Ключові слова: багатотактний ватметр, адитивна похибка, вплив завади, період інтегрування, фаза сигналу.

Ларин Виталий Юрьевич, *доктор технических наук, профессор, кафедра информационно-измерительной техники, Национальный технический университет Украины «Киевский политехнический институт», Украина,* ***e-mail: vjlarin@gmail.com****.*
Синицкий Олег Павлович, *кандидат технических наук, доцент, кафедра информационно-измерительной техники, Национальный технический университет Украины «Киевский политехнический институт», Украина.*
Щербань Анастасия Павловна, *аспирант, кафедра информационно-измерительной техники, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Ларін Віталій Юрійович, *доктор технічних наук, професор, кафедра інформаційно-вимірювальної техніки, Національний технічний університет України «Київський політехнічний інститут», Україна.*
Синицький Олег Павлович, *кандидат технічних наук, доцент, кафедра інформаційно-вимірювальної техніки, Національний технічний університет України «Київський політехнічний інститут», Україна.*
Щербань Анастасія Павлівна, *аспірант, кафедра інформаційно-вимірювальної техніки, Національний технічний університет України «Київський політехнічний інститут», Україна.*

Larin Vitaliy, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,* ***e-mail: vjlarin@gmail.com****.*
Sinitskiy Oleh, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine.*
Shcherban Anastasia, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine*

УДК 543.272.082.5(088.8)

Безрук З. Д.,
Порєв В. А.,
Приміський В. П.

МОДЕЛІ ДІАГНОСТУВАННЯ І ПІДВИЩЕННЯ НАДІЙНОСТІ ГАЗОАНАЛІТИЧНИХ СИСТЕМ

Розглянуто методологію діагностування багатоканальних газоаналітичних систем і визначена ефективність їх роботи. Проаналізовані причини втрат вимірювальної інформації. Запропонована методологія визначення часу відновлення роботи газоаналітичної системи. Наведені залежності дії тестового сигналу на вихідний сигнал газоаналізатора. Проведено порівняння тестового і функціонального діагностування, визначено середні часові характеристики роботи і відновлення систем.

Ключові слова: *методологія діагностування, багатоканальні газоаналітичні системи, вимірювальна інформація, мікропроцесорні системи (МПС).*

1. Вступ

Підвищення екологічних вимог до промислових і енергетичних підприємств, що викидають в атмосферу значні обсяги димових (відпрацьованих) газів вимагає застосування відповідних інструментальних засобів контролю складу і концентрацій газів — автоматизованих багатоканальних газоаналітичних систем (ГАС). Для обґрунтування застосування ГАС в конкретному технологічному процесі необхідно визначити її ефективність і надійність.

2. Постановка задачі

Ефективність ГАС, як інформаційно вимірювальної системи (ІВС) залежить від втрат вимірювальної інформації, обумовлених її обмеженою точністю, надійністю, швидкодією. Показники ефективності, які враховують згадані фактори, являються інтегральною мірою якості — $W(t)$ ГАС [1]. Для лінійної стаціонарної не відновлюваної ГАС при нормальному розподілу вхідного сигналу x в білому Гаусовому шумі при $\sigma_x^2 \gg \sigma_\varepsilon^2$:

$$W(t)=\frac{J_X(t)-\Delta J(t)}{J_X(t)}=\frac{FW_{\text{H}}(t)}{2\Omega}\left(1-\frac{\ln\sigma_\varepsilon\sqrt{2\pi l}}{\ln\sigma_X\sqrt{2\pi l}}\right), \qquad (1)$$

де $J_X(t)$ — кількість інформації на вході ГАС за час роботи t; $J_Y(t)$ — кількість інформації на виході ГАС за час роботи t; $\Delta J = J_X(t) - J_Y(t)$ — сумарні втрати інформації ГАС за час t із-за обмеженої точності і надійності ГАС; F — полоса пропускання ГАС; Ω — максимальна частота спектра змін параметрів джерела вхідної інформації; σ_x^2 — дисперсія шуму; σ_ε^2 — дисперсія вхідного сигналу; $W_{\text{H}}(t)=t_1/t$ — показник ефективності, що враховує надійність ГАС; t_1 — час роботи ГАС до відмови.

Ціллю статті є довести, що самодіагностика ГАС з використанням МПП дозволяє реалізувати оптимальні для конкретної ГАС алгоритми пошуку дефектів як по жорсткій або гнучкій послідовній програмі, так і комбінованій. Таким чином, для організації самодіагностики ГАС і підвищення значення $W(t)$ необхідно розглянути наступні задачі.

3. Аналіз літератури

Газоаналітичні системи є складними багатоканальними інормаційно-вимірювальними системами. Системи можуть будуватись по паралельній, послідовній і паралельно-послідовній структурі вимірювальних каналів.

В таких системах відмова одного з елементів, приладів системи приводить до лавиноподібного наростання

відмов і система виходить з ладу. В відповідних літературних джерелах, розглянуті загальні принципи функціонування і діагностування багатопараметрових вимірювальних систем [1, 2]. Специфіка ж роботи газоаналітичних систем, особливо які працюють на промислових підприємствах для контролю димових, відпрацьованих токсичних, вибухонебезпечних газів потребує розробки більш конкретних алгоритмів і методів функціонування і діагностування ГАС.

4. Методологія визначення часу відновлення ГАС після відмови

Інтервал часу для діагностування і відновлення функціонування ГАС після відмови визначиться як:

$$t = \sum_{i=1}^{n} t_i + \sum_{i=1}^{n} t_{\text{ВО}i} + t_n, \qquad (2)$$

де t_i — час роботи ГАС між $i-1$ і i-ю відмовами; $t_{\text{ВО}i}$ — загальний час відновлення ГАС після i-ї відмови; t_n — час роботи ГАС після відновлення i-ї відмови; n — число відмов ГАС за час t.

Загальний час відновлення ГАС можна представити:

$$\sum_{i=1}^{n} t_{\text{ВО}i} = \sum_{i=1}^{n} t_{ki} + \sum_{i=1}^{n} t_{\text{Д}i} + \sum_{i=1}^{n} t_{\text{В}i}, \qquad (3)$$

де t_{ki} — час контролю ГАС витрачений на знаходження i-ї відмови з урахуванням не миттєвого знаходження відмови; $t_{\text{Д}i}$ — час діагностування ГАС після i-ї відмови; $t_{\text{В}i}$ — час відновлення (ремонту або переключення на резервні блоки) після i-ї відмови.

Інтервал часу справної роботи ГАС визначається як:

$$\sum_{i=1}^{n} t_i + t_n = t - \sum_{i=1}^{n} t_{\text{ВО}i}. \qquad (4)$$

Підставивши рівняння (3) в (1) отримаємо:

$$W(t)_{\text{В}} = \frac{F\left(t - \sum_{i=1}^{n} t_{\text{ВО}i}\right)}{2\Omega T}\left(1 - \frac{\ln \sigma_\varepsilon \sqrt{2\pi l}}{\ln \sigma_X \sqrt{2\pi l}}\right). \qquad (5)$$

Із виразу (5) видно, що $W(t)$ залежить від загального часу відновлення ГАС. При відсутності спеціалізованих засобів час загального відновлення ГАС складає 70—80 % загального часу відновлення [1, 2], тому для підвищення значення $W(t)$ необхідно зменшити час локалізації дефекту шляхом автоматизації процесу діагностування. Це дозволить знизити чисельність обслуговуючого персоналу і знизити вимоги до його кваліфікації.

Сучасні багатоканальні ГАС будуються на основі мікропроцесорних систем (МПС), які мають значні можливості по автоматизації і оптимізації вимірювального процесу, а також дозволяють оперативно обробляти інформацію. В зв'язку з цим для поліпшення значення $W(t)$, скорочення витрат на обслуговування ГАС і для ефективного використання МПС економічно обґрунтованим і технічно доцільним становиться організація само діагностики ГАС.

5. Функціональна і тестова самодіагностика ГАС

Як об'єкт контролю і діагностування ГАС в загальному випадку являється складною, багатомірною, розосередженою в просторі, неоднорідною інформаційно-вимірювальною системою зі складним алгоритмом роботи. Ці Інформацію, яка необхідна для локалізації дефектів ГАС з точністю до змінного блоку, можна представити як:

$$J = J_{\text{И}} + J_{\text{К}} + J_{\text{Д}}, \qquad (6)$$

де $J_{\text{И}}$ — інформація про стан ГАС отримана з метою підвищення точності вимірів; $J_{\text{К}}$ — інформація, отримана в результаті контролю працездатності ГАС; $J_{\text{Д}}$ — додаткова інформація, необхідна для локалізації дефектів ГАС з точністю до змінного блоку:

$$J_{\text{Д}} = J - J_{\text{И}} - J_{\text{К}}. \qquad (7)$$

З виразу видно, що для організації оптимального діагностування ГАС необхідно використовувати інформацію $J_{\text{И}}, J_{\text{К}}$ [2]. Окрім того необхідні додаткові засоби для отримання $J_{\text{Д}}$.

Інформація $J_{\text{Д}}$ може бути отримана, як в процесі функціонування ГАС (функціональна діагностика), так і шляхом організації тестових впливів на основі додаткової апаратури (тестове діагностування).

Для порівняння тестового і функціонального діагностування визначимо середні часові характеристики роботи і відновлення ГАС. Припустимо, що $t_n = 0$, тоді:

$$t = \sum_{i=1}^{n} t_i + \sum_{i=1}^{n} t_{\text{ВО}i}, \qquad (8)$$

а узагальнений час роботи ГАС з урахуванням часу відновлення:

$$T = \frac{1}{n}\left(\sum_{i=1}^{n} t_i + \sum_{i=1}^{n} t_{\text{ВО}i}\right). \qquad (9)$$

Звідси $t = nT$. Середній сумарний час відновлення:

$$T = \frac{1}{n}\sum_{i=1}^{n} t_{\text{ВО}i} = T_{\text{К}} + T_{\text{Д}} + T_{\text{В}}, \qquad (10)$$

де $T_{\text{К}}$ — середній час контролю при n відмовах ГАС; $T_{\text{Д}}$ — середній час діагностування при n-відмовах; $T_{\text{В}}$ — середній час відновлення при n відмовах.

$$W(t)_C = \frac{F(T - T_{\text{ВО}})}{2\Omega T}\left(1 - \frac{\ln \sigma_\varepsilon \sqrt{2\pi l}}{\ln \sigma_X \sqrt{2\pi l}}\right). \qquad (11)$$

Узагальнений час тестового діагностування:

$$T_{\text{ДТ}} = T_{\text{Т}} + T_{\text{О}}, \qquad (12).$$

де $T_{\text{Т}}$ — середній час тестування; $T_{\text{О}}$ — середній час обробки.

Середній час функціонального діагностування $T_{\text{ДФ}} = T_{\text{О}}$, тому що $T_{\text{Т}} = 0$.

Велике значення $T_{\text{Т}}$ зменшує інтегральну ефективність ГАС, тому в ГАС з урахуванням рівняння (7)

доцільно використовувати функціональне діагностування і швидкодіючі, економічні тестові методи локалізації дефектів [3, 4]. Одним з головних питань розробки газоаналізаторів з тестовим сигналом є вибір тривалості тестового сигналу і частоти його повторення. Очевидно, що час тривалості тестового сигналу повинний бути достатнім для того, щоб вихідний сигнал газоаналізатора мав стале значення, яке визначається концентрацією вимірюваного газового компонента і дією тестового сигналу. В ході експериментальних досліджень тестового сигналу на газоаналізаторах, які реалізують різні методи газового аналізу: термомагнітний (вимір O_2), термокондуктометричний (вимір H_2), інфрачервоної спектроскопії (CO, CO_2,), хемілюмінесцентний (вимір NO_x) і т. і. встановлено, що для упевненої фіксації тестового сигналу необхідно, щоб його тривалість була не менш ніж в два рази більше часу перехідного процесу ПВП [5, 6]. Істотним аспектом побудови газоаналізаторів з тестовим сигналом є вирішення питання про існування, форму і тривалість тестового газового імпульсу сигналу в різних газопроводах. Відповіддю на нього може служити рішення рівняння поширення тестового сигналу як домішки по газопроводах, що може бути представлено рівнянням дифузії виду:

$$\frac{\partial c}{\partial t}+V(x,y,z)\frac{\partial c}{\partial z}=D\left[\frac{\partial^2 c}{\partial x^2}+\frac{\partial^2 c}{\partial y^2}+\frac{\partial^2 c}{\partial z^2}\right] \qquad (13)$$

з відповідними начальними і граничними умовами при ламінарному плині газу, тут вісь Z збігається з віссю газового каналу, $c=c(t,x,y,z)$ — концентрація тестового сигналу, $V(x,y,z)$ — швидкість потоку газу, D — коефіцієнт молекулярної дифузії [7, 8]. Зокрема, при розгляді циліндричного газового каналу, (як найбільш поширеного,) в припущенні симетричності дії тестового сигналу щодо циліндричної осі газопроводу, рівняння (13) у циліндричній системі координат здобуває вигляд:

$$\frac{\partial V}{\partial t}+V(z)\frac{\partial c}{\partial z}=D\left[\frac{\partial^2 c}{\partial x^2}+\frac{\partial^2 c}{\partial y^2}+\frac{\partial^2 c}{\partial z^2}\right] \qquad (14)$$

із граничною умовою

$$\left.\frac{\partial A}{\partial z}\right|_{z=0}=\left.\frac{\partial c}{\partial z}\right|_{z=R},$$

де R — радіус труби газопроводу.

Про вирішенні виразу наближеними методами рішення може бути зведене до одномірної задачі поширення середньої концентрації, яке описується рівнянням:

$$Q=\frac{2}{R^2\int\limits_0^R c\cdot z\partial z}, \qquad (15)$$

що описується рівнянням:

$$\frac{\partial Q}{\partial t}+U_0\frac{\partial Q}{\partial z}=\mu\frac{\partial^2 Q}{\partial z}, \qquad (16)$$

де $\mu=D\left(1+\frac{R^2}{48D^2}\right)$ — ефективний коефіцієнт дифузії, а U_0 є середня швидкість потоку газу [9, 10].

Графічні результати чисельного рішення на ПЕОМ рівняння (16) приведені на рис. 1.

При розрахунку передбачалося, що тестовий сигнал вводиться в газовий канал в точці Z_0 (тобто по продольній осі газопроводу) протягом часу $T_к$. Урахування довжини газопроводу L для цікавлячих нас значень часу 1—3 сек. тестового сигналу не привів до істотних змін результатів, що пояснюється ефективною дифузією за рахунок розходження швидкостей тестового сигналу і аналізованої суміші у газовому потоці і наявності молекулярної дифузії. Це дозволяє зробити висновок, що циліндрична о форма газопроводу для введення тестового сигналу зонда є найбільш оптимальною.

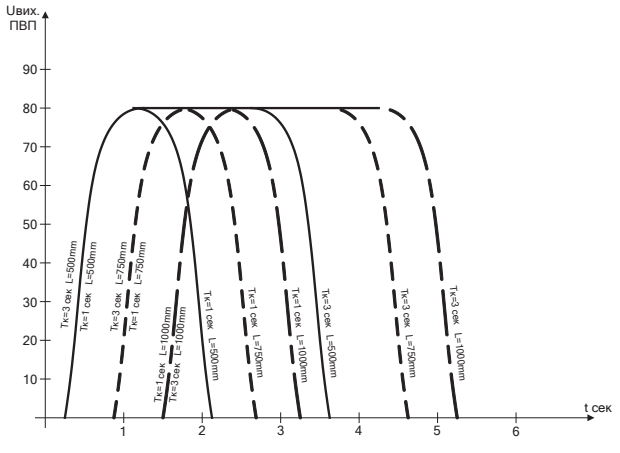

Рис. 1. Графіки дії тестового сигналу, залежність значення $U_{вих}$ від часу t

Аналіз рис. 1 наочно показує, що на визначеному відрізку газопроводу каналу можна говорити про тестовий сигнал як про інформаційно і метрологічно достовірний. За цим відрізком тестовий сигнал у значній мірі розмивається і не може служити в якості інформаційного.

Запропонована методологія побудови газоаналізаторів з тестовим сигналом не компенсує адитивну похибку. Однак, приймаючи до увагу той факт, що адитивна похибка газоаналізаторів, як правило, не перевищує мультиплікативну похибку і визначається процесами в ПВП (що змінюються повільно), адитивну похибку перевіряти і коректувати треба набагато рідше, ніж мультиплікативну. Таким чином, з метою компенсації адитивної похибки ПГС — нульовий газ необхідний, але в значно менших кількостях, чим для газоаналізаторів, побудованих за традиційною схемою прямого перетворення.

Самодіагностика передбачує використання засобів самої ГАС для локалізації дефектів, тому необхідно виділити діагностичне ядро. Ядро повинно мати гарантовану працездатність і бути зв'язаним з усіма іншими підсистемами. Цим вимогам відповідає мікропроцесорний пристрій (МПП) з розвиненою системою контролю і діагностування. На сучасному етапі в ГАС застосовуються як централізовані, так і децентралізовані МПП обробки інформації і керування [4]. Вочевидь, що система діагностування ГАС буде повторювати структуру МПП. При централізованій структурі МПП ГАС основне навантаження по прийому і обробці діагностичної інформації буде повторювати структуру МПП.

Окрім того, ускладнюються ланцюги зв'язків з контрольними і діагностичними сенсорами, що потребує стискування діагностичної інформації. При децентралізованій системі МПП ГАС навантаження по прийому і обробці діагностичної інформації розподіляється між локальними засобами діагностування, що суттєво розвантажує центральний МПП і дозволяє спростити передачу діагностичної інформації з ГАС.

Структурна схема ГАС з централізованою обробкою і керуванням представлена на рис. 2. В МПП входить мікропроцесор (МП), перепрограмований запам'ятовуючий пристрій (ППЗП), аналого-цифровий перетворювач (АЦП), цифро-аналоговий перетворювач (ЦАП), мультиплексом аналоговий (МА), пристрій паралельного вводу інформації (ППВІ), пристрій паралельного виводу інформації (ППВ), пристрій відображення інформації (ПВІ) [8].

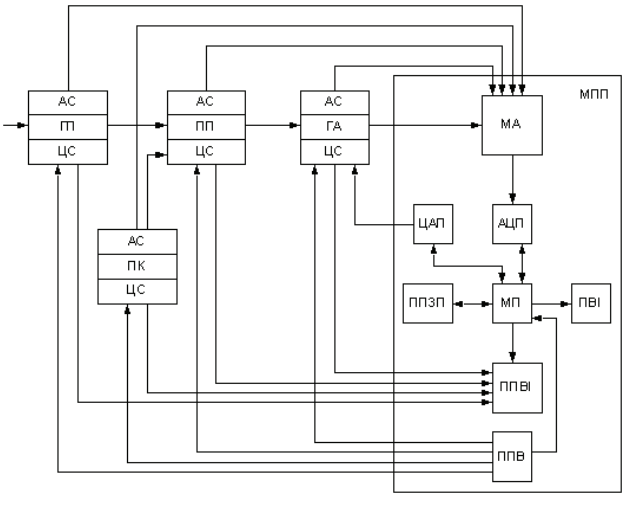

Рис. 2. Структурна схема ГАС з самодіагностикою

Для організації діагностування ГАС необхідні додаткові апаратні засоби цифрові (ЦС) і аналогові (АС) сенсори, які встановлені в пристроях газо (ГП) і пробо підготовки (ПП), газоаналізаторах (ГА), пристроях калі бровки (ПК). Прийом інформації з АС потребує збільшення каналів (ППВІ).

Окрім того, для організації тестових впливів необхідно збільшити число каналів ППВ і ЦАП. Також необхідно відмітити, що в МПП без розвиненої системи контролю і діагностування присутня природна надмірність ліній вводу і виводу інформації. Для збереження діагностичних програм потрібен додатковий об'єм ППЗП. З ЦС і АС в МПП надходить інформація про стан газового тракту (тиск, витрати, температура, вологість і т. і.), електричного і інформаційного трактів. Спрощений алгоритм роботи ГАС з функціональним діагностуванням наведено на рис. 3.

На всіх режимах роботи ГАС на кожному j такті роботи здійснюється порівняння інформації яка надходить з ЦС і АС про стан S^k_j системи з еталонним станом S^k_j, які зберігаються ППЗП. Якщо $S^k_j \neq S^k_j$, то вмикається підпрограма локалізації несправності (дефекта) ГАС. Локалізація відбувається на основі діагностичної моделі ГАС. В зв'язку з тим, що до складу ГАС входять елементи як безперервної так дискретної дії, то найбільш підходящими діагностичними моделями будуть функціональна і логічна [9, 10].

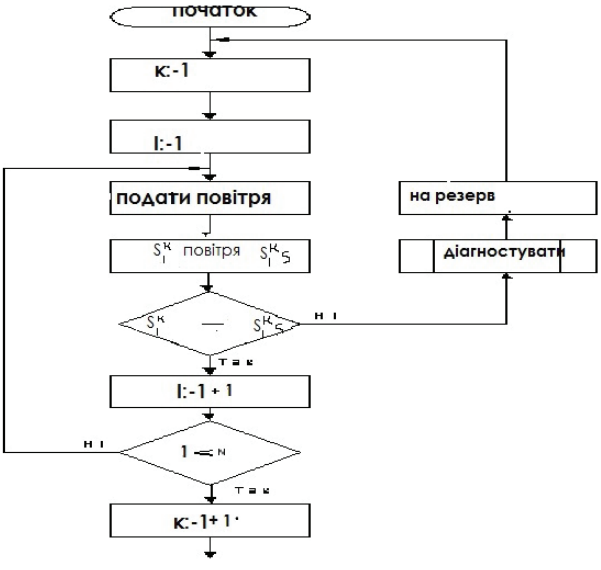

Рис. 3. Алгоритм роботи ГАС з функціональним діагностуванням

6. Висновки

Самодіагностика ГАС з використанням МПП дозволяє реалізувати оптимальні для конкретної ГАС алгоритми пошуку дефектів як по жорсткій або гнучкій послідовній програмі, так і комбінованій [7, 8]. Таким чином, для організації самодіагностики ГАС і підвищення значення $W(t)$ необхідно:

1. Оснастити ГАС вмонтованими сенсорами стану основних блоків, елементів, окрім того необхідно попередньо стискувати діагностичну інформацію.
2. Розробити МПП з розвиненою системою забезпечення експлуатаційної надійності (резервуванням, самодіагностикою, самоконтролем).
3. Створити алгоритм контролю і діагностування ГАС, що мінімізують $T_К$ і $T_Д$.
4. Розробити програми діагностування елементів ГАС з низькою надійністю.
5. Використовувати резервування елементів ГАС з низькою надійністю для автоматичного перемикання на резерв і зменшення часу t.
6. Будувати ГАС з децентралізованою структурою МПП [9, 10].

Література

1. Глазунов, Л. П. Проектирование технических систем диагностирования [Текст] / Л. П. Глазунов, А. Н. Смирнов. — Л.: Энергоатомиздат, 1982. — 168 с.
2. Шибанова, Г. П. Контроль функционирования больших систем [Текст] / Г. П. Шибанова. — М.: Машиностроение, 1977. — 360 с.
3. Приміський, В. П. Методологія побудови автоматичних газоаналізаторів з тестовим сигналом [Текст] // Методи та прилади контролю якості. — 2002. — № 9. — С. 60–63.
4. Герасимов, Б. Н. Микропроцессорные аналитические приборы [Текст] / Б. Н. Герасимов. — М.: Машиностроение, 1989. — 248 с.
5. Газоаналітичний технологічний комплекс з мікропроцесорною системою [Текст] : патент України / Бородавка Б. Н., Безрук З. Д., Дашковський О. А., Приміський В. П. та інші. — № 65505. — 2005. — Бюл 3.

6. Еколого-технологічний газоаналітичний комплекс [Текст] : патент України / Бородавка В. П., Дашковський О. А., Воробйов С. С., Приміський В. П. та інші. — № 64586. — 2004. — Бюл. 2.
7. Безрук, З. Д. Еколого-технологічний моніторінг переробки відходів [Текст] : сборник материалов конференции Пятой научно-технической конференции «Современные информационные и електронные технологии» / З. Д. Безрук, В. П. Приміський. — Одесса, 2004. — 100 с.
8. Визнюк, А. А. Создание систем технолого-экологического мониторинга утилизации промышленных отходов [Текст] : материалы Международной конф. Кацивели, АРК / А. А. Визнюк, З. Д. Безрук, В. П. Приміський // Материалы и покрытия в экстремальных условиях: исследования, применение, экологические чистые технологии производства и утилизации изделий. — Крым, 2004. — С. 563—564.
9. Инструментальный контроль выбросов в атмосферу киевского мусоросжигательного завода «Энергия» [Текст] : материалы II науч.-практ. конф. с междунар. участием / Н. М. Мовчан, З. Д. Безрук, А. А. Дашковский, В. Ф. Примиский и др. // Сотрудничество для решения проблемы отходов. — Харьков, 2005. — 250 с.
10. Безрук, З. Д. Газоаналітичні системи промислового моніторингу [Текст] : матеріали з шостої міжнародної науч.-практ. конф. / З. Д. Безрук, Н. М. Мовчан, О. А. Дашковський // Сучасні інформаційні і електронні технології. — Одесса, 2005. — С. 391.

МОДЕЛИ ДИАГНОСТИКИ И ПОВЫШЕНИЯ НАДЕЖНОСТИ ГАЗОАНАЛИТИЧЕСКИХ СИСТЕМ

Рассмотрена методология диагностирования многоканальных газоаналитических систем и определена эффективность их работы. Проанализированы причины потерь измерительной информации. Предложена методология определения времени восстановления работы газоаналитической системы. Приведены зависимости действия тестового сигнала на выходной сигнал газоанализатора. Проведено сравнение тестового и функционального диагностирования, определены средние временные характеристики работы и восстановления систем.

Ключевые слова: методология диагностирования, многоканальные газоаналитические системы, измерительная информация, микропроцессорные системы (МПС).

Безрук Зоя Домініковна, *асистент, кафедра аналітичного екологічного приладобудування, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: kpi_naeps@ukr.net****.*

Порєв Володимир Андрійович, *доктор технічних наук, професор, завідувач кафедри аналітичного екологічного приладобудування, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: kpi_naeps@ukr.net****.*

Приміський Владислав Пилипович, *кандидат технічних наук, доцент, старший науковий співробітник, кафедра аналітичного екологічного приладобудування, Національний технічний університет України «Київський політехнічний інститут», Україна,* ***e-mail: kpi_naeps@ukr.net****.*

Безрук Зоя Доминиковна, *ассистент, кафедра аналитического и экологического приборостроения, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Порев Владимир Андреевич, *доктор технических наук, профессор, заведующий кафедрой аналитического экологического приборостроения, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Примиский Владислав Филиппович, *кандидат технических наук, доцент, старший научный сотрудник, кафедра аналитического экологического приборостроения, Национальный технический университет Украины «Киевский политехнический институт», Украина.*

Bezruk Zoe, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,* ***e-mail: kpi_naeps@ukr.net****.*

Poryev Vladimir, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine.*

Primisky Vladislav, *National Technical University of Ukraine «Kyiv Polytechnic Institute», Ukraine,* ***e-mail: kpi_naeps@ukr.net***

УДК 621. 391: 519. 2: 519.7

Лисицкий К. Е.

МАКСИМАЛЬНЫЕ ЗНАЧЕНИЯ ПОЛНЫХ ДИФФЕРЕНЦИАЛОВ И ЛИНЕЙНЫХ КОРПУСОВ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Приводятся расчетные соотношения для определения максимальных значений переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок, на основе которых в соответствии с новой методологией оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа расчетным путем определяются показатели доказуемой безопасности ряда современных шифров.

Ключевые слова: *случайная подстановка, блочные симметричные шифры, показатели доказуемой стойкости.*

1. Введение

Как известно, в качестве показателей доказуемой стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа рассматриваются максимальные значения линейных и дифференциальных вероятностей, определяемые соответствующими максимальными значениями переходов XOR таблиц (полных дифференциалов) и смещений таблиц линейных аппроксимаций (линейных оболочек), получающихся на полноцикловой длине этих шифров.