УДК 680.03

О.Ю.Афанасьєва, Б.В.Дурняк, Ю.М.Коростіль, Ю.Ю. Білак

МЕТОД ВЕРИФІКАЦІЇ КЛЮЧОВИХ ЕЛЕМЕНТІВ СИСТЕМИ ЗАХИСТУ СКЛАДНИХ ТЕХНІЧНИХ ОБ'ЄКТІВ

Аннотация.

В статье исследуются компоненты, которые входят в состав системы безопасности, которые предназначены для обслуживания функционирования опасных технических объектов. Особенное внимание уделяется компонентам системы безопасности, которые представляют собой конструктивные средства защиты и в связи с этим более детально рассматриваются непроектные неисправности.

Ключевые слова: непроектные неисправности, конструктивные средства защиты, технический объект, диагностика, безопасность.

Система забезпечення безпечного функціонування складних технічних об'єктів (TO) є обов'язковою частиною технічних засобів, що забезпечують можливість реалізації основних технологічних процесів, на які орієнтований даний об'єкт. Сучасні TO по цілому ряду своїх ключових параметрів, до яких в першу чергу, відносяться потужності, що можуть звільнятися, об'єми негативного впливу на оточуюче середовище різних факторів, які породжуються в рамках TO і які можуть приводити до локальних та глобальних катастрофічних змін в екологічній системі. Тому, засоби забезпечення безпеки повинні не тільки виявляти та протидіяти можливим небезпекам, які можуть ініціювати деструктивні процеси по відношенню до TO, а й виявляти загрози, які існують в межах самого TO та загрози, що існують або виникають в рамках самої системи забезпечення безпеки (SB) функціонування TO. Систему забезпечення безпеки функціонування TO можна умовно поділити на наступні засоби захисту по способу їх реалізації:

- апаратурні засоби,
- програмні засоби,
- конструктивні засоби.

До апаратних засобів відносяться засоби, типовим прикладом яких є датчики різних видів та класів, які можуть представляти собою програмно-апаратну реалізацію тих, чи інших пристроїв. Цей клас засобів є найбільш розвинутим та дослідженим [1]. Вони з'єднуються з інформаційними системами управління та захисту об'єктів та елементи цього класу засобів призначені для створення системи аналізу різноманітних сигналів, які є носіями даних, що відображають текучий стан TO включаючи сигнали, які безпосередньо пов'язані з виникненням несправностей. До цих засобів відносяться також апаратурні системи, що реалізують протидію по відношенню до несправностей, що викають в TO.

До програмних засобів відносяться всі програмні компоненти, що функціонують в рамках відповідної інформаційної системи, які розв'язують задачі діагностики, аналізу та прийняття рішень, які в сукупності забезпечують необхідний спосіб функціонування системи системи безпеки TO. Ця частина системи безпеки найбільш досліджена та розвинута в галузі забезпечення безпеки TO. Цю частину засобів можна розділити на наступні функціональні компоненти:

- компоненти перетворення фізичних сигналів, або різних форм їх представлення в інформаційні елементи, що можуть бути аналізовані в компонентах визначення текучого стану безпеки,
- компоненти, що реалізують аналіз даних про текучий стан TO та на основі такого аналізу формують управляючі дії, які направлені на забезпечення необхідного рівня безпеки,
- програмні засоби, що визначають текучий рівень безпеки TO та прогнозують можливу зміну рівня безпеки на заданий перід часу.

Компоненти першого типу є найбільш дослідженими та розвинутими у зв'язку з дослідженнями діагностичних моделей, основними функуіями яких є виявлення діагностичних ознак, діагностичних параметрів та їх інтерпретація в предметній області діагностування TO [2].

Друга компонента, яка представляє собою систему аналізу текучого стану об'єкту, яка грунтується на використанні моделей, що орієнтовані на задачі опису різного типу несправностей, аварійних ситуацій та інших особливостей, що відображають порушення штатного функціонування TO. Оскільки приведені вище задачі досить складно формалізувати, то відповідні засоби будуються на основі систем експертного аналізу, систем прийняття рішень, інших типів інтелектуальних систем, що орієнтовані на аналіз аспектів, які стосуються впливу людських факторів на порушення безпеки функціонування TO [3].

Компонента, що стосується обчислення текучого рівня безпеки функціонування TO та прогнозування очікуваного рівня безпеки є надзвичайно важливою і вона досліджується у зв'язку з задачами прогнозування виникнення негативних подій на TO [4]. Ця компонента є одним з основних елементів SB. На основі функціонування систем, що складають цю компоненту, здійснюється ініціація і активізація процесів, що пов'язані з протидією розвитку несправностей та протидією виникненню аварійних ситуацій. Необхідність використання цієї компоненти обумовлюється наступними факторами:

- використання засобів захисту, особливо їх активізація та функціонування є досить дорогими, оскільки вони потребують певних ресурсів, які, в ідеальному випадку, повинні призначатися для реалізації процесів функціонування основних технологічних процесів, що особливо характерно для випадків, коли відповідні засоби реалізуються у вигляді певних алгоритмів, що функціонують в середовищі обчислювальних засобів

інформаційних систем TO,

- серед несправностей, які можуть виникати в рамках TO, трапляються несправності, причина виникнення яких може бути не відомою на етапі проектування відповідних TO; приймаючи до уваги, що несправність завжди може мати місце перед виникненням аварійної ситуації, то можна стверджувати, що у випадку виникнення несправності, яка не була вчасно виявлена, в більшості випадків приводить до виникнення аварійних ситуацій і такі аварійні ситуації називаються непректними; засоби прогнозування виникнення непректних несправностей, в більшості випадків, слабо пов'язані з тим, чи іншими можливими причинами виникнення несправностей і тому вони є, на даному етапі, єдиним засобом, з допомогою якого є можливим виявляти та протидіяти непректним несправностям та непректним аварійним ситуаціям [5].

Конструктивні засоби захисту є найменш дослідженими на даний момент, хоча в ряді випадків створення SB вони уже використовуються. Розглянемо наступне, дещо розширене визначення.

Визначення 1. Конструктивними засобами захисту називаються проектні рішення способів реалізації конструкції TO, які є невід'ємною частиною конструктивних рішень, що забезпечують можливість реалізації основного технологічного процесу (TP) і орієнтовані на реалізацію таких процесів по відношенню до ключових технологічних фрагментів, які призначені для зупинки основного TP та нейтралізації можливого негативного впливу факторів, які виникають в наслідок недопустимих способів функціонування TP, чи виникають в період виявлення аварійної ситуації, що обумовлена зовнішніми факторами.

В сучасних проектах TO передбачаються відповідного типу засоби захисту, але вони виконуються у вигляді певних розширень конструктивних елементів конструкції, яка призначена для реалізації основного TP. Такий підхід до створення компонент засобів протидії аваріям не може забезпечити необхідний рівень їх можливостей, оскільки, при їх проектуванні виходять з загально прийнятих, або відомих аварійних ситуацій, що можуть виникати на TO. Практика експлуатації небезпечних TO вказує на те, що, в більшості випадків, аварійні ситуації, що можуть стати причиною виникнення локальних катастроф, виникають в результаті непроектних несправностей. Оскільки, для непроектних несправностей характерною є відсутність даних про можливі причини їх виникнення, то у проектантів не має можливості розробити конструктивні засоби захисту такими, які були би адекватними можливим непроектним аваріям.

Для того, щоб розв'язати зазначену вище проблему, необхідно проектувати технічні засоби захисту на основі наступного підходу, який враховує цілий ряд факторів, що пов'язані з діагностикою та безпекою TO.

1. Всі типи несправностей, що можуть виникнути в TO, з точки зору форми їх прояву є відомими, оскільки TO є об'єктом, який спроектований і

побудований відповідними спеціалістами.

2. Система діагностики разом з діагностичними моделями, які ґрунтуються на визначенні та вимірюванні діагностичних ознак та діагностичних параметрів, є досить розвинутою.

3. Діагностичні моделі можуть розвиватися та удосконалюватися шляхом використання для її реалізації методів, які використовуються при побудові експертних, систем прийняття рішень та інших систем, що представляють собою засоби реалізації штучного інтелекту, можливості якого виходять за рамки строго детермінованих методів розв'язування задач [6].

4. Важливим фактором, який визначає можливість забезпечення певного рівня безпеки, є реалізація в рамках конструктивних, автономних засобів захисту, які незалежно від текучого нормального стану TO, були б здатними до активізації процесів захисту, які передбачені і визначені, як обов'язкові на основі проектних розрахунків та теоретичних досліджень факторів, що обумовлюють можливі небезпечні ситуації, які можуть виникати на TO.

5. Важливим аспектом, який повинен реалізуватися в конструктивних засобах захисту (KZ), є такий спосіб їх конструювання, при якому вони були б незалежними від впливу людських факторів, які могли б впливати на способи реалізації алгоритмів захисту TO від аварійних ситуацій.

6. Система безпеки, що пов'язана з TO, який у відповідності з TP, визначений як такий, що має певний рівень загрози для оточення, чи зовнішнього середовища, відповідна SB повинна включати в себе засоби типу KZ, та повинна допускати моніторинг міри захисту на всіх рівнях управління та забезпечення захисту, в тому числі, які передбачені загальною соціальною структурою, що розміщається на територіях, які можуть бути охоплені дією негативних факторів відповідного TO.

7. Технічний ресурс засобів KZ повинен перевищувати технічний ресурс TO на задану, при проектуванні, величину.

Виходячи з приведених факторів, які повинні враховуватися при побудові KZ, можна наступним чином сформувати базові задачі, що розв'язуються SB, яка включає засоби типу KZ та основні умови, яким повинна відповідати така система безпеки.

Перша і основна задача, яка розв'язується в рамках SB, яка включає KZ, полягає у прогнозуванні та виявленні процесів, що обумовлюються виникненням, або недопустимими змінами значень діагностичних параметрів і приводять до виникнення аварійних ситуацій. Розв'язок цієї задачі полягає у встановленні залежностей між змінами значень діагностичних параметрів та певним типом аварійної ситуації, множина описів яких є відомою. Формально, такий розв'язок можна представити у наступному вигляді, який відображає схему реалізації такого розв'язку:

$$AS_i = \Im\{[L^1_{i1}(y_{11},...,y_{1n})],...,[L^N_{im}(y_{m1},...,y_{mk})]\}, \qquad (1)$$

де $\Im$ - логічна функція, що будується на основі системи логічних

формул $L_{ij}^{m}(y_{j1},...,y_{jr})$, кожна з яких описує ту, чи іншу несправність z_i, що формально описується наступним співвідношенням:

$$z_i = L_i^M(y_{i1},...,y_{ik}), \quad (2)$$

де L_{ij}^{M} - логічна функція, яка описує відповідні логічні залежності між діагностичними параметрами y_{ij}, що описують несправність z_i. Кожен з параметрів y_{ij} є функцією діагностичних ознак, які характеризують та обумовлюють виникнення відповідного діагностичного параметру, або обумовлюють недопустиму зміну його значення, що описується наступним співвідношенням:

$$y_{ij} = f(\xi_{i1},...,\xi_{im}), \quad (3)$$

де ξ_{ij} - діагностична ознака. В більшості випадків, діагностичні ознаки по відношенню до діагностичного параметру описують фізичні процеси, що відбуваються у вузлах TO і приводять до виникнення тих, чи інших несправностей. Наприклад, недопустимі величини навантажень, що можуть виникати в процесі функціонування TO, можуть приводити до виникнення певного дефекту. Розміри такого дефекту та його динамічні характеристики, наприклад, динаміка змін, обумовлюють появу діагностичного параметра, який описує текуче значення розміру відповідного дефекту. Тому, співвідношення (3) описує, в більшості випадків, фізичну модель процесів виникнення та збільшення відповідного дефекту. Певне значення цього діагностичного параметру, або деякої їх сукупності може привести до виникнення несправності z_i. Така несправність описується у вигляді відхилень процесу функціонування відповідного фрагменту TP, від режиму, який запроектований як штатний. Для повністю адекватного опису залежності z_i від y_{ij}, необхідно було би створити складну модель, яка описувала б процеси у деякому вузлі, що обумовлюються діагностичними параметрами. Наприклад, дефект, що обумовлюється спрацьовуванням лопаток турбіни, приводить до виникнення несправності, яка може представляти собою, перевитрату пари, або іншого носія енергії, яка в турбіні перетворюється в механічну енергію обертання валу турбіни. Але поява такої несправності не обов'язково приводить до виникнення аварійної ситуації. Очевидно, що величина зміни діагностичного параметру від приведених в прикладі дефектів може бути описана деякою складною математичною моделлю, яка потребує значних затрат часу та обчислювальних ресурсів для її реалізації. Це є причиною недоцільності її використання в системах діагностики, які повинні функціонувати в режимі реального часу, параметри якого визначаються фізичними параметрами відповідного вузла TO. Для розв'язку цієї проблеми використовується методика ітераційного наближення. На якісному рівні, така методика полягає у наступному.

Рівень значення кожного діагностичного параметру визначається у

вигляді ряду порогових значень, які в предметній області мають власну інтерпретацію, що можна представити у наступному вигляді:

$$y_i = \{\delta_1 y_i, ..., \delta_k y_i\},$$

де δ_i - представляє собою ідентифікатор відповідного порогового рівня множини значень діагностичного параметру. На цій множині ідентифікаторів задається певний порядок. В найпростішому випадку, функція порядку може задаватися операторами $\{<, >, \leq, \geq\}$. В залежності від діапазону порогів у який попадає текуче значення параметру, останнє інтерпретується як допустиме, чи не допустиме, з точки зору міри його впливу на розвиток несправності z_i. Оскільки міра такого впливу по відношенню до текучого значення y_i може бути нелінійною, або локально розподіленою, то область визначення бінарних значень y_i також може бути розподіленою. Уявлення про несправність допускає його бінарну інтерпретацію у випадку, коли система констатує факт наявності, або відсутності відповідної несправності. Таким чином, факт виникнення несправності, а, точніше, умови її виникнення можуть бути описані логічними співвідношеннями у відповідності із співвідношенням (2). Тому, в рамках системи діагностики повинна існувати система логічних формул, в якій кожна формула відповідає одному типу несправності, що формально можна представити у вигляді наступного співвідношення:

$$Z^P = \{[z_1^P = L_1^N(y_{11}, ..., y_{1k})], ..., [z_n^P = L_n^N(y_{n1}, ..., y_{ng})]\}, \quad (4)$$

де L_i^N - логічна формула, що описує умови виникнення несправності z_i в TO, де індекс P означає, що несправність є проектна, або є відомою і може бути описана на етапі проектування. У випадку, коли несправність є непроектною Z_i^N, то це означає, що для несправності z_i існують умови її виникнення, які не описуються в системі (4). Отже, для її визначення необхідно сформувати, або вивести деяку формулу L_i^{N*}. Очевидно, що не має сенсу будувати різні варіанти формул для однієї несправності z_i лише для того, щоб поповнити систему (4). Зрозуміло, що діагностичні ознаки ξ_i і бінарна інтерпретація їх значень є повною в рамках системи діагностування. Розглянемо наступні аспекти, що пов'язані з виявленням непроектної несправності Z_i^N, що може мати місце в TO.

1. Вихідними даними, для реалізації процесу визначення Z_i^N є певна сукупність діагностичних ознак $\{\xi_{i1}, ..., \xi_{in}\}$ та сукупність відомих Z_i^P, що описані у вигляді співвідношення $Z_i^P = L_i^N(y_{i1}, ..., y_{in})$. При цьому, має місце співвідношення $y_{ij} = f(\xi_{i1}, ..., \xi_{ik})$, де f - функція, яка є відомою.

2. Існує система правил виводу Ξ, в якій є сформовані правила

перетворень системи логічних співвідношень, базою яких є система виводу Герцена [7], що розширена логічними правилами перетворень, які відображають особливості предметної області їх інтерпретації. Очевидно, що такі розширення для кожного окремого об'єкту формуються на основі даних про об'єкт.

3. Ціллю перетворень логічних співвідношень є побудова такої логічної формули $L_i^{N\bullet}(y_{i1},..,y_{in})$, для якої існує $Z_i^P(y_{i1},...,y_{in}) \to Z_j^N(y_{j1},...,y_{jm})$.

В рамках такої, досить широкої постановки задачі, виходячи з рівня загальності схем логічних правил виводу довільна перестановка, або заміна одного логічного фрагменту формули може представляти собою опис нової несправності $z_i^N(y_{i1},...,y_{in})$. Щоб цього уникнути, в склад Ξ вводяться обмеження на загальні правила логічних перетворень. Такі обмеження стосуються окремих діагностичних параметрів, які характеризують окремі фізичні зміни, або фізичні прояви елементів різних дефектів.

Як видно із співвідношення (1), аварійна ситуація (AS) є логічною функцією ряду несправностей, що в загальному випадку записується у вигляді:

$$AS_i = \Im_i(Z_{i1},...,Z_{in}).$$

Якщо серед аргументів використовується Z_{ij}^N, то AS_i також являється непроектною аварією, або має місце співвідношення:

$$\forall z_{ij} \exists z_{ik} \{(Z_{ik}^N) \to [\Im_i(z_{i1},...,z_{in}) = AS_i^N]\}.$$

Може мати місце ситуація, коли серед z_{ij} відсутні Z_{ij}^N, а AS_i є непроектною аварією. Це означає, що можлива реалізація аварії AS_i така, що описується логічною формулою, яка відмінна від відомих логічних формул, які описують проектні аварії. Визначення такого типу непроектних аварій реалізується на основі використання процедури виводу, яка будується на основі тієї ж системи Ξ, яка розширена іншими логічними формулами, що описують відповідні обмеження, які відповідають особливостям предметної області інтерпретації відповідних несправностей. Додатковою можливістю, якою повинна володіти система, що реалізує засоби типу KZ є наступне. Переважно, TO і відповідні TP представляють собою об'єкти, ресурс функціонування яких є порівняно великий. Для того, щоб перейти від якісної оцінки величини ресурсу до кількісної, введемо уявлення про період безпечного функціонування, який, по аналогії з уявленням про типи несправностей та аварійних ситуацій, будемо називати проектним періодом функціонування. Очевидно, що визначення проектного періоду функціонування TO, є однією з вхідних вимог до проектування TO, яка відноситься до ключових вимог. Приймемо, що всі вимоги до TO, який передбачається проектувати, виконуються проектантами. Тому, час експлуатації, який є обов'язковим для TO, можна визначати по параметрах

та ознаках, які передбачають визначення його величини у вигляді відповідної умови. До таких ознак можна віднести наступні:

- кількість користувачів продуктами, які продукують відповідні TP, чи окремі TO (S),
- вартість, або об'єм пошкоджень, до яких може привести виникнення катастрофічних ситуацій на TO, яка визначається природою TP, що реалізується у відповідному TO (k),
- інтегральний параметр, який характеризує допустимі модифікації TP, що реалізується у відповідному TO (m),
- активність факторів, що активізуються оточенням відповідного TO.

Очевидно, що параметр S визначає час експлуатації TO, оскільки, із збільшенням S, необхідно збільшувати кількість продукції, а TP має визначену пропускну здатність. Тому, час експлуатації мусить бути достатньо великим. Особливо це актуально, коли всі користувачі постійно використовують відповідний продукт.

Вартість пошкоджень в оточенні TO, до яких можуть привести аварійні ситуації на TO, також впливає на величину часу експлуатації (TE). Це обумовлюється тим, що при виконанні всіх вимог до TO проектантами, аварійні ситуації трапляються переважно в тих випадках, коли закінчується ресурс окремих вузлів, ключових компонент TO, чи всього TO в цілому, або цей час близький до завершення TE. Чим коротший TE, тим більш ймовірним стає виникнення аварії. Тому, чим більший рівень загрози від TO для оточення, тим більшим повинен бути TE, що зменшує ймовірність виникнення аварій на досить тривалому періоді часу.

Зовнішнє середовище, в залежності від природних процесів, що відбуваються в ньому, може проявляти різну активність по відношенню до TO. Це означає, що відповідне TO зі своїм TE повинно вкладатися в періодичність активності відповідного оточення і цей фактор, на відміну від інших, може обумовлювати зменшення величини TE.

1. *Gartler J.* Fault Detection and Diagnosis in Engineering System. – New York: Marcel Dekker, Inc.
2. *Латышев А.А. Латышев Ф.В.* Диагностирование линейных дискретных систем.// Збірник наук. праць, вип.. 14, «Моделювання та інформаційні технології», Київ – 2002. с.111-117.
3. *Chiang J.H., Russel E.L., Bratz R.D.* Fault Detection and Diagnos in Industrial Systems. London: Springer Verlag, 2001.
4. *Шурыгин А.М.* Прикладная стохастика: робастность, оценивание, прогноз. М.: Финансы и статистика, 2005.
5. *Шурыгин Ф.М.* Математические методы прогнозирования. М.: Горячая Линия – Телеком. 2009.
6. Логический подход к искусственному интеллекту: от классической логики к логическому программированию. М.: Мир, 1990.
7. *Мендельсон Э.* Введение в математическую логику. М.: Наука, 1971.

Поступила 24.02.2011р.