Используя алгоритм синтеза [2] оптимальной структуры фильтра-наблюдателя для уточненного входного сигнала определим структуру передаточной функции G_0 .

Подставляя оптимальную структуру G_0 в функционал качества (9), определим изменение минимального значения относительной дисперсии ошибки измерения угловой скорости крена при уточненном входном сигнале

$e_y=e_{min0}/\sigma_r^2$ для различных значений параметра γ^2 "шум-сигнал" и коэффициента усиления k измерителя.

Сравнительная эффективность измерения угловой скорости крена для обоих вариантов фильтров-наблюдателей G и G_0, синтезированных в измерительном канале приведена в таблице. Здесь $e_б$ - относительная дисперсия ошибки измерения угловой скорости в канале крена при синтезированном оптимальном фильтре-наблюдателе G (базовый вариант), e_y - то же при синтезированном фильтре-наблюдателе G_0 (уточненный вариант).

γ^2	10^{-3}	10^{-2}	10^{-1}	10^{0}	10^{1}
$e_б/e_y$	2.45	2.68	3,48	3,63	4,45

На примере измерения угловой скорости крена видно, что с увеличением уровня шума сравнительная эффективность показателей качества уточненной измерительной системы по сравнению с базовой возрастает. Дисперсия ошибки в базовой системе при этом почти в четыре с половиной раза больше дисперсии ошибки в уточненной системе.

Литература:

1. Блохин Л.Н. Динамическое проектирование оптимальных непроизвольных структур комплексов стабилизации движения при стохастических эксплуатационных воздействиях. Автореф. дис .д-ра техн. наук / КИИГА .-К., 1985.
2. Кошевая Л.А. Автономноное оптимальное оценивание стохастических отклонений ЛА от траектории крейсерского полета: Автореф.дис…канд.техн.наук (ДСП): К. НАУ, 2002 - С.16
3. Блохин Л.Н. Оптимальные системы стабилизации. К.: Техника, 1982. -144 с.
4. Блохин Л.Н. Оптимизация характеристик измерительных устройств: Конспект лекций.- К.: КМУГА, 1997.-104 с.
5. Доброленский Ю.П. Динамика полета в неспокойной атмосфере.- М.: Машиностроение. 1969.-256 с.
6. Азарсков В.Н., Косюк М.Ю., Кривоносенко А.П. Определение динамических характеристик навигационных сигналов по данным летных испытаний // Моделирование полета в задачах эксплуатации ВС ГА.- К: КИИГА.-1985.-С.62-68.

Поступила 21.01.2003
После доработки 9.06.2003

УДК 861.3.004

Козлов В.С., Хорошко В.О.

Кількісна оцінка захищеності інформації

Метою технічного захисту інформації (ТЗІ) є запобігання витоку або порушенню цілісності інформації (ІзОД). Ця мета може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ.

Технічний захист здійснюється поетапно:

- 1 етап – визначення й аналіз загроз.

- 2 етап – розроблення системи захисту інформації.
- 3 етап – реалізація плану захисту інформації.
- 4 етап – контроль функціювання та керування системою захисту інформації. [1]

На другому етапі визначається рівень захисту інформації системою кількісних та якісних показників, які забезпечують розв`язання завдання захисту інформації на основі норм та вимог ТЗІ. Окрім того, на четвертому етапі слід провести контроль ефективності захисту. Ці заходи забезпечують ліцензування системи захисту, а саме, дають змогу оцінити якість та надійність заходів захисту інформації.

На сьогодні, кількісна оцінка якості та надійності захищеності інформації на об`єкті, яка б могла урахувати велику кількість варіантів впливу на нього, авторам невідома. Тому розроблені формули, які пройшли апробацію, для кількісної оцінки захищеності інформації, що циркулює на технічному об`єкті (ТО) з урахуванням імовірності методів несанкціонованого доступу (МНД), імовірності методів захисту інформації (МЗІ), завад і дискретних сигналів.

Згідно з цього, загальна схема для рішення поставленої задачі наведена на мал.1.

При вирішенні задачі введемо наступні обмеження та припущення.

Вхідні умови:

- інформаційні сигнали – дискретні, які використовуються для передачі (прийому) інформації;
- завада типу ВПШ;
- алгоритм взаємодії інформаційних сигналів та перешкод – адитивний.

зв'язку

Методи несанкціонованого доступу (МНД) до інформації в ТО i=[0,M]. При цьому:

$P_1(A_0)$ – імовірність функціонування ТО, $P_1(A_0) = [1,0]$

$P_2(A_i)$ – апріорна імовірність доступу МНД до інформації в ТО, $0 \le P_2(A_i) \le 1$

$P_3(A_j)$ – апріорна імовірність МЗІ в ТО, $0 \le P_3(A_j) \le 1$

$P_4 = P_{ош}[\xi(t)]$ – імовірність помилки через $\xi_1(t)$, $[P_4[\xi(t)=1]$.

МЗІ – методи захисту в ТО, j=[0,N].

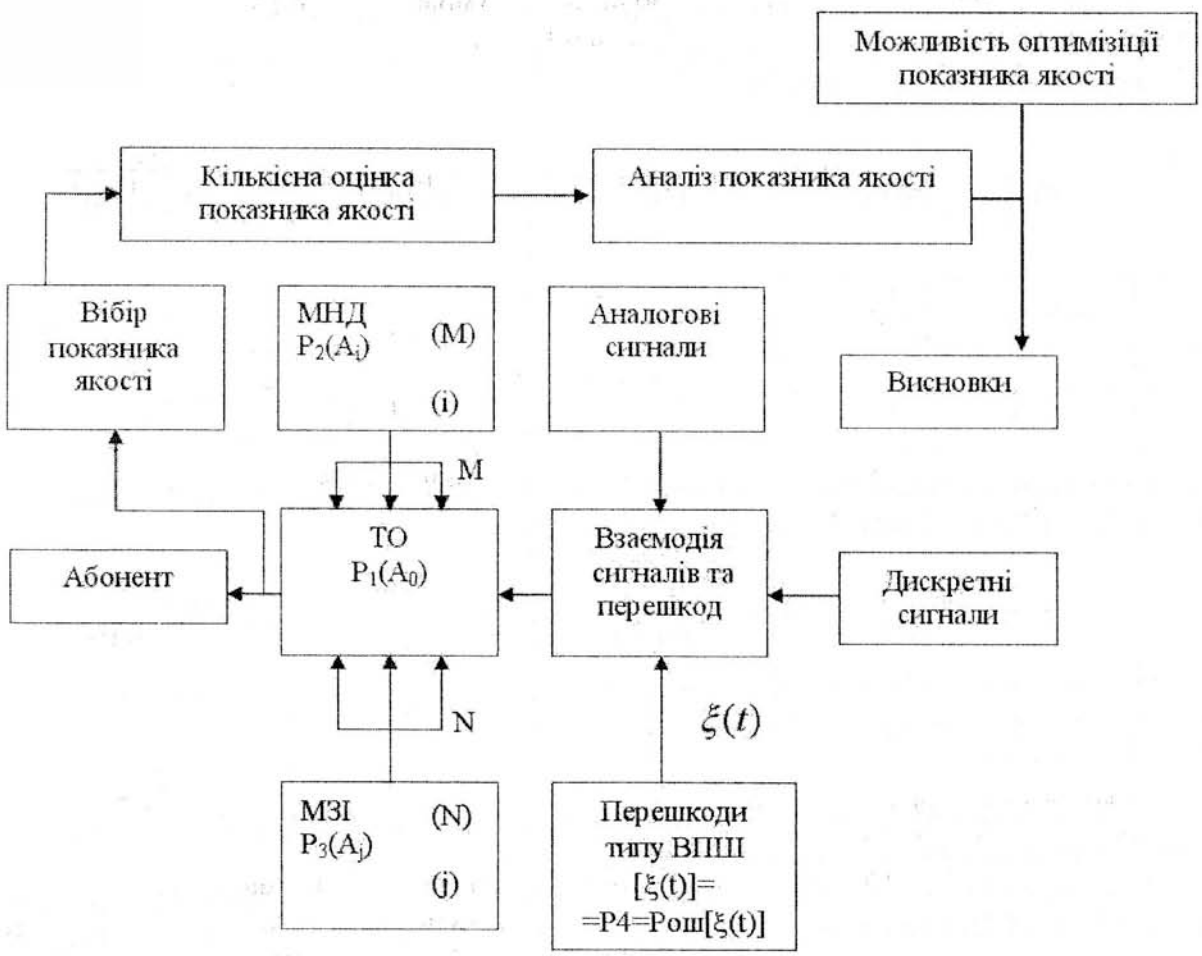
ДП – джерела завад, з відомим законом розподілу $\xi_k(t)$ (математичні моделі завади, що діє в ТО), i = 1, F

В подальшому розгляді враховується завада $\xi_1(t)$, де $\xi_1(t)$ – ВПШ – внутриприйомний шум у ТО, або інша завада з Гаусовим законом розподілу.

Випадкові події A_i – МНД та A_j – МЗІ незалежні й несумісні.

Згідно вказаного вище, повну матрицю функціонування ТО, при наявності МЗІ, МНД та $\xi_1(t)$, можна скласти, якщо враховувати, що $P_1[A_0]=[1,0]$; $P_2[A_i]=[1,0]$, $P_3[A_j]=[1,0]$; $P_4=P_{пом}[\xi_1(t)]=[1]$.

У цьому випадку, $N = m^n = 2^4 = 16$, де N – повна матриця станів ТО.



Мал. 1

Тобто повна матриця станів функціонування ТО може бути записана так:

Табл.1

N / P_i {i=1,4}	$P_1(A_0)$	$P_2(A_i)$ МНД	$P_3(A_j)$ МЗІ	$P_4[\xi(t)]$ $=P_{пом}[\xi(t)]$
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0
15	1	1	1	1

Аналіз повної матриці ТО проводимо за умови, що $P_1[A_0]=[1]$; $P_2[A_i]=[1,0]$, $P_3[A_j]=[1,0]$; $P_4=P_{пом}[\xi_1(t)]=[1]$. З огляду на те, що $P_1[A_0] = 1$, та $P_4 = 1$, то повну матрицю ТО можна скоротити до вигляду (табл.2):

Табл.2

N P_i, i=1,4	$P_1(A_0)$	$P_2(A_i)$	$P_3(A_j)$	$P_4=P_{пом}[\xi(t)]$
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1

З урахуванням подій A_i, A_j та значень табл.2, імовірностей присутності завад типу ВПШ у ТО $P_{пом}[\xi_1(t)] = 1$, матриця приймає вигляд (табл.3):

Табл.3

N P_i,	$P_1(A_0)$	$P_2(A_i)$	$P_3(A_j)$	$P_4=P_{пом}[\xi(t)]$
11	1	1	0	1
14	1	0	1	1

Отже, розробка формули для кількісної оцінки захищеності інформації у „абонента" може бути отримана з урахуванням ситуації 11 та 14 табл.3.

Обґрунтування вибору показника якості (захищеності інформації) ТО при його взаємодії з МЗІ, МНД і завад типу ВПШ у „абонента", за умов, що $P_1(A_0) = 1$ та $P_4=P_{пом}[\xi(t)] = 1$, означає, що імовірність помилки на стороні „абонента" $P_4=P_{пом}[\xi(t)]$ завжди має місце.

Як показник захищеності інформації на стороні „абонента" можна розглядати:

- імовірність правильного прийому інформації „абонентом" (P);
- імовірність помилки при прийомі інформацій „абонентом" (Q);

Таким чином, відповідно до теорем теорії імовірності (розділ випадкових подій) [2] та прийнятих обмежень, як показник якості захищеності інформації на стороні „об`єкта" використаємо вирази:

$$P = 1 - \left\langle \left\{ \left[\prod_{i=0}^{N} (1 - P(A_i)) \right] \left[\prod_{j=0}^{N} (1 - P(A_j)) \right] \right\} + P_{пом}[\zeta(t)] \right\rangle \qquad (1)$$

або

$$Q=1-P \qquad (2).$$

де:

$\prod_{i=0}^{M}[1 - P(A_i)]$ - добуток імовірностей пропуску з боку МЗІ при впливі невідомих МНД. Це імовірність помилки з боку МЗІ.

$\prod_{j=0}^{N}[1 - P(A_j)]$ - добуток імовірностей доступу з боку МНД при недосконалості „N", „МЗІ".

При цьому можливо:

- глушіння;
- прослуховування з помилками через дію завади ξ(t);
- містифікації інформації у ТО;

- порушення трафіка та ін.

Якщо проаналізувати співвідношення (1) і (2) з урахуванням припущень: $P_2(A_i) = P_3(A_j) = 0$; $P_1(A_0) = 1$; $P_4[\xi_1(t)] = 1$; $Q = P_{пом}[\xi_2(t)]$; та якщо $P_2(A_i) = P_3(A_j) = Q$; $P_1(A_0) = 1$; $P[\xi_1(t)] = 1$; $P = 1 - P_{пом}[\xi(t)]$ чи $P = 1 - Q$, то можна зробити висновок, що захищеність інформації у „абонента" залежить від імовірності МЗІ з імовірністю МНД і завад типу ВПШ $[\xi_1(t)]$ з Гаусовим законом розподілу.

При цьому співвідношення (1) та (2) з позицій теорії імовірності (розділ випадкових подій) правильні і можуть бути використані для кількісної оцінки захищеності інформації на стороні „абонента" з урахуванням імовірностей МНД, імовірностей МЗІ, імовірностей функціонування ТО та імовірності помилки через заваду $\xi_1(t)$.

Окрім того, кількісна оцінка (математична) захищеності інформації на стороні „абонента" при наявності завад з Гаусовим законом розподілу миттєвих значень, враховуючи (1) та (2) можливо розглядати як завади типу ВПШ $\xi_1(t)$ миттєвих значень з параметрами a_{S1} та σ_{31}^2, де:

a_{S1} - математичне чекання завади типу ВПШ;

σ_{31}^2 - дисперсія завади типу ВПШ.

При цьому, якщо $\xi_1(t)$ – завада з $a_1 \neq 0$ та $\sigma_3^2 \neq 0$, то її миттєве значення описується як:

$$\omega(\xi_1) = \frac{1}{\sigma_{\xi 1} \cdot \sqrt{2\pi}} e^{-\frac{\xi_1 - a_1}{2\sigma_{\xi 1}}} \qquad (3)$$

або якщо заваду $\xi_1(t)$ розглядати в лінійному тракті і $a_1 = 0$, тоді:

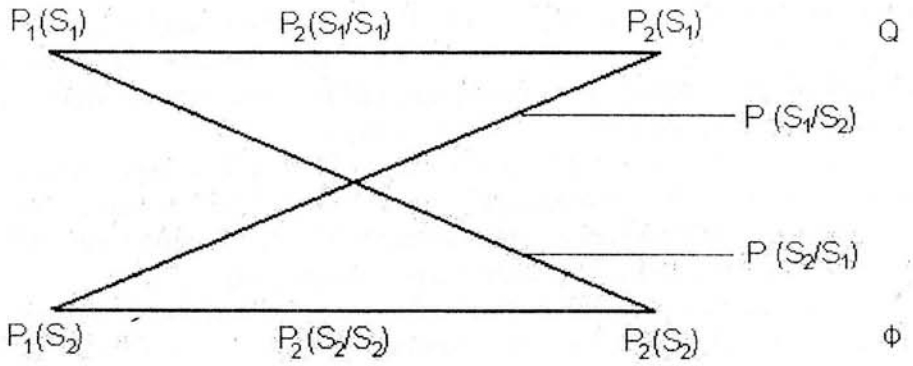
$$\omega(\xi_1) = \frac{1}{\sigma_{\xi 1} \cdot \sqrt{2\pi}} e^{-\frac{\xi_1^2}{2\sigma_{\xi 1}}} \qquad (4)$$

При кількісній оцінці захищеності інформації в ТО з урахуванням (3) та (4) необхідно враховувати наступні початкові умови:

- розглядається цифрова система зв`язку (локальна обчислювальна мережа, мережа керування та інші), по яким передача інформації здійснюється за допомогою цифрових сигналів;
- цифрові сигнали передаються у стані кодових комбінацій, представлених у двоїчній системі числення;
- елементарні цифрові сигнали у кодовій комбінації $S_1(t)$ та $S_2(t)$;
- перекручування та завмирання в каналі зв`язку відсутні;
- у каналі зв`язку діє завада $\xi_1(t)$ типу ВПШ, миттєві значення якої описуються співвідношеннями (3) або (4).

Функціонування в ТО здійснюється при передачі інформації кодовими комбінаціями, тобто при використанні кодових сигналів $S_1(t)$ та $S_2(t)$.

В подальшому вигляді за умов скорочення будемо використовувати слідуюче написання формул: $S_1(t) = S_1$ та $S_2(t) = S_2$. При цьому граф функціонування ТО буде мати такий вигляд:



Мал.2

Де:
$P_1(S_1)$ – апріорна імовірність використання сигналу S_1 при передачі інформації „абоненту"
$P_1(S_2)$ – апріорна імовірність використання сигналу S_2 при передачі інформації „абоненту"
$P(S_1/S_1)$ – умовна імовірність правильного прийому сигналу S_1 „абонентом", якщо був переданий сигнал S_1.
$P(S_2/S_2)$ – умовна імовірність правильного прийому сигналу S_2 „абонентом", якщо був переданий сигнал S_2.
$P(S_1/S_2)$ – умовна імовірність помилки на стороні „абонента", якщо був переданий сигнал S_1, а прийнятий – сигнал S_2. („Помилка").
$P(S_2/S_1)$ – умовна імовірність помилки на стороні „абонента", якщо був переданий сигнал S_2, а прийнятий – сигнал S_1. („Помилка").
Ф[S1,S2] – повна імовірність правильного прийому інформації „абонентом", при передачі сигналів S_1 та S_2.
Q[S_1,S_2] – повна імовірність помилкового прийому інформації „абонентом", при передачі сигналів S_1 та S_2.
$P_2(S_1)$ – повна імовірність прийому сигналу S_1 „абонентом", за умови, що передавався сигнал S_2 і він через завади був прийнятий як сигнал S_1.
$P_2(S_2)$ – повна імовірність прийому сигналу S_2 „абонентом", за умови, що передавався сигнал S_1 і він через завади був прийнятий як сигнал S_2.
A – рівень потенціалів при передачі сигналів S_1 та S_2.
V – поріг „чутності людиною" чи поріг ухвалення рішення „V" технічною системою.

Подалі розглянемо випадок, коли завада $\xi_1(t)$ є Гаусовою та центрованою, а сигнали S_1 та S_2 передаються з амплітудою A_0 = [1,0]. У цьому випадку імовірність помилок і правильність прийому визначаються при відсутності МНД характеристиками завад $\xi_1(t)$ і, зокрема, СКО $\xi_1(t)$, V – порогом ухвалення рішення й амплітудою сигналів в кодовій комбінації А. При цьому треба враховувати, що помилка типу $P(S_1/S_2)$ відбувається тоді, коли $P[\xi_1(t) < V - A]$.

Її значення визначається по формулі:

$$P(S_1/S_2) = \int_{-\infty}^{V-A} \omega(\xi_1) d\xi_1$$

З обліком Гаусової завади при $a_1 = 0$

$$P(S_1/S_2) = \int_{-\infty}^{V-A} \frac{1}{\sigma_{\xi 1}\sqrt{2\pi}} e^{\frac{-\xi^2}{2\sigma_{\xi 1}^2}} d\xi,$$

та після заміни $x = \xi\sigma_{\xi 1}$, одержимо:

$$P(S_1/S_2) = \frac{1}{2\pi} \int_{-\infty}^{\frac{V-A}{\xi}} e^{\frac{-x^2}{dx}} = \Phi(\frac{V-A}{\sigma_{\xi 1}}), \qquad (5)$$

де $\Phi(\frac{V-A}{\sigma_{\xi 1}})$ - табулірований інтеграл імовірностей.

Помилки типу $P(S_2/S_1)$ обчислюються за виразом:

$$P(S_2/S_1) = 1 - \Phi(\frac{M}{\sigma_{\xi 1}}), \qquad (6)$$

Значення інтегралу імовірності можна знайти в [3].

Розглянемо приклад використання співвідношень (5) та (6). Якщо припустити, що A = 1[B]; V = 0,5A[B]; $\sigma_{\xi 1}$= 0,3[B], то відповідно до формули (5): $P(S_1/S_2) = 1 - \Phi(\frac{0,5-1}{0,3})$. З огляду на те, що $\Phi(-\alpha) = 1 - \Phi(\alpha)$, то $P(S_1/S_2) = 1 - \Phi(1,66) = 1 - 0,95515 = 0,05$.

Це означає, що імовірність оцінки по стороні „абонента" при прийомі цифрової інформації дорівнює приблизно 0,05 [4,5].

Якщо враховувати попередні припущення та (6), то $P(S_2/S_1) = 1 - \Phi(\frac{V}{\sigma_{\xi 1}})$, тоді маємо $P(S_2/S_1) = 1 - \Phi(\frac{0,5}{0,3}) = 1 - \Phi(1,66)$. $\Phi(1,66) \approx 0,95$, тоді $P(S_2/S_1) = 1 - 0,95 = 0,05$.

Згідно з цього можливо зробити висновок, якщо $P(S_1/S_2) = P(S_2/S_1)$, то канал зв`язку у мережі є симетричним. У цьому випадку: $P(S_1/S_2) = P(S_2'/S_1) = 0,5$.

Згідно з цього можливо зробити наступні висновки:

Математичні співвідношення (1), (2), (3), (4), (5) відповідають теорії імовірностей і їх можливо використовувати для кількісної оцінки захищеності інформації в ТКО на стороні „абонента" за умови загальної структури щодо вирішення задачі;

Можливо вирішення задачі структурної та параметричної оптимізації.

Література:

1. ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.
2. Сторский В.П. Математический аппарат инженера. – К.: Техніка, 1975. – 768с.
3. Тихонов В.И. Статистическая радиотехника. М.: Радио и связь, 1966. – 166с.
4. Зюно А.Г. Теория передачи сигналов. – М.: Связь, 1973. – 376с.
5. Атергауз С.М. и др. Справочник по вероятностным расчётам. – М.: Сов. радио, 1983. – 326с.

Надійшла 28.05.2003р.