УДК 004.621.3 **Хорошко В.О., Хохлачова Ю.Є.**

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

У даній статті розроблено методику оцінки захищеності інформації від зловмисних та несанкціонованих дій до інформації, що захищається, в засобах обчислювальної техніки та автоматизованих системах на основі застосування принципів системотехніки. Обґрунтовано висновки, які пов'язані з експлуатацією технічних засобів захисту інформації.

Ключові слова: захист інформації, системи захисту інформації, несанкціонований доступ, система обробки даних.

Вступ. Інформація давно припинила бути просто необхідністю для виробництва та прояву будь-якого роду діяльності людини. Вона придбала значну цінність, яка чітко визначається реальним прибутком, що отримується від її використання, або розміром збитку внаслідок її страти або несанкціонованого доступу (НСД) до неї.

Засоби захисту інформації різноманітних класів, що використовуються у теперішній час, та існуючі методики не дозволяють зробити оцінку їх стійкості від дій зловмисників. Рішення даної задачі можливо шляхом використання принципів системотехніки: процес, що вивчається, описується на мовах теорій, які найбільш розвинуті, та оцінюється за показниками ефективності надсистеми – людини, яка визначає корисність створеної системи захисту інформації (СЗІ). При цьому система математичних моделей, що використовується, має ієрархічну структуру, де математичні моделі "нижчих" рівнів уточнюють параметри моделей "вищих" рівнів.

Той факт, що СЗІ характерна невизначеність (наскільки бездоганною є створена система, а також якою є її часова стійкість), дозволяє застосувати для оцінки захищеності інформації показники ефективності імовірнісно-часової групи показників:

- середній час безпечного функціонування системи, що захищається;
- час безпечного функціонування системи, що захищається, з імовірністю її поразки НСД не вище заданої;
- економічна ефективність створеної СЗІ.

Мета роботи. Метою даної статті є розробка методики оцінки захищеності інформації від зловмисних та несанкціонованих дій до інформації, що захищається, в засобах обчислювальної техніки (ЗОТ) та автоматизованих системах (АС) на основі застосування принципів системотехніки та обґрунтування висновків, пов'язаних з експлуатацією технічних засобів захисту інформації.

Основна частина. У статті задача оцінки стійкості СЗІ від НСД може бути сформульована таким чином:

- нехай є система обробки даних (СОД), у якій реалізована комплексна (СЗІ) на основі технічних засобів захисту;
- нехай зловмисник має екземпляр даного технічного засобу та вивчає його

Таким чином, потрібно оцінити стійкість системи захисту від її зловмисного вивчення за обраними показниками ефективності.

Розглянемо математичну модель зловмисника, який розшифровує технічний засіб захисту. Ця модель повинна відповісти на питання – які чисельні характеристики ймовірностей виявлення спроб НСД на певному інтервалі часу. Рішення задачі розробки моделі зловмисника передбачає пошук системи теорій:

1. Теорії, яка би дозволила зв'язати складність реалізованого алгоритму захисту інформації та перебуваючого у конкретному технічному засобі та часу, необхідному зловмисникові для розшифровування цього алгоритму.

2. Теорії, яка була би спроможна зв'язати знайдений час розшифровки алгоритму з ймовірністю того, що зловмисник зміг розшифрувати алгоритм за деякий інтервал часу.

Проведений аналіз показує, що задача першого роду може бути вирішена за допомогою використання лінійної теорії алгоритмів, яка була викладена Холстедом [1].

Задача другого роду може бути вирішена за допомогою теорії катастроф, яка описується у теорії масового обслуговування [2].

Розглянемо більш детально обидві теорії стосовно для даної задачі.

Лінійна теорія алгоритмів у рішенні задачі оцінки часу, необхідного зловмисникові для розшифровування системи захисту інформації, полягає у наступному. Враховуючи, що задача розшифрування програми довжиною N за складністю співпадає з написанням програми довжиною N біт на тій самій мові, скористаємося апроксимацією рівняння часу, необхідного для написання програми, якщо відома тільки довжина програми – N біт. У цьому випадку середній час розшифрування програми T можна визначити як:

$$T = \frac{N_2^2 \cdot \log_2 \eta}{4 \cdot S} \text{ (сек)}, \quad (1)$$

де: η - алфавіт мови тексту програми; S – число Страуда (S=4÷20 операцій в секунду), що характеризує кількість об'єктів, якими може оперувати зловмисник одночасно (свого роду характеристика швидкодії зловмисника, що розшифровує текст програми); N – довжина тексту програми (команди + операнди) у бітах. У співвідношенні з "Холстедом", у випадку, якщо потрібно написати програму на машинній мові [1] $T = N^2(C)$.

Так як програми захисту інформації характеризуються великою довжиною, введемо поправку на стомлювання зловмисника, тоді вираз для T буде мати вигляд:

$$T = 3N^2(C) \quad (2)$$

А теорія катастроф у рішенні задачі оцінки імовірності розшифровки тексту програми на інтервалі часу потребує розглядати зловмисника як суб'єкта вищої кваліфікації, що дає можливість поставити зловмисному процесу розшифровки СЗІ функцію-розподіл розумного зловмисника – експоненціальний розподіл з параметром $S = 1/T(1/C)$. Причому тут T – середній час розшифровки тексту програми.

У цьому випадку, імовірність не розшифровки тексту програми (P_H) за деякий інтервал часу, розподіленому за експоненціальним законом з параметром β, можна представити як перетворення Лапласа-Стільтьєса [2]. Функції розподілу інтервалу часу на якому оцінюється імовірність розшифровки тексту $\mathrm{B}(t)$:

$$P_H = \int_0^\infty e^{-st} d\mathrm{B}(t) = \frac{\beta}{\beta + S} \quad (3)$$

Таким чином, вдалося "плавно" перейти від довжини тексту програми N, яка написана на алгоритмічній мові, яку "передбачив" для зловмисника розробник СЗІ, до імовірності нерозшифовки тексту програми захисту за деякий інтервал часу, розподілений за експоненціальним законом. Припустимо, що апаратні засоби СЗІ допускають "розгортання" у текст програми кінцевої довжини, а "текст програми захисту" представляє собою суму текстів програмної та апаратної частин.

На основі попередніх роздумів розглянемо математичну модель взаємодії інформації, яка захищається, СЗІ, СОД та зловмисника. При цьому процес взаємодії складається з наступних станів:

- зловмисника, що розшифровує СЗІ та оцінює успішність НСД;
- спроможність СОД обробляти та зберігати інформацію, що надійшла до неї та потребує захисту;
- інформацію, яка надійшла в СОД;
- створена розробником СЗІ характеризується кінцевою множиною можливих станів

$$S = (S_1, S_2, ..., S_r). \quad (4)$$

Процес у кожну мить часу t характеризується лише одним з цих станів.

Через деякі інтервали часу мають місце переходи з одного стану в інший (має місце крок процесу).

Імовірність того, що на черговому кроці система перейде зі стану S_i у стан S_j, у

загальному випадку, залежить від початкового стану системи та від усіх проміжних станів, аж до поточного. У теперішній час, найбільш детально вивчені цілі, що володіють Марковською властивістю [3]. У цьому випадку імовірність переходу на черговому кроці зі стану S_i у стан S_j залежить тільки від стану S_i, в якому ціль з'явилась після попереднього кроку (поведінка системи у наступному залежить від її стану у даний момент та не залежить від того, яким чином вона прийшла в цій стан).

Таким чином можна передбачити що:

- імовірність одночасної зміни станів двох та більше елементів дуже мала;
- імовірності переходів з одного стану в інший не залежить від часу;
- за нескінченно малий проміжок часу неможливий перехід у деякий "сусідній" стан та повернення з нього, тоді процес взаємодії, що розглядається, математично характеризується напівмарківським процесом [3]: з матрицею ймовірностей переходів, поглинаючого ланцюга (поглинаючий стан характеризує той факт, що зловмисник, за його думкою, розшифрував СЗІ та готов на практиці реалізувати спробу НСД до інформації, що захищається):

$$P = \begin{vmatrix} P_{11} & P_{12} & \dots & P_{1r} \\ P_{21} & P_{22} & \dots & P_{2r} \\ & \dots & & \dots \\ P_{r1} & P_{r2} & \dots & P_{rr} \end{vmatrix} \qquad (5)$$

Для подальших роздумів введемо наступні позначення : S_1 - множина безповоротний станів напівмарківського процесу; $N = \|n_{ij}\|$ - фундаментальна матриця вкладеної поглинаючого марківського ланцюга; m_i - середній час однократного перебування напівмарківського процесу у безповоротних станах $S_i \in S; N^* = \|n_{ij}^*\|$ - матриця середніх часів n_{ij}^* перебування напівмарківського процесу у стані $S_i \in S$ до поглинання при умові, що початковим був стан $S_i \in S; T^* = \|t_i^*\|$ - матриця строчка середніх часів t_i^* перебування марківського процесу в множині безповоротних станів при початковому стані $S_i \in S$ до переходу у сусідній стан; t^* - середній час перебування напівмарківського процесу у множині безповоротних станів при вільному початковому розподілення імовірностей станів $P(0)$.

У загальному випадку, система, що розглядається, формально представляє собою СОД, на вхід якої поступає інформація, що підлягає захисту. Надходження інформації характеризується пуасонівським потоком з параметром β, а інформації, що надходить до СОД у деякий час, який характеризується параметром γ. Окрім цього, цікавість зловмисника до інформації, що підлягає захисту, характеризується потоком спроб НСД з параметром НСД λ.

За "Холстедом" та використанням теорії катастроф, отримаємо чисельні значення ймовірностей: P_1 – імовірність виявлення спроби НСД в моменти часу, коли у системі відсутня інформація, що захищається; P_2 – імовірність виявлення спроби НСД на етапі аутентифікації прийнятої інформації; P_3 – імовірність виявлення спроби НСД на етапі обробки або збереження інформації, що надходить.

Окрім цього відомі:

- прибуток C_1 одиниць цінності, яка отримується від обробки інформації, що захищається;
- збиток C_2 одиниць цінності від НСД до інформації, що захищається.

Тоді задача оцінки ефективності захисту зводиться до оцінки середнього часу перебування напівмарківського процесу у множині безповоротних станів до поглинання та використання його для отримання імовірністно-часових характеристик показників

ефективності.

Таким чином, перейдемо до виведення математичного виразу оцінки середнього часу безпечного функціонування системи, що досліджується. Оскільки система, що розглядається, характеризується поглинаючим станом – станом, коли зловмисник виявив, що для нього немає таємниць та він готовий до реалізації своєї задумки, тоді математичний вираз середнього часу безпечного функціонування системи, що досліджується, можна визначити як середній час перебування системи, яка розглядається, у множині безповоротних станів. У відповідності з [4] середній час t перебування процесу, що досліджується у множині безповоротних станів може бути знайдений як добуток матриць:

$$t = P(0)N^*E, \qquad (6)$$

де $P(0)$ – матриця-вектор початкового стану, з якого почався процес, що досліджується; $N^* = \left\| n_{ij}^* \right\|$ - матриця середнього часу n_{ij}^* перебування напівмарківського процесу у стані $S_j \in S$ до поглинання при умові, що початковим був стан $S_j \in S$.

Окрім цього N^* можна записати також наступним чином:

$$N^* = \left\| n_{ij} m_j \right\|,$$

де m_j - середній час однократного перебування напівмарківського процесу у безповоротних станах $S_i \in S$; n_{ij} - елемент функціональної матриці $N = \left\| n_{ij} \right\|$, отримується з виразу $N = (I - Q)^{-1}$; I – одинична діагональна матриця; Q – матриця переходів в безповоротній множині станів; E – вектор-стовбчик одиничних елементів.

Таким чином, для того, щоб визначити середній час безпечного функціонування системи, що досліджується, необхідно [5]:

1. З матриці переходів процесу P, що досліджується, отримати матрицю переходів у безповоротній множині станів Q та m_j - середні часи однократного перебування напівмарківського процесу в безповоротних станах $S_i \in S$.

2. Отримати фундаментальну матрицю $N = \left\| n_{ij} \right\|$ згідно виразу $N = (I - Q)^{-1}$

3. Отримати матрицю середніх часів n_{ij}^* перебування напівмарківського процесу у стані $S_i \in S$ до поглинання при умові, що початковим був стан $S_j \in S$:

$$N^* = \left\| n_{ij} m_j \right\|.$$

4. Конкретизувати вектор-стовбчик початкового стану, з якого почався процес, що досліджується.

5. Використанням виразу $t = P(0)N^*E$ отримати чисельний вираз середнього часу безпечного функціонування системи, що захищається.

Тепер можна здійснити виведення математичного виразу для оцінки проміжку часу, на якому імовірність виключення НСД захищеної інформації не нижче заданого значення. Так як вираз (6) дозволяє оцінити середній час безпечного функціонування системи, що захищається. Однак СЗ повинна експлуатуватися. Експлуатація повинна містити перевірку справності системи захисту за досягненням системою деякого порогу довіри – імовірності виключення НСД до інформації, що захищається, нижче заданого.

Апроксимуємо функцію розподілу часу, на якому довіра до системи захисту інформації не нижче заданого, а також функцію розподілу часу безпечного функціонування експоненційними розподілами з параметрами S та μ відповідно.

$$\mu = 1/T.$$

Оскільки згідно з теорією катастроф імовірність виключення НСД $P_{НСД}$ на інтервалі, що є розподілений за експоненційним законом з параметром S складе

$$P_{НСД} = \int_0^{\infty} e^{-\mu t} dS(t) = \frac{S}{S+\mu}. \quad (7)$$

Тоді *ТО* – середній час безпечного функціонування системи, що захищається, з імовірністю виключення НСД не нижче $P_{НСД}$ можна знайти як

$$TO = \frac{1}{S} = \frac{t(1-P_{НСД})}{P_{НСД}}. \quad (8)$$

З виразу (8) витікає, що за витоком часу *ТО* для підтримки довіри до системи захисту інформації, що створюється, необхідно проведення регламентних робіт по перевірці працездатності СЗІ. Методика проведення регламентних робіт повинна бути достатньо ефективною.

У якості форми повернення "довіри" до СЗІ може бути й впровадження чергової версії технічного засобу захисту інформації. Цим ми умовно ставимо зловмисника перед необхідністю освоювання кожний раз все нового технічного засобу захисту.

Таким чином, для того, щоб оцінити середній час між проведеннями регламентних робіт необхідно:

1. У відповідності з виразом (6) отримати чисельне значення середнього часу безпечного функціонування системи, що захищається.
2. Оцінити рівень захисту інформації, що потребується, нижнім порогом довіри до СЗІ - $P_{НСД.}$
3. Використанням виразу (8) отримати чисельне значення інтервалу часу, протягом якого забезпечується захищеність інформації не нижче заданого нижнього порога.

Як відмічалося раніше, інформація давно припинила бути просто необхідністю для виробництва та проявом всілякого роду діяльності. Інформація придбала відчутну цінність, вона чітко визначається реальним прибутком, що отримується від її використання, або розміру збитку внаслідок її втрати або НСД до неї. Покладемо цей постулат в основу виведення математичного виразу оцінки прибутку, що отримується від використання СЗІ.

Оскільки процес функціонування системи, що досліджується через рівномірні інтервали часу, включає проведення регламентних робіт, то обробка кожної інформації, що надходить, з імовірністю $P_{НСД}$ приносить прибуток в C_1 одиниць вартості, а з імовірністю (1- $P_{НСД}$) – збиток в C_2 одиниць вартості. В даному випадку математичний вираз прибутку *Д*, що приноситься кожним пакетом інформації, яка надходить, складе:

$$Д = C_1 \cdot P_{НСД} - C_2(1-P_{НСД}). \quad (9)$$

Природно слід рахувати, що у випадку $Д>0$ застосування технічних засобів захисту інформації приносить прибуток.

При оцінюванні імовірності розшифровки програмного модуля СЗІ між моментами надходження інформації до СОД приймемо:

P_1 – імовірність нерозшифровки тексту програми модуля захисту інформації на етапі відсутності інформації в СОД між сусідніми надходженнями її до СОД (імовірність не блокування СЗІ для даного етапу);

P_2 – імовірність нерозшифровки тексту програми модуля захисту інформації на етапі прийому (формування) інформації в СОД між сусідніми моментами надходження її до СОД (імовірність не блокування СЗІ для даного етапу);

P_3 – імовірність нерозшифровки тексту програми модуля захисту інформації на етапі обробки та зберігання її у СОД між сусідніми надходженнями інформації до СОД (імовірність не блокування СЗІ для даного етапу).

Оскільки запропонован Пуасонівський закон надходження інформації до СОД, імовірність нерозшифровки програмного модуля довжиною N_1 СЗІ між моментами надходження інформації до СОД оцінюється згідно (3) як:

$$P_1 = P_2 = P_3 = 1 - \frac{1/T}{\beta + 1/T}. \quad (10)$$

При розробці математичної моделі взаємодії СОД, інформації, що надходить до СОД, та діями зловмисника потрібно враховувати, що система взаємодії, яка вивчається, формально представляє собою систему обробки даних, на вхід якої надходить інформація, що потребує захисту. У СОД реалізована СЗІ на основі технічних засобів. Ці засоби забезпечують захист інформації на всіх етапах її обробки та перебування у системі.

Таким чином, система, що досліджується, характеризується:

1) пуасонівським потоком подій, пов'язаних з НСД з параметром λ;

2) пуасонівським потоком інформації, що потребує захисту, з параметром β;

3) експоненціальним розподілом часу обробки (перебування) інформації у системі, що захищається, з параметром γ;

4) в СОД створена комплексна СЗІ, яка забезпечує:

- захист інформації на інтервалі, коли її немає у системі, що захищається, з імовірністю P_1=0,999997;
- захист інформації на інтервалі часу, коли інформації надійшла у систему, що захищається – на етапі попередньої обробки (аутентифікації) інформації, яка надійшла – P_2=0,999997;
- захист інформації у процесі обробки повідомлення, що надійшло (обробки інформації) – P_3=0,999997.

Слід відмітити, що з формалізмами, пов'язаними з пуасонівськими потоками інформації на вході СОД та експоненціальними розподілами часу перебування інформації у них, пов'язані найважливіші результати досліджень в області теорії обчислювальних мереж, теорії телетрафіка та інших областях техніки. Тому застосування даних формалізмів має місце.

Будемо враховувати, що зловмисникові цікаве кожне повідомлення, яке надійшло до системи. Це робить можливим для системи, що розглядається, використання формалізму з пуасонівським потоком подій, пов'язаних з НСД до повідомлень з параметром, чисельно рівним параметру потоку інформаційних повідомлень.

У нашому випадку, процес функціонування системи, що захищається, може бути представлений у вигляді графу переходів рис. 1 та виразом матриці переходів (11). Тут: S_1, S_2, S_3, S_4, S_5 – множина станів:

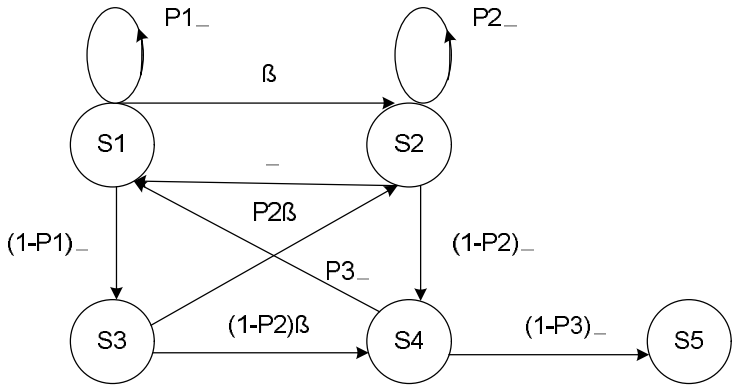

Рис. 1. Граф переходів

S_1 - складний стан, що включає:

- відсутність інформаційних повідомлень у системі;
- виявлення факту НСД на етапі відсутності інформації у системі та миттєве відновлення системи після виявлення факту НСД.

S_2 – складний стан, що включає:

- надходження інформації до системи;
- виявлення факту НСД на етапі перевірки повідомлення та миттєве відновлення системи

після виявлення факту НСД.

S_3 – стан не виявлення факту НСД, коли у системі немає інформації;

S_4 – стан перевірки системи при наявності факту НСД на етапі обробки повідомлення, що надходить.

S_5 – стан не виявлення факту НСД по закінченні обробки інформаційного повідомлення, що надійшло.

Приймемо допущення про те, що процес переходів є марківським, тоді процес переходів представляється матрицею переходів (11):

$$P = \begin{vmatrix} P_{11} & P_{12} & P_{13} & 0 & 0 \\ P_{21} & P_{22} & 0 & P_{24} & 0 \\ 0 & P_{32} & 0 & P_{34} & 0 \\ P_{41} & 0 & 0 & 0 & P_{45} \\ 0 & 0 & 0 & 0 & 0 \end{vmatrix}, \tag{11}$$

де

$$P_{11} = \lambda P_1/(\lambda+\beta); P_{12} = \beta/(\lambda+\beta); P_{13} = \lambda(1-P_1)/(\lambda+\beta);$$
$$P_{21} = \gamma/(\lambda+\gamma); P_{22} = P_2\lambda(\lambda+\gamma); P_{24} = (1-P_2)\cdot\lambda/(\lambda+\gamma);$$
$$P_{32} = P_2; P_{34} = 1-P_2;$$
$$P_{41} = P_3; P_{45} = 1-P_3.$$

При цьому, середній час одиничного перетворення системи у кожному з безповоротних станів складе:

$$M = \left| \frac{1}{\lambda+\beta} \frac{1}{\lambda+(1-P_2)\gamma} \frac{1}{\beta} \frac{1}{\gamma} \right|. \tag{12}$$

Оцінка середнього часу безпечного функціонування системи, що захищається, полягає в обчислюванні середнього часу перебування процесу у множині безповоротних станів матриці (11). Для чого отримаємо матрицю Q шляхом обчислювання 5-ї строчки та 5-го стовпчика матриці P.

$$Q = \begin{vmatrix} P_{11} & P_{12} & P_{13} & 0 \\ P_{21} & P_{22} & 0 & P_{24} \\ 0 & P_{32} & 0 & P_{34} \\ P_{41} & 0 & 0 & 0 \end{vmatrix} \tag{13}$$

Середній час безпечного функціонування системи, що розглядається – середній час перебування процесу у множині безповоротних станів обчислюється за формулою (6).

Нехай:

1. Процес розпочався з початкового стану S_1 . Цьому відповідає вектор-строчка $P(0)=(1,0,0,0)$.

2. M – матриця середніх часів однократного перебування процесу, що розглядається, у кожному зі станів множини станів описується виразом (12).

Матриця $(I-Q)$ буде мати вигляд:

$$(I-Q) = \begin{vmatrix} (1-P_{11}) & P_{12} & P_{13} & 0 \\ P_{12} & (1-P_{22}) & 0 & P_{24} \\ 0 & P_{32} & 0 & P_{34} \\ P_{41} & 0 & 0 & 0 \end{vmatrix} \tag{14}$$

Таким чином, матриця $(I-Q)^{-1}$ отримується у відповідності з виразом матричного перетворення:

$$(I-Q)^{-1} = 1/A \begin{vmatrix} A_{11} & A_{21} & A_{31} & A_{41} \\ A_{12} & A_{22} & A_{32} & A_{42} \\ A_{13} & A_{23} & A_{33} & A_{43} \\ A_{14} & A_{24} & A_{34} & A_{44} \end{vmatrix},$$

де A визначник матриці (вираз 12); A_{ij} - алгебраїчні доповнення відповідних елементів матриці (вираз 14).

Звідки матриця N^* буде мати вигляд:

$$N^* = 1/A \begin{vmatrix} A_{11}m_1 & A_{21}m_1 & A_{31}m_1 & A_{41}m_1 \\ A_{12}m_2 & A_{22}m_2 & A_{32}m_2 & A_{42}m_2 \\ A_{13}m_3 & A_{23}m_3 & A_{33}m_3 & A_{43}m_3 \\ A_{14}m_4 & A_{24}m_4 & A_{34}m_4 & A_{44}m_4 \end{vmatrix}.$$

Оскільки для вибраного початкового стану суттєвими є чисельні значення A, A_{11}, A_{21}, A_{31}, A_{41}, визначимо їх.

$$A = (1-P_{20})(1-P_{11}-P_{41}P_{34}P_{13}) - P_{21}(P_{12}+P_{13}P_{32}) - P_{41}P_{24}(P_{21}+P_{13}P_{32});$$

$$A_{11} = 1-P_{22};$$

$$A_{21} = P_{12}+P_{13}P_{32};$$

$$A_{31} = P_{13}(1-P_{22});$$

$$A_{41} = (1-P_{22})P_{13}P_{34} + P_{24}(P_{12}+P_{13}P_{32}).$$

Звідки середній час безпечного функціонування системи, що розглядається, складе:

$$t = \frac{m_1}{A}(A_{11}+A_{12}+A_{13}+A_{41}).$$

Висновки.

Запропонована методика дозволяє:

- обгрунтувати ряд нормативних положень, керуючих документів по технічному захисту інформації в Україні;
- порівняти технічні засоби захисту інформації від НСД, що реалізовані програмними та програмно-апаратними засобами;
- формувати системний підхід при рішенні задачі організації експлуатації технічних засобів захисту інформації та інших задач.

ЛІТЕРАТУРА

1. Майника Э. Алгоритмы оптимизации на сетях и графах / Майника Э. – М.: Мир, 1981. – 323 с.
2. Розенберг В.Я. Что такое теория массового обслуживания / Розенберг В.Я., Прохоров А.И. – М.: Сов. радио, 1962. – 254 с.
3. Вунш. Г. Теория систем / Вунш. Г. – М.: Сов. радио, 1978. – 288 с.
4. Феллер В. Введение в теорию вероятностей и ее приложения. В 2-х томах. / Феллер В. – М. Мир, 1967.
5. Ленков С.В. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

Надійшла: 17.10.2012р.

Рецензент: д.т.н., проф. Козловський В.В.