УДК 004.891

С.В. Лєнков,
доктор технічних наук, професор
В.М. Джулій,
кандидат технічних наук, доцент
І.В. Муляр,
кандидат технічних наук, доцент

ДИНАМІЧНІ ПОКАЗНИКИ ОЦІНКИ РІВНЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

У статті розглядаються підходи до розрахунку основних динамічних показників захищеності інформації та аналіз щодобових розподілів імовірностей неприпинених нелегальних доступів у інформаційну систему. Запропоновано ймовірнісні функції, що визначають ступінь захищеності інформації на часовому інтервалі (0, t), розроблено методики їх використання для двох можливих випадків прогнозування процесу захисту.

Показано підходи до розрахунку основних динамічних показників захищеності інформації, апробовані до наявних реальних статистик припинених спроб нелегального доступу до інформації.

Ключові слова: *динамічні показники, система захисту, імовірнісні функції, ймовірність відбиття атак, нелегальні користувачі, прогнозування.*

В статье рассматриваются подходы к расчету основных динамических показателей защищенности информации и анализ ежесуточных распределений вероятностей непрекращенных нелегальных доступов в информационную систему. Предложены вероятностные функции, определяющие степень защищенности информации на временном интервале (0, t), разработаны методики их использования для двух возможных случаев прогнозирования процесса защиты.

Показаны подходы к расчету основных динамических показателей защищенности информации, апробированы по имеющимся реальным статистикам приостановленных попыток нелегального доступа к информации.

Ключевые слова: *динамические показатели, система защиты, вероятностные функции, вероятность отражения атак, нелегальные пользователи, прогнозирования.*

Paper discusses several approaches to the calculation of basic dynamic performance data protection and analysis of daily probability distributions of non-terminated illegal access to an information system. The proposed probabilistic features defining the degree of protection of the information in the time interval (0, t), developed methods of using them for two possible cases of forecasting the protection process: when the data of the experiment or data protection system developer known for the average probability of reflection attacks of illegal users, thereby directly is known for the intensity of the flow of illegals entering the system to protect and where such data are not available and the problem is solved under conditions of uncertainty in the parameter.

Keywords: *dynamic performance, protection system, probability function, probability of reflection attacks, illegal users, forecasting.*

Вступ. Зростання погроз несанкціонованого доступу нелегальних користувачів до електронних джерел інформації вимагає розробки й упровадження адекватних заходів щодо припинення подібних спроб. Протидія можливим незаконним проникненням у інформаційне поле об'єкта здійснюється програмно-апаратними засобами, сукупність яких утворює *систему захисту* (далі – СЗ) цього об'єкта.

Постановка й проведення дослідження можливостей програмно-апаратних засобів захисту електронних джерел інформації становлять актуальну дослідницьку задачу і мають на меті розробку математичної моделі функціонування системи захисту на розглянутому проміжку часу тривалістю *t*.

Виконана статистична обробка наявних спостережень по припиненню спроб несанкціонованого доступу до електронних носіїв інформації показує, що статистичні розподіли вибірок відбитих СЗ атак нелегалів переважно описуються законом Пуассона. Так, за результатами досліджених щомісячних статистичних спостережень (43 вибірки) в 38 випадках гіпотеза пуассонівського розподілу мала безумовне підтвердження на рівні значимості $\alpha = 0.05$, у 3-х випадках час між подіями апроксимується законом Релея, у 2-х – нормальним законом. Це стало досить переконливою підставою для того, щоб вважати вступаючий у діалог із СЗ потік звернень нелегальних користувачів пуассонівським або, у всякому разі, близьким до нього, а сам процес "відбиття – невідбиття" спроб вторгнень, що протікає в системі захисту – марківським процесом з дискретними станами й безперервним часом.

Постановка задачі. При розрахунку показників надійності захисту інформації в умовах невизначеності дослідник має у своєму розпорядженні неупорядковану (по кількості відбитих атак) статистичну сукупність по типу табл. 1 і статистичний розподіл по типу табл. 2, з якого визначається інтенсивність λ_0. Щодо інтенсивності λ-вхідного потоку атак (спроб нелегального проникнення до інформації) будь-які дані відсутні.

Таблиця 1

Кількість щоденних відбитих атак за місяць

Дні місяця	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Кількість відбитих атак	3	1	0	2	0	4	1	3	2	0	2	2	3	2	2	1
Дні місяця	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	–
Кількість відбитих атак	0	2	2	1	3	3	2	2	0	0	1	0	0	1	1	–

Таблиця 2

Статистичний розподіл вибірки відбитих атак

x_i	0	1	2	3	4
n_i	8	7	10	5	1

Щоб вирішити невизначеність по невідомому параметру λ, конче необхідне деяке загальне погоджувальне правило (допущення, домовленість), на основі якого можна здійснити обґрунтований вибір шуканого невідомого. Крім того, необхідно визначитися щодо початкових умов, які повинен задовольняти параметр λ.

Варто погодитися із двома природньо обмежувальними початковими умовами:

а) виконанням нерівності $\lambda > \lambda_0$, що випливає з рівняння витрат;

б) припущенням, що розроблювачі СЗ гарантують забезпечення високої надійності $P_{OA} = \dfrac{\lambda}{\lambda_0}$ захисту інформації, такої, що виконуються нерівності

$$0 < \lambda - \lambda_0 < \varepsilon, \qquad \lambda_0 < \lambda < \lambda_0 + \varepsilon, \tag{1}$$

де ε – досить мала величина.

Загальна методика розрахунку показників надійності захисту інформації в умовах невизначеності. Для розрахунку інтенсивності λ вхідного потоку нелегальних користувачів використаємо метод екстремальної точки. Викладемо концептуальний підхід до питання й методики його рішення в рамках поставлених початкових умов.

Нехай є варіаційний ряд щодобових спостережень припинених спроб нелегального доступу до інформації з типу табл. 1. Послідовно підсумовуючи число таких спроб, створимо *накопичені* часткові суми $\{S_i(t_i)\}$ їхнього припинення на і-ту добу:

$$\{S_i(t_i)\}: \; S_1(1) = n_1, \;\; S_2(2) = n_1 + n_2, \; \ldots, \;\; S_i(i) = n_1 + n_2 + \ldots + n_i, \tag{2}$$

де n_i – число припинених спроб в і-ту добу; $i = \overline{1, n}$.

Знайдені суми (2) поставимо у відповідність до часу спостереження. Таким чином, визначиться функція $S(t)$, задана таблично (табл. 3).

Таблиця 3

Табличне завдання функції $S(t)$ накопичених сум припинення спроб нелегальних вторгнень у інформаційне поле об'єкта

$t_i(сутки)$	1	2	…	i	…	n
$S_i(t_i)$	n_1	n_2	…	$n_1 + n_2 + \ldots + n_i$	…	$n_1 + n_2 + \ldots + n_n$

$S(t)$ – функція натурального аргументу, тому її графік зобразиться на декартовій площині $0tx$ (рис. 1) у вигляді множини $(t_i, S_i(t_i))$ ізольованих точок.

Введемо основні поняття, що будуть використовуватися надалі.

Позначимо через $X(t)$ невідому функцію *накопичених сум усіх спроб нелегальних проникнень* до інформації, що захищається, на момент часу *t*. Очевидно, що сума всіх спроб не може бути менше суми припинених спроб, якщо обидві суми віднесені до того самого часу t, то у всіх випадках –

$$X(t) \geq S(t) \tag{3}$$

Зауважимо, що рівняння (3) може бути порушене в будь-якій точці проміжку спостережень. При цьому, будучи порушеним хоча б тільки раз, воно надалі залишається нерівністю зазначеного в (3) змісту до закінчення спостережень, маючи тенденцію до свого посилення в процесі функціонування СЗ. Для неідеального захисту значення $X(t)-S(t)$ на проміжку часу спостережень кінцевої тривалості t_n може виражатися тільки числом натурального ряду. Отже, у самій сприятливій нагоді різниця накопичених сум має точну нижню границю, рівну найменшому натуральному числу, тобто,

$$X_n(t_n)-S_n(t_n)\geq 1\,.$$

Цією різницею, у свою чергу, визначається нижня оцінка (оцінка ліворуч) $\lambda_л$ для шуканої інтенсивності λ на вході СЗ , а саме:

$$\frac{S_n(t_n)+1}{t_n}=\lambda_л\leq\lambda \tag{4}$$

Складніше в умовах невизначеності коректно виконати оцінку шуканої λ праворуч. Покажемо один із прийнятних варіантів такої оцінки для СЗ, що задовольняють нерівностям (1).

У найпростіших пуассонівських системах дискретній множині $(t_i,S_i(t_i))$ ставиться у відповідність безперервна лінійна функція

$$S(t)=\lambda_0 t\,, \tag{5}$$

з'єднуюча початок координат із точкою $K(t_n,S_n(t_n))$ закінчення спостережень. Зауважимо при цьому, що статистична інтенсивність λ_0 припинення спроб нелегальних вторгнень є не що інше як відношення накопиченої суми $S_n(t_n)$ таких спроб на проміжку спостережень до довжини цього проміжку, тобто,

$$\lambda_0=\frac{S_n(t_n)}{t_n}\,. \tag{6}$$

Зовсім неважливо, по якому шляху на площині $0tx$ відбувалося нагромадження часткових сум відбиття спроб нелегального доступу до інформації (рис. 1), значення має тільки кінцева точка K цього шляху.

Пряму $0K$, що виражається рівнянням

$$\lambda_0 t-S(t)=0\,, \tag{7}$$

назвемо *базисною прямою* цієї дискретної множини $(t_i,S_i(t_i))$.

Базисна пряма ділить координатну площину на дві напівплощини. Точки множини $(t_i,S_i(t_i))$ над цією прямою перетворюють рівність (7) у нерівність:

$$\lambda_0 t_i-S_i(t_i)<0\,;$$

точки тієї ж множини під базисною прямою – в нерівності протилежного змісту:

$$\lambda_0 t_i-S_i(t_i)>0\,.$$

Екстремальною для цієї множини $(t_i, S_i(t_i))$ назвемо точку *E,* розташовану над базисною прямою на найбільшій відстані від неї (рис. 1).

Положення екстремальної точки можна визначити на графіку $S(t)$. Покажемо аналітичний спосіб.

Відстань від точки до прямої визначається довжиною перпендикуляра, опущеного із точки на пряму. Якщо пряма задана її загальним рівнянням у системі координат $0xy$, то шукана відстань α обчислюється по формулі

$$\alpha = \frac{\left| Ax^* + By^* + C \right|}{\sqrt{A^2 + B^2}}, \tag{8}$$

де A, B – коефіцієнти рівняння прямої, C – вільний член рівняння, x^*, y^* – координати точок.

У системі координат $0tx$ у формулі (8) змінну x^* необхідно замінити на t_i, змінну y^* на S_i.

У рівнянні (7) базисної прямої $A = \lambda_0$, $B = -1$, $C = 0$, тому відстань від будь-якої точки множини $(t_i, S_i(t_i))$ до цієї прямої становить

$$\alpha_i = \frac{\left| \lambda_0 t_i - S_i(t_i) \right|}{\sqrt{1 + \lambda_0^2}}. \tag{9}$$

Перебором точок табл. 3 і розрахунками по формулі (9) визначається та точка *E*, у якій $\alpha_i = \alpha_{\max}$. Обчислення можна скоротити розрахунком числової послідовності

$$\delta_i = \lambda_0 t_i - S_i(t_i) \tag{10}$$

і на множині $\{\delta_i\}$ вибрати найменше (від'ємне) значення. Йому будуть відповідати координати $t_E = t_i, x_E = S_i$ екстремальної точки.

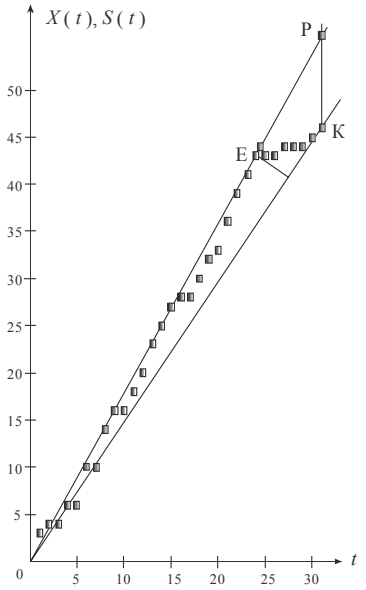

Рис. 1. Дискретна множина спостережуваних накопичених сум припинених спроб нелегального доступу до інформації

Усе зазначене повною мірою ставиться до невідомої (віртуальної) дискретної множини $(t_i, X_i(t_i))$, для якої існують і екстремальна точка E', і базисна пряма

$$X(t) = \lambda_n t, \tag{11}$$

де λ_n – постійна інтенсивність (оцінка зверху або праворуч шуканої інтенсивності λ).

Зауважимо, що така множина $(t_i, X_i(t_i))$ є підмножиною множини $(t_i, X_i(t_i))$, тобто

$$(t_i, X_i(t_i)) \supset (t_i, S_i(t_i)), \tag{12}$$

і перетину їхніх елементів $(t_i, X_i(t_i)) \bigcap (t_i, S_i(t_i))$ відповідають ті точки спостереження, де спроби нелегального проникнення в інформаційне поле об'єкта не мали успіху до тієї критичної точки $(t_i^*, X_i^* > S_i(t_i))$, де вперше це відбулося хоча б один раз. Очевидно, що

$$(t_i, X_i(t_i)) \setminus (t_i, S_i(t_i)) = \overline{(t_i, S_i(t_i))} \tag{13}$$

Очевидно також, що чим надійніша СЗ, тим більший проміжок часу $(0, t_i^*)$, тим менше число елементів містить різниця (13). Водночас реалізований однократний прорив СЗ активізує наступний процес нелегальних проникнень.

Приймемо, що критична точка t^* одиночного нелегального доступу до інформації збігається з t_E так, що елемент $(t_E, x_E + 1 \in)\overline{(t_i, S_i(t_i))}$ і є його першим елементом. Приймемо також, що координати точки проникнення $\Pi(t_E, x_E + 1)$ в інформаційну систему задовольняють рівняння (13). Тоді для оцінки шуканої інтенсивності λ зверху (праворуч) одержимо такий вираз:

$$\lambda = \frac{x_E + 1}{t_E} \tag{14}$$

Перепишемо рівняння (11) з урахуванням (14). Отримаємо рівняння:

$$X(t) = (x_E + 1)\frac{t}{t_E}. \tag{15}$$

Отже, накопичена сума всіх спроб нелегальних проникнень складе величину

$$X_n(t_n) = (x_E + 1)\frac{t_n}{t_E}. \tag{16}$$

Знайдене значення ординати (16) розрахункової токчи P (рис. 1) треба округлити до найближчого цілого числа й уточнити оцінку (14). Остаточно отримаємо таку інтервальну оцінку для інтенсивності λ на вході СЗ –

$$\frac{S_n(t_n) + 1}{t_n} \le \lambda < \frac{\overline{X}_n(t_n)}{t_n}, \tag{17}$$

де $\overline{X}_n(t_n) > X_n(t_n)$ і ціле.

Покажемо приклад розрахунку інтервальної оцінки (17) за викладеною методикою для конкретного випадку спостережень відбиття атак нелегальних користувачів (табл. 1).

За вихідними даними табл. 1 порахуємо послідовність часткових сум (12) і заповнимо табл. 4.

Таблиця 4

Функція $S(t)$ накопичених сум припинених спроб нелегального доступу до інформації

Дні місяця	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Кількість відбитих атак	3	4	4	6	6	10	11	14	16	16	18	20	23	25	27	28
Дні місяця	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	–
Кількість відбитих атак	28	30	32	33	36	39	41	43	43	43	44	44	44	45	46	–

З табл. 4 знайдемо $\lambda_0 = \frac{S_{31}}{31} = \frac{46}{31} = 1.4838709 \frac{1}{добу}$ й напишемо вираз (10): $\delta_i = 1.4838709 t_i - S_i(t_i)$.

На підставі даних табл. 4 обчислюємо послідовність $\{\delta_i\}$.

Отримаємо

$\delta_1 = -1.5161291$, $\delta_2 = -1.0322582$, $\delta_3 = 0.4516127$, $\delta_4 = -0.0645164$, . . .

. . . $\delta_{21} = -4.83871$, $\delta_{22} = -6.354839$, $\delta_{23} = -6.870968$, $\delta_{24} = -7.387097$, . . .

. . . $\delta_{28} = -2.451613$, $\delta_{29} = -0.967742$, $\delta_{30} = -0.483871$, $\delta_{31} = 0$

Члену послідовності $\delta_{24} = -7.387097$ відповідає екстремальна точка *E*. Її координати $t_E = 24, x_E = 43$.

По формулі (16) знайдемо $\overline{X}_n(t_n) = \frac{44*31}{24} = 56.833333$, отже $\overline{X}_n(t_n) = 57$, і інтервальна оцінка (17) тут виходить така:

$$\frac{47}{31} \le \lambda < \frac{57}{31}, \quad 1.516129 \le \lambda < 1.8387096 \tag{18}$$

Для середньої ймовірності $P_{OA} = \lambda_0/\lambda$ відбиття атак нелегальних користувачів числові нерівності (18) перетворяться в нерівності протилежного змісту. Отримаємо

$$\frac{1.4838709}{1.8387096} \le P_{OA} < \frac{1.4838709}{1.516129}, \quad 0.80701753 < P_{OA} \le 0.97872338.$$

Середині інтервалу відповідає значення $P_{OA} = 0.89287045$. Таким чином, використовувана на об'єкті СЗ відповідає системам 2-го класу.

Обчислення інтервальної оцінки (17) зводиться до такого алгоритму.

1. Неупорядковану статистичну сукупність у вигляді таблиці 1 необхідно перетворити в таблицю 4 накопичених сум припинених спроб нелегальних проникнень в інформаційну систему.

2. За координатами останньої точки й формулою (3.20) визначається оцінка інтенсивності λ ліворуч.

3. За формулою (14) визначається λ_B .

4. За формулою (10) обчислюється послідовність $\{\delta_i\}$.

5. З $\{\delta_i\}$ вибирається найменше число $\delta_{\min} < 0$ й відповідні цьому числу координати t_E, x_E екстремальної точки.

6. За формулою (16) обчислюється $\overline{X}_n(t_n)$ і найближче до знайденого значення ціле число $\overline{X}_n(t_n)$.

7. За формулою (17) формується інтервальна оцінка шуканої інтенсивності λ.

Блок-схема алгоритму визначення числової нерівності (17) показана на рис. 2.

В умовах невизначеності за параметром λ розрахунок і аналіз функціональних показників ефективності застосовуваної СЗІС реалізується двома блоками комп'ютерних програм: блоком інтервальної оцінки цього параметра й розробленим раніше блоком обчислення основного показника $P_0(t)$ і його доповненням $\overline{P}_0(t)$ до одиниці. При цьому функціональні показники $P_0(t)$, $\overline{P}_0(t)$ обчислюються за оцінним значенням λ ліворуч і праворуч (формула (17)). У табл. 5 для прикладу показані розрахункові значення зазначених функцій для $\lambda_л = 1{,}516129$, $\lambda_n = 1{,}8387096$. На рис. 3 побудовані графіки основного функціонального показника $P_0(t)$ для обох оцінок $\lambda_л, \lambda_n$ і відповідні їм криві $\overline{P}_0(t)$.

Таблиця 5

Розрахунок значень $P_0(t)$, $\overline{P}_0(t)$ на граничних значеннях інтенсивностей $\lambda_л, \lambda_n$ вхідного потоку нелегальних користувачів

t (доба)	0	5	10	15	20	25	30
$P_0(t)_л$	1	0, 927105	0, 854903	0, 788324	0, 726930	0, 670317	0, 618114
$P_0(t)_n$	1	0, 414964	0, 162973	0,064006	0, 025138	0, 009872	0, 003877
$\overline{P}_0(t)_л$	0	0, 072894	0, 145096	0, 211675	0, 273069	0, 329682	0, 381885
$\overline{P}_0(t)_n$	0	0, 585035	0, 837026	0, 935993	0, 974861	0, 990127	0, 996122

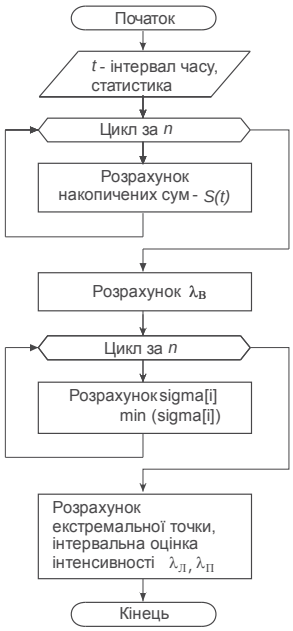

Рис. 2. Блок-схема алгоритму розрахунку інтервальної оцінки λ в умовах невизначеності

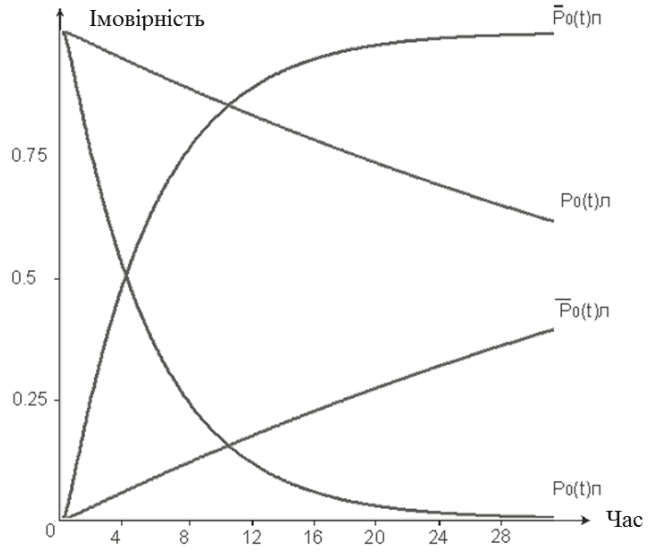

Рис. 3. Графіки основних функціональних показників ефективності системи захисту інформаційної системи на границях оцінного інтервалу інтенсивності λ

Висновки. Для розрахунку основних динамічних показників захищеності інформації й аналізу щодобових розподілів імовірностей неприпинених нелегальних доступів у інформаційну систему розроблені імовірнісні функції, що визначають ступінь захищеності інформації на часовому інтервалі (0, t), розроблені методики їх використання для двох можливих випадків прогнозування процесу захисту: коли за даними проведеного експерименту або за даними розроблювача системи захисту відома середня ймовірність P_{OA} відбиття атак нелегальних користувачів і таким чином безпосередньо відома інтенсивність λ потоку нелегалів на вході СЗ; коли такі дані відсутні й завдання вирішується в умовах невизначеності за параметром λ.

Показані методики апробовані до наявних реальних статистик припинених спроб нелегального доступу до інформації.

Принциповою відмінністю реалізованого підходу до завдань від тих описових схем, з якими повсюдно доводиться зустрічатися в періодичних виданнях і в Інтернеті, є його завершеність на рівні аналітичних функцій і кількісних оцінок ефективності захисту інформації, які не тільки дозволяють об'єктивно судити про можливості діючої на об'єкті СЗІС, але й вчасно вживати адекватні заходи з її раціонального використання й удосконалювання в процесі експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко. – К. : "МК-Пресс", 2006. – 320 с.
2. Программирование алгоритмов защиты информации : учебное пособие / А.В. Домашев, В.О. Попов, Д.И. Правиков, И.В. Лрокофьев, А.Ю. Щербаков. – М. : "Нолидж", 2000. – 288 с.
3. *Домарев В.В.* Безопасность информационных технологий. Системный подход / В.В. Домарев. – К. : ООО "ТИД "ДС", 2004. – 992 с.
4. *Овчаров Л.А.* Прикладные задачи теории массового обслуживания / Л.А. Овчаров. – М. : "Машиностроение", 1989. – 324 с.
5. *Галицкий А.В.* Защита информации в сети – анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньган. – М. : ДМК Пресс, 2004. – 616 с.

Отримано 13.06.2016
Рецензент Рибальський О.В., д.т.н.