блоків IKSZ і BAAP,

- система управління SZ складається з блоку BUZS і ініціюється системою, що представляє собою OZ. В цьому розумінні будемо в цю систему включати OZ.

1. *Зайцев О. В.* ROOTKITS, SPYWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. — СПБ.: БХВ. Петербург, 2006.
2. *Соколов А. В., Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. — М. ДМК, 2002.
3. *Козлов Д. А., Парандовский А. А., Парандовский А. К.* Энциклопедия компьютерных вирусов. — М.: «Соломон-Р», 2001.
4. *Смит Р. Э.* Аутидентификация: от паролей до открытых ключей. — М.: Издательский дом «Вильямс», 2002.

Поступила 16.08.2010р.

УДК 629.52.7.

О.А. Машков, д.т.н., профессор, ВАК Украины; В.Р. Косенко

ОСОБЛИВОСТІ МОДЕЛЮВАННЯ НЕШТАТНИХ (АВАРІЙНИХ) СИТУАЦІЙ В ІНФОРМАЦІЙНО-КЕРУЮЧИХ КОМПЛЕКСАХ ДИНАМІЧНИХ ОБ'КТІВ КЕРУВАННЯ

Методика виявлення відмов в інформаційно-керуючих комплексах, заснована на використанні «оновлюючих» процесів

Виділимо із загальної задачі виявлення відмов окремий клас задач керування рухом динамічного об'єкта, що містить інформаційно-керуючий комплекс (ІКК), у яких відмови моделюються у вигляді адитивних ефектів у рівняннях стану та спостереження.

Позаштатний стан ІКК моделюється одним з наступних рівнянь:

$$X(k+1) = \Phi(k+1, k)X(k) + W(k) + \vartheta\,\delta(k+1, m); \qquad (1)$$

$$X(k+1) = \Phi(k+1, k)X(k) + W(k) + \vartheta\,1(k+1, m); \qquad (2)$$

$$Y(k) = H(k)X(k) + U(k) + \vartheta\,\delta(k, m); \qquad (3)$$

$$Y(k) = H(k)X(k) + U(k) + \vartheta\,1(k, m), \qquad (4)$$

де ϑ – невідомий вектор, що характеризує величину відмови,

m – невідомий момент її виникнення.

Рівняння (1), (2) описують широке коло моделей відмов, пов'язаних зі зміною динаміки об'єкта за рахунок появи стрибків або зрушень у компонентах вектора стану. Рівняння (4) можна застосовувати для моделювання окремих рідких аномальних вимірів, а рівняння (70) – для опису раптових зрушень (зсувів), що з'являються в інформаційновимірювальній системі ІКК.

Сутність методу виявлення відмов, що використовує «оновлюючі» процеси, полягає в наступному:

Якщо ІКК функціонує нормально, то «оновлюючий» процес $\tilde{Z}(k/k-1) = Y(k) - H(k)\hat{X}(k/k-1)$ в алгоритмі фільтрації являє собою білий гаусівский шум з нульовим середнім і кореляційною матрицею $P_{\tilde{Z}}(k) = H(k)P(k/k-1)H^T(k) + R(k)$. Якщо ж у системі відбуваються відмови, то статистичні характеристики процесу $\tilde{Z}(k/k-1)$ змінюються, і ці зміни можна використовувати для виявлення відмов.

Процедура методу наступна. Сформуємо статистику виду:

$$l(k) = \sum_{j=k-M+I}^{k} \tilde{Z}^T(j/j-1) P_{\tilde{Z}}^{-1}(j) \tilde{Z}(j/j-1), \tag{5}$$

що має розподіл типу X^2 з MS ступенями свободи, де S – розмірність вектора $\tilde{Z}(k/k-1)$, M – число використовуваних реалізацій (ширина рухомого вікна).

Вирішальне правило має вигляд:

$l(k) \le l_0$ – «нормальний режим»;

$l(k) > l_0$ – «відмова».

При цьому варто враховувати, що занадто велике значення призводить до згладжування ефектів, викликаних відмовами в ІКК, занадто мале – до збільшення ймовірності помилкової тривоги.

До недоліків методу варто віднести те, що даний метод виявлення не забезпечує можливості ідентифікації відмов і оцінювання їхньої величини. Цей метод придатний тільки для виявлення досить різких змін у системі, що сильно впливають на статистичні характеристики процесу, що $\tilde{Z}(k/k-1)$ оновлюється.

Розглянемо інший підхід до вирішення даної задачі, позбавлений зазначених недоліків.

Насамперед, оцінимо вплив кожної з моделей відмов (1) – (4) на характеристики процесу, що $\tilde{Z}(k/k-1)$ оновлюється. Вихідні співвідношення алгоритму фільтрації:

$$X(k) = X_1(k) + X_2(k); \qquad \tilde{X}(k/k) = \hat{X}_1(k/k) + \hat{X}_2(k/k);$$

$$Y(k) = Y_1(k) + Y_2(k); \quad \tilde{Z}(k/k-1) = \hat{Z}_1(k/k-1) + \hat{Z}_2(k/k-1),$$

де $X_1(k)$, $\hat{X}_1(k/k)$, $Y_1(k)$, $\hat{Z}_1(k/k-1)$ – складові відповідних векторів, пов'язані з нормальним функціонуванням ІКК, а $X_2(k)$, $\hat{X}_2(k/k)$, $Y_2(k)$, $\hat{Z}_2(k/k-1)$ – складові, обумовлені винятково впливом відмов.

Виразимо останні через параметри ІКК і невідомі величини ϑ і m для кожного з типів відмов (1) – (4). Припустимо, що відмови в ІКК з'являються в момент $k = m$, тоді:

$$X_2(k) = \Phi(k, m)\,\vartheta\,; \quad Y_2(k) = H(k)\Phi(k, m)\,\vartheta\,; \tag{6}$$

$$\hat{X}_2(k) = F(k, m)\,\vartheta\,; \quad \tilde{Z}_2(k / k - 1) = G(k, m)\,\vartheta\,, \tag{7}$$

де матриці $F(k, m)$, $\Phi(k, m)$, $G(k, m)$ відмінні від нуля тільки при $k \geq m$ і задовольняють наступним співвідношенням:

$$\Phi(k + 1, m) = \Phi(k + 1, k)\,\Phi(k, m); \quad \Phi(m, m) = I; \tag{8}$$

$$F(k, m) = \sum_{j=m}^{k} \theta(k, j)K(j)H(j)\,\Phi(j, m); \tag{9}$$

$$G(k, m) = H(k)\,[\Phi(k, m) - \Phi(k, k - 1)\,F(k - 1, m)]. \tag{10}$$

Вхідна в (44) матриця $\theta(k, j)$ може бути обчислена рекурентним чином:

$$\theta(k, m) = [I - K(k)H(k)]\Phi(k, k - 1)\theta(k - 1, m); \tag{11}$$

$$\theta(m, m) = I.$$

Далі, оновлюваний процес узгоджується з гіпотезами відсутності (H_0) і наявності відмов у ІКК (гіпотеза H_1):

$$H_0\text{:}\ \tilde{Z}(k / k - 1) = \tilde{Z}_1(k / k - 1)\,; \tag{12}$$

$$H_1\text{:}\ \tilde{Z}(k / k - 1) = G(k, m)\,\vartheta + \tilde{Z}_1(k / k - 1)\,, \tag{13}$$

де $\tilde{Z}_1(k / k - 1)$ – білий гаусівский шум з нульовим середнім і кореляційною матрицею $P_{\tilde{Z}}(k)$.

Оскільки в отриманому вирішальному правилі розподілу ймовірностей величини ϑ і m невідомі, то для вирішення загальної задачі виявлення відмов, що включає їхню ідентифікацію й оцінювання, можна скористатися критерієм узагальненого відношення правдоподібності.

Ідея застосування цього критерію припускає наступні два етапи:

1. Визначення оцінок максимальної правдоподібності вектора $\hat{\vartheta}$ і моменту виникнення відмови $\hat{m}$ в припущенні справедливості гіпотези H_1.

2. Обчислення на основі $\hat{\vartheta}$, $\hat{m}$ звичайного відношення правдоподібності для перевірки гіпотез H_1, H_0.

Оцінки $\hat{\vartheta}$ і $\hat{m}$ знаходяться з умови:

$$\hat{\vartheta}(k),\ \hat{m}(k) = \underset{\vartheta,\mathrm{m}}{\arg}\ \max f[\tilde{Z}(1/0),\ldots,\tilde{Z}(k / k - 1)H_1,\ \vartheta\,,\ m]. \tag{14}$$

Узагальнене відношення правдоподібності:

$$\lambda(k) = \frac{f[\tilde{Z}(1/0),\ldots,\tilde{Z}(k / k) / H_1, \vartheta = \hat{\vartheta}, m = \hat{m}]}{f[\tilde{Z}(1/0),\ldots,\tilde{Z}(k / k - 1) / H_0]}. \tag{15}$$

Вирішальне правило при цьому має вигляд:

$$\lambda(k) \underset{H_0}{\overset{H_1}{\gtrless}} \eta, \tag{16}$$

де η – поріг ухвалення рішення, зумовлений виходячи з умови забезпечення заданого рівня помилкових тривог.

При цьому

$$\vartheta(k) = P_{\vartheta}^{-1}(k,\hat{m}(k))Z(k,\hat{m}(k));$$

$$P_{\vartheta}(k,m) = \sum_{j=1}^{k} G^T(j,m)P_{\tilde{Z}}^{-1}(j)G(j,m); \tag{17}$$

$$Z(k,m) = \sum_{j=1}^{k} G^T(j,m)P_{Z}^{-1}(j)\tilde{Z}(j/j-1).$$

За допомогою (17) знайдемо узагальнений показник правдоподібності:

$$\lambda(k, \hat{m}(k)\ (k)) = 2\ln\lambda(k) = \max Z^T(k, m)\, P_{\vartheta}^{-1}\ (\mathrm{k, m})\mathrm{Z(k, m)},\ \mathrm{m} \le \mathrm{k}. \tag{18}$$

Остаточне вирішальне правило набирає вигляду:

$$\lambda(k,\hat{m}(k)) \underset{H_0}{\overset{H_1}{\gtrless}} 2\ln\eta = \eta_0. \tag{19}$$

Оптимальний алгоритм виявлення–ідентифікації–оцінювання позаштатних ситуацій ІКК може бути реалізований за допомогою наступної структурної схеми (рис. 1):

До недоліку даного оптимального алгоритму варто віднести нескінченно зростаючий обсяг обчислень. Цього можна уникнути, обмеживши аналізований часовий інтервал рухомого вікна шириною M. Тоді оцінку $\hat{m}(k)$ варто шукати тільки в межах тимчасового проміжку $k - M < \hat{m}(k) \le k$.

Якщо ширина вікна M досить велика, щоб забезпечити виявлення найбільш істотних відмов, то таке погіршення не призводить до помітного погіршення характеристик даного алгоритму.

У цьому випадку доцільно величини $P_{\vartheta}(k,m), Z(k,m)$ обчислювати рекурентно:

$$P_{\vartheta}(k, m) = G^T(k, m)\, P_{\tilde{Z}}^{-1}\ (k)G(k, m) + P_{\vartheta}\ (k-1, m); \tag{20}$$

$$Z(k, m) = G^T(k, m)\, P_{\tilde{Z}}^{-1}\ (k)\, \tilde{Z}\ (k/k-1, m), \tag{21}$$

причому

$$G(k, m) = H(k)[\Phi(k, m) - \Phi(k, k-1) + F(k-1, m)]; \tag{22}$$

$$F(k, m) = K(k)G(k, m) + \Phi(k, k-1)F(k-1, m). \tag{23}$$

Запропонована методика дозволяє реалізувати обговорювані ідеї в ІКК при обмежених обчислювальних ресурсах.

Ідентифікація позаштатних ситуацій в ІКК на основі розрізнення багатьох гіпотез

Для моделей відмов ІКК, що не можуть бути описані адитивними ефектами в рівняннях стану та спостереження, розглянутий вище алгоритм малопридатний, оскільки при цьому неможливо в загальному випадку отримати явний вираз для матриці $G(k, m)$. Безпосереднє узагальнення даного підходу може бути отримане на основі використання статистичних методів розрізнення багатьох гіпотез.

Розглянемо вирішення загальної задачі ідентифікації позаштатних ситуацій стосовно до ІКК, у яких відмови моделюються стрибкоподібними змінами кожного з N параметрів.

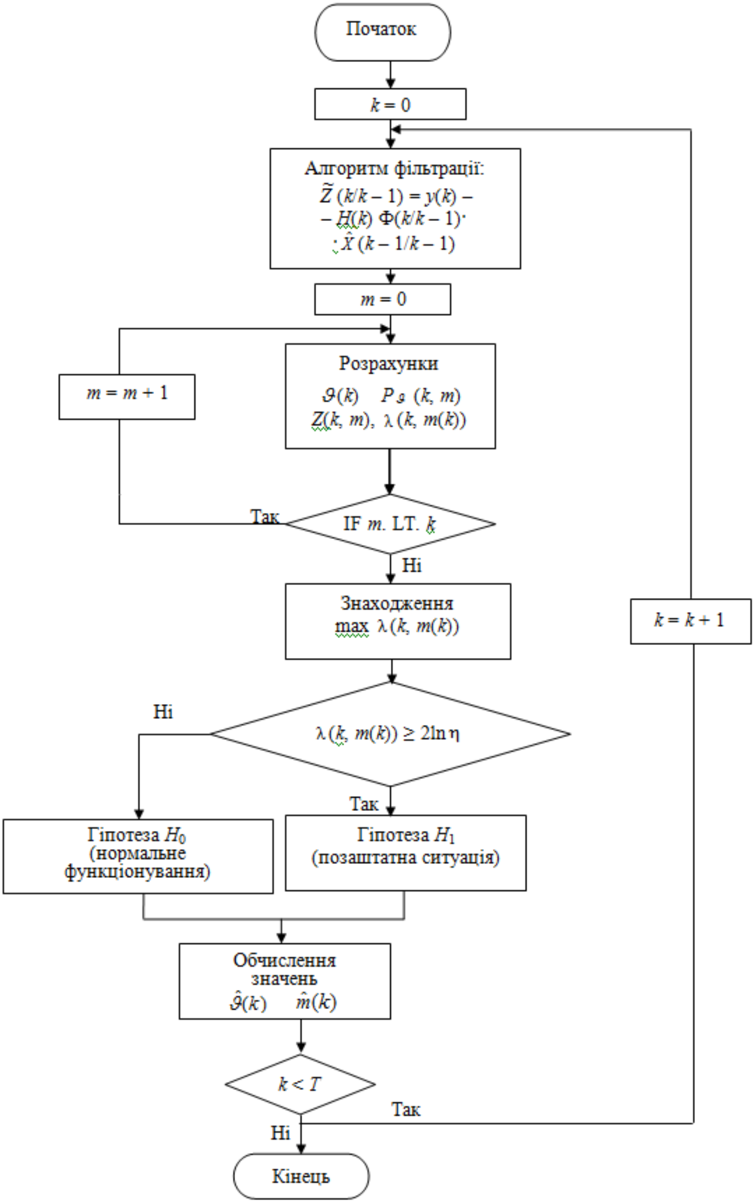

Рис.1 – Оптимальний алгоритм виявлення позаштатних ситуацій в ІКК

Вважаємо, що в режимі нормального функціонування ІКК (гіпотеза H_0) описується різницевими рівняннями:

$$X(k+1) = \Phi(k+1, k)X(k) + B(k+1, k)U(k) + W(k);$$
$$Y(k) = H(k)X(k) + D(k)U(k) + V(k),$$

в яких усі параметри $\vartheta_i^{(0)}, i = \overline{1, N}$, що визначають матриці $\Phi(k+1, k)$, $H(k)$, $D(k)$, $B(k+1, k)$ і вектори $W(k)$ і $V(k)$, задані.

Нехай у випадкові моменти часу m_i, ймовірнісні характеристики яких невідомі, *j*-й параметр $i = \overline{1, N}$ зазнає стрибкоподібних змін, приймаючи одне з S дискретної множини значень $\vartheta_i^{(j)}, j = \overline{1, S}$, причому:

$$\vartheta_i^{(j)}(m_i) - \vartheta_i^{(0)}(m_i) = \vartheta_i(m_i), \tag{25}$$

– величина стрибка відповідного параметра.

Припустимо, що стрибки відбуваються зрідка, і в розпорядженні є досить часу для їхнього виявлення, ідентифікації й оцінювання, і що протягом цього часу виникає тільки одна відмова.

Позначимо через $H_1(i, m_i, j)$ гіпотезу, що полягає в тому, що *j*-й параметр, який стрибкоподібно змінився в момент часу m_i, набув значення $\vartheta_i^{(j)}$. У цьому випадку загальна задача вияву відмови зводиться до задачі розрізнення $NSk + 1$ гіпотез. Оскільки k – дискретний час, то число розрізнених гіпотез зі зростанням k необмежено зростає. Тому обмежимо інтервал ухвалення рішення тимчасовим проміжком $k - M + 1 < m_i \le k$.

Для вирішення поставленої задачі скористаємося критерієм узагальненого відношення правдоподібності, що дозволяє не тільки знайти сам факт виникнення відмови, але й оцінити значення:

– $\hat{i}$ – визначити, який саме параметр змінився;

– $\hat{m}_i$ – зафіксувати момент виникнення відмови;

– $\hat{j}$ – знайти величину стрибка (відмови).

Узагальнене відношення правдоподібності в розглянутому випадку можна записати:

$$\lambda(k) = \frac{f[Y(k-M+1),...,Y(k)/H_1(i=\hat{i}, m_i=\hat{m}_i, j=\hat{j})]}{f[f(k-M+1,...,Y(k)/H_0]}, \tag{26}$$

де оцінки $\hat{i}, \hat{m}_i, \hat{j}$ визначаються в такий спосіб:

$$\hat{i}, \hat{m}_i, \hat{j} = \underset{i, m_i, j}{\arg\max} f[Y(k-M+1),...,Y(k)/H_1(i, mi, j)]. \tag{27}$$

Знайдемо вираз умовних щільностей розподілу, що входять у (61).

Застосовуємо правило Байєса:

$$f[Y(k-M+1), \ldots, Y(k)/H_0] = f[Y(k-M+1)/H_0] \cdot \tag{28}$$
$$\cdot f[Y(k-M+2)/Y(k-M+1), H_0] \cdot \ldots \cdot f[Y(k)/Y(k-1), \ldots, Y(k-M+1), H_0].$$

Робимо припущення про те, що кожен із співмножників, що входять у вираз (64), являє собою гаусівську щільність. Тоді:

$$f[Y(k-M+1), \ldots, Y(k)/H_0] = \prod_{n=k-M+1}^{k} N[H(n)\,\hat{X}\,(n/n-1), H_0), P_{\tilde{Z}}\,(n/H_0)] \quad (29)$$

Аналогічно, для чисельника виразу (62) маємо:

$$f[Y(k-M+1), Y(k-m+2), \ldots, Y(k)/H_1(\hat{i}, \hat{m}_i, \hat{j})] =$$

$$= \prod_{n=k-M+1}^{k} N[H(n)\,\hat{X}\,(n/n-1), H_1(\hat{i}, \hat{m}_i, \hat{j})], P\,\tilde{Z}\,(n/H_1(\hat{i}, \hat{m}_i, \hat{j}))]. \qquad (30)$$

Підставляючи (28), (29) у вираз (26), отримуємо наступний вираз для логарифма узагальненого відношення правдоподібності:

$$\lambda(k, i, m_i, j) = 2\ln \lambda(k) =$$

$$\sum_{n=m_i}^{k} [\tilde{Z}^T(n/n-1, H_0) P_{\tilde{Z}}^{-1}(n/H_0)\tilde{Z}(n/n-1, H_0) - \tilde{Z}^T(n/n-1, H_0) -$$

$$-\tilde{Z}^T[n/n-1, H_1(i, m_i, j)]P_{\tilde{Z}}^{-1}[n/H_1(i, m_i, j)]\tilde{Z}[n/n-1, H_1(i, m_i, j)] + \ln\det P_{\tilde{Z}}(n/H_0) -$$

$$-\ln\det P_{\tilde{Z}}\,(n/H_1(i, m_i, j))]. \qquad (31)$$

Максимально правдоподібну оцінку $\hat{i}, \hat{m}_i, \hat{j}$ можна визначити з умови:

$$\hat{i}, \hat{m}_i, \hat{j} = \max_{i, m_i, j} \lambda(k, i, m_i, j). \qquad (32)$$

Вирішальне правило в даному випадку має вигляд:

$$\lambda(k, \hat{i}, \hat{m}_i, \hat{j}) \underset{H_0}{\overset{H_1(i, m_i, j)}{\gtreqless}} \eta_0\ , \qquad (33)$$

де значення $\hat{m}_i$ належить інтервалу $k - M + 1 < \hat{m}_i < k$.

Блок-схема цього алгоритму, побудована у відповідності до вирішального правила (33), показана на рис.2. Схема включає $NSM + 1$ паралельно працюючих фільтрів, кожен з яких погоджений з відповідною гіпотезою $H_1(i, m_i, j)$.

Слід зазначити, що при великих значеннях N, M, S розглянутий алгоритм виявлення–ідентифікації потребує значного обсягу обчислень і практично може бути використаний тільки в процесі проектування ІКК для оцінювання ефективності спрощених процедур виявлення відмов. Тому практичне використання розглянутого алгоритму може бути можливе, якщо кількість змінюваних параметрів невелике ($i = 1, 2$), а сприймані значення у стані відмови відомі, причому S – невелике ($j = 1, 2$).

Структурна схема системи, що забезпечує реалізацію алгоритмів виявлення–ідентифікації відмов у ІКК, показана на рис.3. Дана система містить оптимальний фільтр, погоджений з параметрами нормально функціонуючої ІКК, пристрій виявлення, оцінювання, ідентифікації. З появою у вимірах $Y_i(k)$, $i = 1, S$ випадкового зсуву (відмова, позаштатна ситуація) за допомогою відповідного алгоритму визначається момент відмови $\hat{m}_i$, канал відмови $i = 1,S$, дискретна величина зсуву $\hat{F}_j(k),\ j = \overline{1, N}$ і замикається ланцюг компенсації оптимального фільтра, за яким на віднімаючий вхід суматора надходить оцінка цього зсуву $\hat{F}_i(k)$.

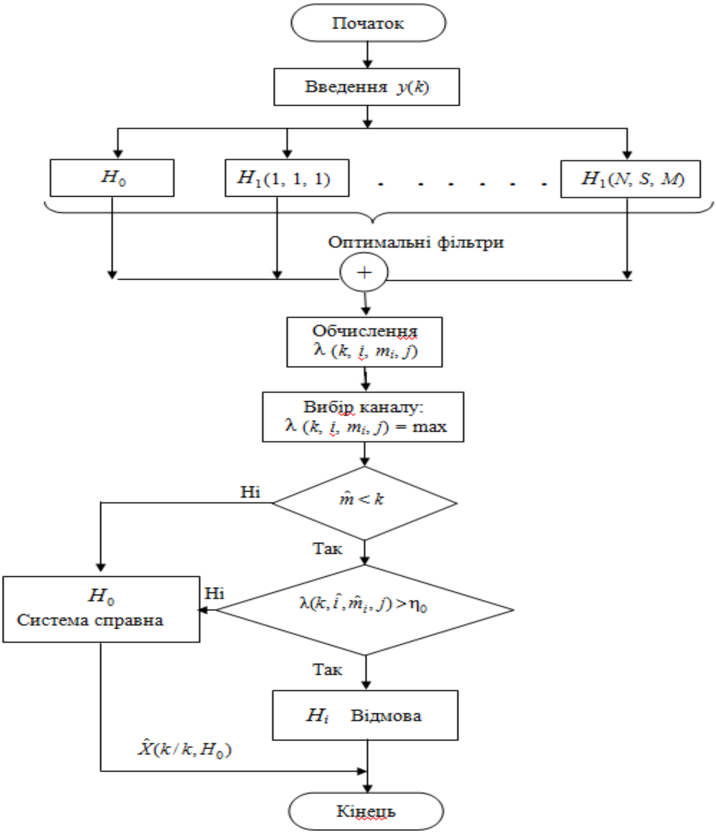

Рис.2 – Блок схема алгоритму ідентифікації

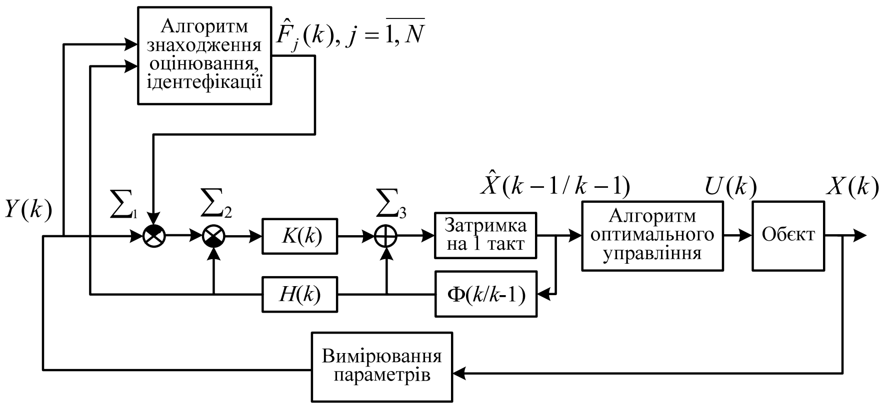

Рис.3 – Структурна схема алгоритму виявлення ідентифікації відмов у ІКК

Метод виявлення відмов на основі розрізнення багатьох гіпотез уможливлює вирішення задач діагностування нелінійних бортових інформаційно-керуючих комплексів.

1. *Машков О.А., Кравченко Ю.В., Савченко В.А.* Синтез високоточної радіонавігаційної системи на основі метода аналізу ієрархій показників якості / Зб. наук. пр. НАН України, ІПМЕ – „Моделювання та інформаційні технології”, 2003, Вип.. 22, с. 41- 48.
2. *Машков О.А. Чумакевич В.О., Шуренок В.А.* Шляхи створення та дослідження функціонально-стійкої моделі вимірювально-обчислювального комплексу/Зб. наук. пр. НАН України, ІПМЕ – „Моделювання та інформаційні технології”, 2003, Вип.. 24, с. 40- 47.
3. *Машков О.А., Барабаш О.В.*Топологічні критерії та показники функціональної стійкості складних ієрархічних систем /Зб. наук. пр. НАН України, ІПМЕ – „Моделювання та інформаційні технології”, 2003, Вип.. 25, с. 29-35.
4. *Машков О.А., Кононов О.А.* Возможности обеспечения функциональной устойчивости эргатических систем управления в рамках существующего методического аппарата / Зб. наук. пр.: ІПМЕ Вип. 32, Київ, 2006, с.151-157.
5. *Азарсков В.М., Дурняк Б.В., Кондратенко С.П., Машков О.А.* Анализ возможних вариантов построения функционально устойчивого комплекса управления дистанционно пилотируемыми летательными аппаратами с применением псевдоспутниковых технологий / Зб. наук. пр.: ІПМЕ НАН України, вип. 42, 2007, с. 28-40.
6. *Азарсков В.М., Дурняк Б.В., Кондратенко С.П., Машков О.А.* Проблемы построения моделей функционально устойчивого комплекса управления дистанционно пилотируемыми летательными аппаратами с применением псевдоспутниковых технологий / Моделювання та ынформацыйны технології / ІПМЕ НАН України, вип. 43, 2007, с. 118-127.
7. *Машков О.А., Усаченко Л.М.* Теоретические основы построения функционально-устойчивой автоматизированной системы обслуживания воздушного движения (терминология и модели) / Моделювання та інформаційні технології / ІПМЕ НАН України, вип. 47, 2008, с. 3-17.
8. *Дурняк Б.В., Машков О.А., Усаченко Л.М., Сабат В.І.* Методологія забезпечення функціональної стійкості ієрархічних організаційних систем управління / Зб. наук. пр.: ІПМЕ НАН України, вип. 48, 2008, с. 3-21.

Поступила 6.09.2010р.