламентуються цим документом, в основному стосуються заходів технічної безпеки і направлені

на деякі нетехнічні аспекти, такі як захисні операційні процедури для персонального, фізичного та процедурного захисту (але тільки там, де це стосується засобів технічного захисту).

При розробці критеріїв оцінки ІТ-захисту було проведено значний обсяг робіт з вивчення потреб і вимог країн-учасниць та їх органів акредитації, які дещо відрізняються. Найважливіші з них, що передували масштабним розробкам, взяті за основу. Це «Критерій оцінки надійної комп'ютерної системи», відомий як TCSEC або «Orang book» («Помаранчова книга»), видана для оцінки продукту Департаментом безпеки США. Інші країни, в основному європейські, також мають великий досвід в оцінці ІТ-безпеки. В Британії це Меморандум № 3 (CESG 3), що використовується урядовим Департаментом торгівлі і промисловості, та «Зелена книга» (DTIEC) для ІТ-захисту комерційних продуктів. У Німеччині Національне інформагентство безпеки видало у 1989 р. першу версію власного Критерію захисту продукції (так званого ZSIEC). Розроблено критерії і у Франції – «Голуба – біло – червона книга» (SCSSI) та ін.

З огляду на перспективність досліджень, Франція, Англія, Нідерланди та Німеччина визнали необхідність подальшої співпраці у розробці погоджених загальних критеріїв ІТ-безпеки на базі документа ITSEC при максимальній сумісності з TCSEC [65]. Це забезпечить спільний базис сертифікації національних сертифікатів у повному обсязі з об'єктивним міжнародним рішенням про взаємні визнання оцінок результатів. Для цього є принаймні три важливі причини: а) у різних країнах накопичено свій значний досвід, а тому найкраще – спільно опиратися на нього; б) сучасна промисловість уже не хоче мати різні критерії у різних країнах; в) у всіх країнах та у всіх комерційних, урядових і оборонних застосуваннях будуть однакові основні концепції і підходи для рівноправної конкуренції.

Не відстають від інтеграційних процесів і Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (МЕС), які в ІТ-галузі заснували Об'єднаний ТК (ISO/MEC JTC1, Інформаційна технологія, Підкомітет SC1, Словник) [71]. Ними у 1997р. підготовлена друга редакція стандарту ISO/MEC 2382 обсягом близько 35-ти частин під загальною назвою: Інформаційна технологія – Словник (ISO/MEC 2382 will consist of 35 parts, under the general title Information technology – Vocabulary) на заміну першої редакції (ISO 2382; 1978). Метою Словника є стандартизація термінології, визначень і таксономії в ІТ-галузі, включаючи життєвий цикл, життєздатність, безпеку, кредитоздатність та інші фундаментальні атрибути гарантоздатності і безпеки як глобального інтегруючого підходу.

3. Висновки

Безумовні успіхи окреслених вище інтеграційних процесів, завдяки енергійним зусиллям зазначених Міжнародних наукових і науково-технічних організацій і товариств, урядів 32-х країн-учасниць та підрозділів акредитації і особливо їх провідних університетів, спонукали до активних дій провідні корпорації, що є виробниками сучасної ІТ-індустрії. Показовим прикладом цього є заява Крейґа Манді (Craig Mundie) – старшого віце-президента Microsoft і керівника стратегічної програми під назвою «Захищені інформаційні системи» (Trustworthy Computing) на конференції RSA (Conference '2002) у м. Сан-Хосе (штат Каліфорнія, США) дослівно: «Ми провели глибоку, докорінну переорієнтацію корпорації, щоб зробити цю програму нашим пріоритетом номер один, без усяких

виключень. За своєю природою – це складна, довгострокова задача, на розв'язання якої IT-індустрія може затратити років десять і більше. Безпека – ключова складова того, що ми називаємо захищеними інформаційними системами, але тільки одна із багатьох – поряд з конфіденційністю, готовністю до роботи, безвідмовністю та цілісністю. Захищені інформаційні системи – це такі системи, які так само готові до роботи, безвідмовні та захищені, як і електроенергія, водопостачання або телефонний зв'язок. І це першочергова довгострокова ціль для усієї корпорації Microsoft» [72].

СПИСОК ЛІТЕРАТУРИ

1. Димлевич Н. Киберпространство: новые угрозы / Н. Димлевич // R&D.News. – 2009. – № 1. – С. 13 – 21.
2. Jones A. The Challenge of Building survivable information-intensive systems / A. Jones // IEEE Computer. – 2000. – Vol. 33, № 8. – P. 39 – 43.
3. Avizjienis A. Fundamental Concepts of Dependability / A. Avizjienis, J.-C. Laprie, B. Randell // IEEE Computer. – 2000. – № 10. – 16 p.
4. Гутер Р.С. Новое в жизни, науке и технике / Гутер Р.С., Полупанов Ю.Л., Бэббедж Ч. – Серия Математика, кибернетика. – М.: Знание, 1973. – 64 с.
5. First draft of a report on the EDVAC fulfilled by John von Neumann for Contract № W-670-ORD-4926. – USA, 1945. – P. 43.
6. Дж. фон Нейман Теория самовоспроизводящихся автоматов / Дж. фон Нейман; пер. с англ. В.Л. Стефанюка; под ред. В.И. Варшавского. – М.: Мир, 1971. – 384 с.
7. Вычислительные машины (СЕАК и ДИСЕАК) Национальное бюро стандартов США / Под ред. В.М. Тарасевича. – М.: Государственное научно–техническое издательство машиностроительной литературы, 1958. – 208 с.
8. The STAR (Self – Testing – and – Repairing, STAR) Computer: An Investigation of the Theory and Practice of Fault –Tolerant Computer Design / A. Avizjienis, G.C. Gilley, F.P. Mathur [et al.] // IEEE Trans. Computers. – 1971. – Vol. C-20. – P. 1312 – 1321.
9. Винер Н. Кибернетика или управление и связь в животном и машине / Винер Н. – М.: Советское радио, 1958. – 214 с; Wiener N. Cybernetics of Control and Communications in the Animal and the Machine. The Technology Press and John Wiley & Sons, Inc. / N. Wiener. – New York – Hermann et Cie, Paris, 1948. – 193 p.
10. Винер Н. Кибернетика или управление и связь в животном и машине / Винер Н. – 2-е изд. – М.: Наука, 1983. – 340 с.; Wiener N. Cybernetics of Control and Communications in the Animal and the Machine / N. Wiener. – 2-nd ed. – The M.I.T. Press and John Wiley & Sons, Inc., New York – London, 1961. – 230 p.
11. Глушков В.М. О некоторых задачах вычислительной техники и связанных с ними задачах математики / В.М. Глушков // Украинский математический журнал. – 1957. – Т. 9, № 4. – С. 369 – 376.
12. Глушков В.М. Абстрактная теория автоматов / В.М. Глушков // Успехи математических наук. – 1961. – Т. 16, № 5. – С. 3 – 62.
13. Глушков В.М. Самоорганизующиеся системы и абстрактная теория автоматов / В.М. Глушков // Вычислительная математика и математическая физика. – 1962. – № 3. – С. 459 – 466.
14. Глушков В.М. Введение в теорию самосовершенствующихся систем / Глушков В.М. – Киев: Издательство КВИРТУ, 1962. – 109 с.
15. Глушков В.М. Синтез цифровых автоматов / Глушков В.М. – М.: Физматгиз, 1962. – 476 с.
16. Глушков В.М. Введение в кибернетику / Глушков В.М. – Киев: Издательство АН УССР, 1964. – 324 с.
17. Капітонова Ю.В. Парадигми та ідеї академіка В.М. Глушкова / Ю.В. Капітонова, О.А. Летичевський. – Київ: Наукова думка, 2003. – 456 с.
18. Avizienis A. Fault-Tolerance: The survival attribute of digital system / A. Avizienis // Proc. of the IEEE. – 1978. – Vol. 66, N 10. – P. 1109 – 1125; Авиженис А. Отказоустойчивость – свойство, обеспечивающее постоянную работоспособность цифровых систем / А. Авиженис; пер. с англ. // ТИИЭР. – 1979. – Т. 66, № 10. – С. 5 – 25.
19. Нейман Дж. Вероятностная логика и синтез надежных организмов из ненадёжных компонент / Дж. Нейман // Автоматы. – М.: ИЛ, 1956. – С. 68 – 139.
20. Avizienis A. Design of fault-tolerant computers / A. Avizienis // Proc. 1967 AFIPS Fall Joint Computer conf., AFIPS Proc. conf. – 1967. – Vol. 31. – P. 733 – 743.
21. Інформаційні технології. Словник термінів. Частина 14. Безвідмовність, ремонтопридатність та готовність (ISO/IEC 2382 – 14:1997, IDT): ДСТУ 2668 – 2005. – Київ: Держспоживстандарт України, 2007. – 20 с. (Національний стандарт України).
22. Avizienis A. Fault-Tolerant Computing: An Overview / A. Avizienis // COMPUTER. – 1971.– N 5. – P. 5 – 8.
23. Avizienis A. Fault-Tolerant Computing: Progress, problem, and prospects / A. Avizienis // Proc. IFIP Congress '77. – Toronto, Canada, 1977. – P. 405 – 420.
24. Погребинский С.Б. Проектирование и надёжность многопроцессорных ЭВМ / С.Б. Погребинский, В.П. Стрельников. – М.: Радио и связь, 1988. – 168 с.
25. Дослідження комплексу проблем архітектурної, структурної та технологічної організації високопродуктивних обчислювальних засобів (ВОЗ) для роботи в умовах жорстких обмежень / Б.Г. Мудла, О.М. Шалейко, Г.С. Теслер [та ін.]: Звіт з НДР. – Шифр "Обмеження"; Інв. № 125. – К.: ІПММС НАНУ, 1999. – 157 с.

26. Дослідження відмовостійких обчислювальних засобів у критичних інформаційних системах обробки інформації і керування об'єктами на основі мережної взаємодії / Б.Г. Мудла, О.М. Шалейко, Г.С. Теслер [та ін.]: Звіт з НДР. – Шифр "Відмовостійкість"; № Держобліку 0204U006760. – К.: ІПММС НАНУ, 2004. – 264 с.
27. Wilcox R.H. Redundancy Techniques for Computing Systems / R.H. Wilcox, W.C. Mann. – Washington: Spartan Press, Inc., D.C., 1962. – 234 p.
28. Toy W.N. Fault-Tolerant design of local ESS processors / W.N. Toy // Proc. of the IEEE. – 1978. – Vol. 66. – P. 1126 – 1145.
29. Downing R.W. N1 ESS: maintenance plan / R.W. Downing, J.S. Novak, L.S. Tuomenoksa // Bell Syst. Tech. J. – 1964 – Vol. 43, N 5. – Part 1. – P. 5 – 12.
30. Kuehn R.E. Computer redundancy: Design, performance and future / R.E. Kuehn // IEEE Trans. on Reliability. – 1969. – Vol. R-18, N 1. – P. 3 – 11.
31. Cooper A.E. Development of on-board space computer systems / A.E. Cooper, W.T. Chow // IBM, J. Res. Devel. – 1976. – Vol. 20, N 1. – P. – 3 – 11.
32. Hopkins A.L. FTMP – a highly reliable fault-tolerant multiprocessor for aircraft / A.L. Hopkins, T.B. Smith III, J.H. Lala // Proc. of the IEEE. – 1978. – Vol. 66, N 10. – P. 1221 – 1239; Хопкинс А.Л. FTMP – высоконадежный устойчивый к отказам мультипроцессор для управления самолётом / А.Л. Хопкинс, Т.Б. Смит III, Дж. Х. Лала; пер. с англ. // ТИИЭР. – 1979. – Т. 66, № 10. – С. 142 – 165.
33. Rennels D.A. Architectures for fault-tolerant spacecraft computers / D.A. Rennels // Proc. of the IEEE. – 1978. – Vol. 66, N 10. – P. 1255 – 1268; Реннелс Д.А. Архитектура космических бортовых вычислительных систем, устойчивых к отказам / Д.А. Реннелс; пер. с англ. // ТИИЭР. – 1979. – Т. 66, № 10. – С. 186 – 205.
34. SIFT: Design and analysis of a fault-tolerant computer for aircraft control / J.H. Wensley, L. Lamport, J. Goldberg et al. // Proc. of the IEEE. – 1978. – Vol. 66, N 10. – P. 1240 – 1255; SIFT: Проектирование и анализ отказоустойчивой вычислительной системы для управления полётом летательного аппарата / Дж.Х. Уэнсли, Л. Лэмпорт, Дж. Голдберг и др.; пер. с англ. // ТИИЭР. – 1979. – Т. 66, № 10. – С. 166 – 186.
35. Fault-Tolerance Computing System with Three Symmetric Computers / H. Ihara, K. Fukuoka, Y. Kubo [et al.] // Proc. of the IEEE. – 1978. – Vol. 66, N 10. – P. 1160 – 1177; Отказоустойчивая вычислительная система с тремя симметричными вычислительными машинами / Х. Ихара, К. Фукуока, Ю. Кубо и др.; пер. с англ. // ТИИЭР. – 1979. – Т. 66, № 10. – С. 68 – 89.
36. Short R.A. The Attainment of Reliable Digital Systems Through the Use of Redundancy – a Survey / R.A. Short // IEEE Computer Group News. – 1968. – Vol. 2, N 2. – P. 2 – 17.
37. Bouricius W.G. Reliability modeling techniques for self-repairing computer systems / W.G. Bouricius, W.C. Carter, P.R. Schneider // Proc. 24th National Conference of ACM. – 1969. – P. 295 – 309.
38. Randell B. System structure for software fault tolerance / B. Randell // IEEE Transctions on Software Engineering. – 1975. – Vol. SE-1, N 10. – P. 1220 – 232.
39. Randell B. Reliability Issues in Computing System Design / B. Randell, P.A. Lee, P.C. Treleaven // Computing Surveys. – 1978. – Vol. 10, N 2. – P. 123 – 165.
40. Avizienis A. On the implementation of N-version programming for software fault tolerance during execution / A. Avizienis, L. Chen // Proc. IEEE COMPSAC '77. – 1977. – P. 149 – 155.
41. Avizienis A. The N – Version Approach to Fault – Tolerance Software / A. Avizienis // IEEE Transactions on Software Engineering. – 1985. – Vol. SE-11, N 12. – P. 1491 – 1501.
42. Sklaroff J.R. Redundancy management technique for space shuttle computers / J.R. Sklaroff // IBM J. Res. Develop. – 1976. – Vol. 20. – P. 20 – 28.
43. Глушков В.М. О применении абстрактной теории автоматов для минимизации микропрограмм / В.М. Глушков // Известия АН СССР. Техническая кибернетика. – 1964. – № 1. – С. 3 – 12.
44. Глушков В.М. Теория автоматов и формальные преобразования микропрограмм / В.М. Глушков // Кибернетика. – 1965. – № 5. – С. 1 – 9.
45. Глушков В.М. Вычислительная машина "Киев" / В.М. Глушков, Е.Л. Ющенко. – Киев: Гостехиздат, 1962. – Т. II. – 181 с.
46. Мудла Б.Г. Становлення і розвиток теоретичних та науково-практичних засад створення високо інтегрованих мобільних (бортових) машин, систем і комплексів реального часу / Б.Г. Мудла // Математичні машини і системи. – 2008. – № 3. – С. 23 – 61.
47. Weber H. A microprogramming implementation of EULER on IBM System/360 Model 30 / H. Weber // Comm. ACM. – 1967. – Vol. 10, N 9. – P. 37 – 49.
48. Heart F.E. The ARPA network / F.E. Heart; R.L. Grimsdale, F.F. Kuo (eds.) // Computer Communication Networks. – Leyden, The Netherlands; Noordhoff Int.Publ., 1975. – P. 19 – 23.
49. Logic design for dynamic and interactive recovery / W.C. Carter [et al.] // IEEE Trans. Computers. –1971. – Vol. C-20, N 11. – P. 1300 – 1305.
50. Algorithms for detection of faults in logic circuits / W.G. Bourisius [et al.] // IEEE Trans. Computers. –1971. – Vol. C-20, N 11. – P. 1300 – 1305.
51. Cost effectiveness of self checking computer design / W.C. Carter [et al.] // Proc. FTCS-7: Seventh Annual Int. Conf. Fault-Tolerant Computing. – Los Angeles, CA, 1977. – P. 117 – 123.
52. Oblonsky J. Some features of the Czechoslovak relay computer SAPO / J. Oblonsky // Nachrichtentechnische Fachberichte. – 1956. – Vol. 4. – P. 73 – 75.
53. Svoboda A. Logical design of a data-processing system with built-in time sharing / A. Svoboda, J. Oblonsky // Inform. Processing Mashines. – 1963. – Vol. 9. – P. 15 – 24.
54. Oblonsky J. A self-correcting computer / J. Oblonsky // Digital Information Processors. – New York: Interscience, 1962. – P. 533 – 542.

55. Maison F.P. The MECRA: A self-repairable computer for highly reliable process / F.P. Maison // IEEE Trans. Computers. – 1971. – Vol. C-20, N 11. – P. 1382 – 1393.
56. Meraud C. COPRA: A modular family of reconfigurable the computers / C. Meraud, R. Lloret // Proc. of IEEE NAECON. – 1978. – P. 822 – 827.
57. Базова технологія мікроміниатюризації бортової радіоелектронної апаратури (РЕА) для систем обробки інформації і управління / А.О. Морозов, О.О. Голубченко, М.Д. Кардащук, Б.Г. Мудла / Міжнародний симпозіум «Аерокосмічна індустрія та екологія. Проблеми конверсії і безпеки»: Тези доповідей. – Дніпропетровськ, 1996. – С. 42 – 43.
58. Sedmak R.M. Fault-tolerance of a general purpose implemented by very large scale integration / R.M. Sedmak, H.L. Liebergot // Int. Symp. Fault-Tolerance Computer. – Toulouse, France, 1978. – P. 117 – 123.
59. Avizjienis A. The Evolution of Fault Tolerant Computing at the Jet Propulsion Laboratory and at UCLA: 1960 – 1986 / A. Avizjienis, D.A. Rennels // The Evolution of Fault-Tolerant Computing. – Vienna and New York: Springer-Verland, 1987. – P. 271.
60. Avizenis A. Dependable Computing: From concepts to design diversity / A. Avizenis, J.-K. Laprie // Proc. of the IEEE. – 1986. – Vol. 76, N 5. – P. 629 – 638.
61. Laprie J.-K. Dependable computing and fault–tolerance: concepts and terminology / J.-K. Laprie // Proc. 15th IEEE Int. Symp. on Fault-Tolerance Computing. – Ann Arbor, Michigan, 1985. – P. 2 – 11.
62. Goldberg J. A time for integration / J. Goldberg // Proc.12th Int. Symp. on Fault-Tolerance Computing. – Los Angeles, 1982. – P. 79 – 83.
63. Hosford J.E. Measures of dependability / J.E. Hosford // Operations Research. – 1960. – Vol. 8, N 1. – P. 204 – 206.
64. Laprie J.-C. Dependability: Basic Concepts and Terminology / J.-C. Laprie. Springer-Verlag. – 1992. – P. 2 – 11.
65. Laprie J.-C. Dependability – Its Attributes, Impairments and Means / J.-C. Laprie // Predictability Computing Systems. – 1995. – P. 3 – 24.
66. Dobson J.E. Building reliable secure computing systems out of unreliable insecure compnents / J.E. Dobson, B. Randell // Proc. IEEE Symp. Security and Privacy. – Oakland, Calif, 1986. – P. 187 – 193.
67. Fray J.M. Intrusion tolerance using fine-grain fragmentation-scattering / J.M. Fray, Y. Deswarte, D. Powell // Proc. IEEE Symp. Security and Privacy. – Oakland, Calif, 1986. – P. 194 – 201.
68. Joseph M.K. A fault tolerance approach to computer viruses / M.K. Joseph, A. Avizienis // Proc.1988 IEEE Symposium on Security and Privacy. – Oakland, Calif, 1986. – P. 52 – 58.
69. A taxonomy of computer program security flaws / C.E. Landwehr [et al.] // ACM Computing Surveys. – 1994. – Vol. 26, N 3. – P. 211 – 254.
70. Information Technology Security Evaluation Criteria (ITSEC) // Commission of The European Communities, Office for Official Publications of the European Communities. – 1991. – 163 p.
71. International Standard ISO/IEC 2382-14. Information technology – Vocabulary – Part 14: Reliability, Maintainability and availability. – 1997. – 25 p.; ISO/IEC 2382-20. Information technology – Vocabulary – Part 20: System development. – 1990. – 22 p.
72. www.microsoft.com/PressPress/features/2002/feb02-20mundieqa.asp (EN).

Стаття надійшла до редакції 22.01.2010