УДК 004.052.42:004.725

Ю.В. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ДІАГНОСТИЧНОГО ПРОЦЕСУ

У статті розглянуто особливості процесу діагностування сучасних комп'ютерних систем, коли виникає проблема забезпечення надійності діагностичного процесу. У статті проведено аналіз та розглянуто різні типи перекручу вань діагностичної інформації та розглянуто методи захисту діагностичного процесу. В якості об'єкту діа гностування виступають інформаційні потоки, які проходять у комп'ютерних системах.

The article deals with the peculiarities of the process of diagnosing modern computer systems when there is the problem of ensuring the reliability of the diagnostic process. The paper analyzed and discussed the different types of distortions diagnostic information and protection methods considered diagnostic process. As an object of diagnosing act information flows that take place in computer systems.

Ключові слова: діагностування, діагностичний процес, комп'ютерні системи, тестові послідовності.

Вступ. Сучасні комп'ютерні технології використовуються у різних сферах життєдіяльності. За собом передачі інформації у таких технологіях використовують комп'ютерні системи. Розгалуженість та складність комп'ютерних систем створюють проблему забезпечення надійності та вірогідності їх функціонування. Тому для забезпечення ефективної роботи мереж використовують системи діагностування при пошуку та іде нтифікації несправностей. Для більшості систем діагностування які працюють у реальному масштабі часу, необхідні досить висока ві рогідність та безперервність генерування діагностичних впливів. Неприпустимі значні перерви та перекручування у видаванні діагностичних тестів. Для виконання цих умов спеціалісти змушені вживати спеціальних заходів захисту від усіх перекручувань, виходячи з припущення, що вони можуть з'явитися у будь-який момент. При цьому варто вжити заходів захисту від помилок, що найбільше спотворюють вихідні діагностичні результати і не дозволяють системі діагностування виконувати свої функції.

У дослідженні комп'ютерні системи розглядаються як об'єкт діагностування. До особливостей передачі інформації у комп'ютерних системах віднесемо:

- неоднозначність діагностичної інформації;
- наявність в окремих компонентах системи засобів вбудованого контролю;
- наявність несправностей визначеного типу залежно від видів використовуваних протоколів та конфігурації системи;
- значну схильність до перекручування програмного забезпечення і діагностичної інформації від "вірусів";
- залежність прояву несправностей від щільності мережного трафіку та кількості підключених абонентів.

Для забезпечення більш ефективного та достовірного діагностування систем необхідно провести аналіз і роз глянути типи перекручувань діагностичної інформації та методи захисту діагностичного процесу та використо вувати систему яка може провести діагностування з врахуванням всіх особливостей функціонування.

Постановка проблеми. При діагностуванні комп'ютерних систем шляхом подачі тестових послідовностей необхідно розв'язувати задачу їхньої коректно сті. Сигнали тестових впливів, які подаються на об'єкт діагностування (ОД), у випадку наявності специфічних несправностей та перекручувань у його структурі не повинні призводити до катастрофічних відмов.

Для діагностування комп'ютерних систем та побудови системи діагностування найбільш придатними, на думку автора є методи, в основі яких лежить схема безупинної (послідовної) ідентифікації, тобто ідентифікації методом на основі адаптивної моделі. Найчастіше використовують параметричну адаптивну модель, тобто модель, у якої змінюються параметри при незмінній структурі. Однак можливе застосування моделі, у якої в процесі адаптації змінюються не тільки параметри, але й структура [1].

При класичній побудові адаптивної моделі обирають міру помилки між виходами моделі та об'єкту і роз робляють алгоритм пошуку невідомих параметрів за умов мінімізації обраної міри помилки. Як міру помилки можна використовувати середню квадратичну помилку, максимальне значення помилки, інтеграл від квадрата помилки, інтеграл від абсолютного значення помилки, статистичні критерії максимуму апостеріорної імовір ності і максимуму правдоподібності, або різні варіанти названих критеріїв з використанням функцій ваги.

Незалежно від джерел будь-які перекручування зрештою виявляються в результуючих діагностичних даних системи діагностування. Тому у всіх випадках критерієм якості діагностування є вірогідність та точність обробленої інформації і виданих тестових впливів. Розподіл методів захисту зводиться до захисту діагностичного процесу і до захисту інформації.

Дослідження існуючих методів. Оскільки система діагностування працює в реальному масштабі часу, необ хідно оперативне виявлення перекручувань діагностичної інформації та її наслідків, а також оперативне й ав томатичне вживання заходів щодо ліквідації чи зменшенню можливих відхилень процесу

діагностування від нор мального режиму без його зупинки чи тривалого переривання. При цьому повинна враховуватися тривалість прояву наслідків перекручування в результатах функціонування діагностичної системи і застосовуватися коре гування ходу діагностичного процесу, що забезпечує максимальне скорочення тривалості прояву цих наслід ків. Для забезпечення захисту діагностичного процесу й інформації викори стовується інформаційна і часова надмірність. При цьому під тимчасовою надмірністю системи діагностування розуміють можливість використання деякої частки продуктивності системи для контролю вико нання діагностичних програм. Для цього при проектуванні системи діагностування повинен передбачатися запас продуктивності, що буде вико ристовуватися для оперативного кон тролю і підвищення надійності функціонування. Величина тимчасової надмі рності залежить від вимог до надійності функціонування системи і знаходиться звичайно в межах від 5– 10 % продук тивності простої системи (один рівень перевірки) до двох, три і чотириразового дублювання продуктив ності в складних системах (багаторівневі перевірки) [2].

Тимчасова надмірність чи резерв часу використовується для контролю і виявлення перекручувань, на його діагностику й ухвалення рішення по відновленню діагностичного процесу і на реалізацію операцій віднов лення. Виявлені перекручування за їхніми наслідками можна розподілити на три групи: не знецінюють, що част ково знецінюють і цілком знецінюють всі отримані резуль тати [3]. Якщо після відновлення діагностичного процесу його можна продовжити без повто рення з місця, де виявлене перекручування, то така відмова не знецінює результат. При відмові, що цілком знецінює, необхідно повторювати всі діагностичні операції, пророб лені до моменту відмови. У проміжному випадку при відмові, що частково знецінює результат, проте зберігає цінність, деякі проміжні результати, що звичайно відповідають моменту попере днього контролю працездатності можуть використовуватись для аналізу.

При функціонуванні системи діагностування у реальному масштабі часу величина резерву часу для конт ролю і відновлення діагностичного процесу й інформації заздалегідь не встанов люється. Для діагностування пере кручувань і операцій відновлення у за гальному випадку необхідний довільний інтервал часу, що виділяється за рахунок резерву, або за рахунок скорочення часу розв'язання діагностичних задач.

Забезпечення стійкості діагностичного процесу. При розробленні системи діагностування такого об'єкту діагностування як комп'ютерні системи та ви користанні ідентифікації методом адаптивної моделі обов'язковим є використання формального опису ОД – моделі. При побудові моделі будемо виходити з того що складна сис тема – наприклад, мережа, підкоряється визначеним законам: фізичним, електричним, механічним та іншим, які характеризують кількісні співвідношення різних компонентів структури мережі.

Формалізований опис моделі структурного рівня системи представимо як

$$Mc = \langle Ln, Ls, K, Dl, Dmp, Tp, Ac, Eskew, T2l, Ip, Nc, Uc \rangle \quad (1)$$

До факторів, параметрів та станів які будуть активно впливати на адекватність моделі реальній системи на нижніх рівнях моделі OSI, відносяться:

$Ln = f(Lsi), \quad де\ i = 1.....m,$ довжина системи;

$Ls = \{lsi\}, \quad де\ i = 1.....n,$ довжина сегментів;

$K = \{ki\}, \quad де\ i = 1.....n,$ кількість мережних пристроїв;

$Dl = f(Ln, K)$, затримки розповсюдження сигналу;

$Dmp = \{dmi\}, \quad де\ i = 1.....n,$ затримки в перехідних мережевних при строях (мости, маршрутизатори, комутатори тощо);

$Tp = \{tpi\}, \quad де\ i = 1.....n,$ зменшення мінімального часу між паке тами;

$Ac = \{a_{ci}\}, \quad де\ i = 1.....n,$ затухання в кабелі та ближньому і дальньому кінці;

$Eskew = \{e_{skewi}\}, \quad де\ i = 1.....n,$ розкид затримок проходження сигналу по витій парі;

$T2l = f(Ln),$ час обігу чи прослуховування;

$Ip = \{i_p\}, \quad де\ i = 1.....n,$ довжина пакету;

$Nc = \{n_{ci}\}, \quad де\ i = 1.....n,$ кількість конфліктів у системі;

$Uc = \{u_{ci}\}, \quad де\ i = 1.....100,$ утилізація каналу зв'язку.

До множини вхідних, вихідних та внутрішніх станів відносяться $I_{p,}$ T_{2l}, N_{c}, $U_{c.}$ До множини функцій переходів і виходів структурних вузлів відносяться $D_{1,}$ $D_{mp,}$ $T_{p,}$ $A_{c,}$ E_{skew}. До структурної схеми відно сяться $L_{n,}$ $L_{s,}$ N.

Виходячи з схеми ідентифікації та моделі ОД необхідно провести аналіз типів перекручувань діагностичної інформації та методів захисту діагностичного процесу при перевірці комп'ютерних систем адаптивною систе мою діагностування. Аналізі і реєстрація перекручувань у результатах дозволить в подальшому викори стовувати цю інформацію для повторюваних перекручувань та наступної локалізації

дже рела помилки і її лікві дації.

Адаптивна система діагностування – це система керування подачею, прийомом та аналізом тестових дій при подачі їх на складні об'єкти діагностування з характеристиками та параметрами, що змінюються. Принцип дії системи діагностування полягає в керуванні подачею тестових впливів на основі прогнозу вихідних характе ристик об'єкту діагностування, що були одержані за допомогою регулярно обновлюваної моделі в зворотному зв'язку. Для системи діагностування потрібне постійне уточнення моделі в зв'язку з характеристиками та параметрами, що змінюються в часі. До них відносяться постійна зміна трафіку системі, кількість вузлів підключених до мережі, модернізація та удосконалювання апаратного та програмного і т.д., що в свою чергу призводять до зміни характеристик і параметрів об'єкту. Для такого класу об'єктів діагностування зміни харак теристик і зовнішніх впливів необхідно враховувати безпосередньо в процесі діагностування. Відсутність та недоліки апріорної інформації про об'єкт діагностування як на стадії проектування системи, так і в процесі експлуатації, велика інерція об'єкту, стохастичний характер зв'язків вимагають використання моделі ОД для керування по подачі тестів на основі прогнозу вихідних перемінних з врахуванням вхідним перемінних. Застосування методів керування, що базуються на постійній, незмінній моделі тут неможливо.

Типи перекручувань діагностичної інформації та методи захисту діагностичного процесу. Проведемо класифікацію наслідків перекручувань інформації й діагностичного процесу та зробимо хоча б наближену оцінку їхнього впливу на загальний критерій функціонування системи діагностування за аналогією [2]. З погляду побудови засобів захисту і розподіл ресурсів, які доцільно виділити для захисту від перекручувань, помилки результатів можна розділити по їх наслідках на три типи [3]. До першого типу належать:

- перекручування результатів, що приводять до припинення виконання системою основ них функцій чи їхньої частини на тривалий чи невизначений час (цілком знецінюють);
- перекручування, що короткочасно, але значно спотворюють величину чи значеннєвий зміст окре мих результатів (частково знецінюють);
- перекручування, що короткочасно впливають на результати, видавані системою керуючих ал го ритмів.

Такий якісний розподіл перекручувань визначає розподіл ресурсів по захисту системи. Найбільші ресурси доцільно виділяти для захисту від перекручувань інформації й діагностичного процесу першого типу, наслідки яких мо жуть виявлятися у системі діагностування у наступ ному виді:

- зациклення, тобто послідовна повторювана реалізація визначеної групи тестів, що не припи няється без зовнішнього втручання;
- зупинка і припинення рішення діагностичних задач;
- перекручування процесів взаємного переривання тестів, що призводить до блокування мож ливості де яких типів переривань;
- значне зниження темпу рішення діагностичних задач внаслідок переванта ження по пропускній здатності;
- значне перекручування чи втрата накопиченої інформації про поточний стан діагностичного про цесу.

Перекручування інформації й діагностичного процесу другого типу також дуже небезпечні і для захисту від них варто застосовувати досить ефективні заходи. Ці перекручування можуть виявля тися в наступному виді:

- пропуск тестів чи їхніх істотних частин;
- вихід на тест чи їхні частини, що різко спотворюють результати;
- обробка помилкових чи сильно перекручених повідомлень з ОД.

Третій тип перекручувань характерний, в основному, для квазінеперервних величин. Ці помилки мало спо творюють загальні результати, однак окремі викиди можуть сильно впливати на діагностичний процес і потрі бен досить ефективний захист від рідких значних відхилень резуль татів.

Перераховані типи перекручувань істотно розрізняються не тільки по величині зміни результатів, але і по тривалості прояву їхніх наслідків. Методи, застосовувані для ліквідації наслідків помилок, також розрізняються по тривалості їхньої дії. Залежно від ступеня прояву і причин виявлених перекручувань, можливі наступні оперативні заходи для ліквідації їхніх наслідків [3]:

- відновлення інформації і збереження стійкості процесів діагностування;
- ігнорування виявленого перекручування внаслідок його слабкого впливу на весь процес діагносту вання і на вихідні результати;
- повторення функціонального алгоритму чи тесту при тих же вихідних даних;
- виключення тесту з обробки внаслідок перекрученості чи труднощів відновлення діагностич ного процесу;
- короткочасне припинення рішення задач функціонального алгоритму до відновлення вихід них даних;
- перебудова режиму роботи алгоритму для зниження впливу перевантаження в зв'язку з втратою інфо рмації про хід діагностичного процесу.

Ці методи можуть істотно розрізнятися не тільки за величиною пе рекручувань результатів, що виправля ються, але і за тривалістю прояву наслідків помилки. Засто сування цих методів вимагає аналізу характеру про яву помилки, стану інформації про хід процесу діагностування, інформації в повідомленнях, що надходять, стану системи та ОД тощо. При цьому схема прийняття рішень на застосування методів захисту повинна забезпечу вати оперативне нагромадження й індикацію виявлених перекручувань, а також довгострокове нагро мадження результатів контролю для більш детального аналізу джерела помилок і виявлення мож ливості їхньої локаліза ції й усунення шляхом коректування тесту чи виправлення роботи системи. Оперативний захист повинний також передбачати реєстрацію й індикацію перекручувань для аналізу. Помилки, що виявляються систематично і досить часто, варто аналізувати на можливість виправлення тесту.

Існує досить багато методів захисту діагностичного процесу. Розглянемо захист від за циклювання тестів. У діагностичних тестах ши роко використовуються однотипні діагностичні операції, що утворять цикли для по шуку, упо рядкування й однотипного перетворення інформації. Причиною зациклення можуть бути не тільки помилки в тесті й перекручування вихідної інформації, але і збої в апаратурі системи діагностування. Тому при виявленні пер винного зациклення доцільно повторити включення тестів при тих же вихідних даних. Якщо зациклення не повторюється, то, швидше за все, воно відбулося в результаті випадкового збою. Повторне зациклення при од накових вихідних даних може бути обумовлено помилкою в тесті при правильної вихідної інформації, перекру чуванням вихідної чи інформації частковим відмовленням апаратури. При багаторазових зацикленнях з різними вихідними даними причиною є, швидше за все, часткове відмовлення в апаратурі чи перекручування інформації про процес діагностування.

Захист від зупинок методично близька до захисту від зациклення. У цьому випадку також припиняється рішення тестових задач і система зупиняється на деякій довільній команді. Зупинка системи може відбутися або через помилку при формуванні тесту (часткове чи відмовлення збій), або через помилку в тесті, що приводить до виходу на ділянку тесту, що містить команду зупинка. Автоматичне виявлення зупинок аналогічно вияв ленню зациклення, наприклад, періодичним порівнянням часу завершення підпрограми тесту чи функціональ ного алгоритму з поточним часом лічильника у системі. При виявленні зупинок логіка відновлення функціону вання системи аналогічна логіці захисту від зациклення, тобто послідовно перевіряється можливість повторення даного алгоритму, можливість його пропуску і необхідність переходу на справну систему.

Захист від перекручувань взаємного переривання підпрограм, що приводять до блокування можливості де яких типів переривань, а отже, до блокування прийому і видачі інформації відповідним ОД, здійснюється, в основному, апаратними методами. При цьому контролюється правильність виконання операцій переривання, переходу до програми, що перериває, і наступного повернення до перерваної програми. Для захисту від таких помилок, а також від апаратних збоїв при перериваннях повинний передбачатися контроль виконання перери вань і періодичний контроль взаємодії з всіма ОД. Для виконання цих функцій спеціальна періодична програма повинна підготовляти контрольні тести і видавати їх ОД. При порушенні періодичного обміну з яким-небудь ОД, що може бути наслідком як тестової помилки, так і безлічі інших причин, порушення обміну звичайно усувається позапрограмними методами.

Захист від помилок, що призводять до пропуску тесту чи їхніх частин, виробляється, в основному, ме тодом контролю ключових кодів, що визначають перелік підпрограм, що повинні бути включені. Захист від пропуску підпрограм тестів застосовується переважно при включенні періодичних підпрограм, а також для окремих функціональних тестів, де порушення послідовності їхньої роботи може істотно відбитися на функціонуванні всієї системи.

Захист від помилок, що приводять до виходу на тести чи їхні частини, що різко спотворюють ре зультати, методично близький до захисту від пропуску підпрограм тестів. Однак у даному випадку може бути більше варіантів, тому що внаслідок помилкових сполучень чи формувань команд в принципі можливий помилковий перехід, з будь-якої підпрограми на будь-яку іншу підпрограму тесту. Тому цілком захиститися від помилкових під ключень підпрограм неможливо, але деякі особливо небезпечні, неприпустимі сполучення підпрограм іноді має сенс заблокувати.

Захист від перевантаження системи по пропускній здатності припускає виявлення і зниження впливу наслідків швидкого алгоритмічного розподілу ресурсів, обумовлених неправильним визначенням необхідної пропус кної здатності системи для роботи у реальному масштабі часу. Крім цього, перевантаження можуть бути наслідком неправильного функціонування джерел інформації з ОД і перевищення нормального (розрахункового) рівня інтенси вності потоків повідомлень. Для виявлення перевантаження по пропускній здатності системи можна використову вати:

- контроль тривалості збереження повідомлень, що підлягають обробці за нижчими пріоритетами;
- контроль заповнення буферних нагромаджувачів повідомленнями низьких пріоритетів;
- контроль заповнення буферних нагромаджувачів повідомленнями високих пріоритетів;
- контроль часу включення диспетчером алгоритму нижчого пріоритету при наявності за явок на включення;
- контроль частоти включення диспетчера з послідовним аналізом усіх пріоритетних рів нів без рішення задач.

При виявленні перевантаження бажана також оцінка її величини і причини появи. Контроль завантаження буферних нагромаджувачів організується дуже просто шляхом перевірки записуваних адрес, підлягаючих обробці повідомлень і корисний не тільки при прийомі, але й при видачі повідомлень. Це дозволяє, зокрема, виявляти помилки в тестах, що ведуть до по рушення нормального темпу формування тестів для деяких ОД.

Застосовуючи алгоритмічні методи захисту, можна істотно знизити шкідливий вплив перевантажень ре сурсів системи і адаптацію алгоритмів на рівень припустимого завантаження. Зокрема така адаптація істотно знижує вплив помилок у структурі побудови алгоритмів, що ведуть до невеликих короткочасних переванта жень.

Висновки. Особливості забезпечення стійкості діагностичного процесу, оперативний захист від перекручувань інформації й об числювального процесу може викори стовуватися як засіб виявлення помилок які складно виявляються, що особливо необхідно на завершальних ета пах діагностування та у процесі експлуатації системи діагностування. Головна задача оперативного захисту від різних перекручувань складається в забезпеченні безперервності процесу керування з припустимими помилками у вихідних повідомленнях ОД. В системі діагностування використовуються наступні міри для забезпечення стійкості діагностичного процесу: відновлення інформації та збереження стійкості процесів діагностування, ігнорування виявленого перекручування внаслідок його слабкого впливу на весь процес діагносту вання і на вихідні результати, повторення функціонального алгоритму чи тесту при тих же вихідних даних, виключення тесту з обробки внаслідок його перекрученості чи труднощів відновлення діагностич ного процесу, короткочасне припинення розв'язання задач даного функціонального алгоритму до відновлення вихід них даних, перебудова режиму роботи алгоритму для зниження впливу перевантаження в зв'язку з втратою інфо рмації про хід діагностичного процесу.

Література

1. Хмельницький Ю.В. Метод адаптивного діагностування комп'ютерних мереж Вісник ТУП, № 3 / Хмельницький Ю.В. – Хмельницький : ХНУ, 2003. – С. 43– 48.

2. ДСТУ 2389-94. Технічне діагностування та контроль технічного стану. Терміни та визначення. – К. : Держстандарт України, 1994. – 24 с.

3. Хмельницький Ю.В. Дослідження та аналіз несправностей локальних обчислювальних мере Вісник ТУП, № 2 / Хмельницький Ю.В. – Хмельницький : ХНУ, 2003. – С. 152– 155.

Надійшла 25.9.2012 р.
Рецензент: д.т.н. Мясіщев О.А.

УДК 681.518

В.П. НЕЗДОРОВІН, К.Л. ГОРЯЩЕНКО
Хмельницький національний університет
Є.Г. МАХРОВА
Буковинський державний медичний університет

РЕАЛІЗАЦІЯ ПРОТОКОЛУ MODBUS В СЕРЕДОВИЩІ CODESYS 2.3

Розглянуто застосування сучасних програмних середовищ розробки програмного забезпечення для програмованих логічних контролерів на прикладі CoDeSys.

Application of modern software development environments software for programmable logic controllers on the example of CoDeSys.

Ключові слова: програмований логічний контролер, SCADA.

Задачі автоматизації технологічного процесу на підприємстві можуть бути розв'язані шляхом використання засобів комп'ютерної та мікропроцесорної техніки. Основу реалізації автоматизації сучасного промислового підприємства складають промислової комп'ютери – ПЛК (програмовані логічні контролери), задача яких полягає у виконанні програми користувача із високим ступенем автономності. Найперший в світі програмований контролер MOdular DIgital CONtroller (Modicon) 084, що мав пам'ять всього 4 кбайт, був виготовлений у 1968 р. ПЛК розроблені для заміни релейних схем керування, які виготовлені із застосуванням дискретних елементів: реле, таймери, лічильники, елементи жорсткої логіки.

Принцип роботи ПЛК полягає у зборі та обробці даних згідно прикладної програми користувача. Наслідком виконання програми є формування вихідної послідовності сигналів на виконавчі пристрої.

Найбільш типові галузі застосування програмованих (інтелектуальних) контролерів:

- Автоматизація невеликих агрегатів для виробництва, збирання, обробки і упаковки;
- Автоматизація сільськогосподарських сфер (системи іригації, теплиці);
- Автоматизація шлагбаумів, відкатних воріт, систем контролю доступу;
- Автоматизація компресорів та систем кондиціонування повітря;