УДК 519.876.5

О.В. Бойченко[1], І.В. Пампуха[2], Н.М. Берназ[3]

[1] *Національний авіаційний університет, Київ*
[2] *Військовий інститут Київського національного університету ім. Т. Шевченка, Київ*
[3] *Одеський національний політехнічний університет, Одеса*

# МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ВИБОРУ РАЦІОНАЛЬНОГО РОЗМІРУ БЛОКІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ, ЩО ПІДЛЯГАЮТЬ ЗАХИСТУ

*Розглядається питання моделювання вибору раціонального розміру блоків інформаційної системи, що підлягають захисту. Запропонована математична модель створення умов для знаходження оптимального числа захищених блоків інформаційних систем підтримки рішень (ІСПР), при яких досягається найбільший ефект від захисту.*

***Ключові слова:*** *інформаційна система підтримки рішень, система захисту.*

## Вступ

**Постановка проблеми.** Практика функціонування інформаційних систем підтримки рішень (ІСПР) при виконанні завдань, пов'язаних із правоохоронною діяльністю, вказує на доволі суттєву низку проблем, визначених прогалинами в підсистемі захисту інформаційних ресурсів ІСПР [1 – 3]. Незважаючи на доволі потужний ресурсний потенціал системи інформаційної безпеки ІСПР, вказані проблеми загострюються з приводу суттєвого збільшення обсягів даних сучасних ІСПР, невизначеністю їхніх форматів за обсягом та часом, а також застосуванням різноманітних систем безпеки для захисту блоків ІСПР [4 – 6]. У такому випадку необхідним є розроблення математичної моделі вибору раціонального розміру блоків ІС, що підлягають захисту.

**Мета роботи** полягає у розробці математичної моделі дозволяє створення умови для знаходження оптимального числа захищених блоків ІСПР, при яких досягається найбільший ефект від захисту.

## Виклад основного матеріалу

Формула для вибору раціонального розміру блоків, що підлягають захисту, може бути отримана із таких міркувань. Нехай $b_i$ – число команд в блоці $M_i$, що захищений паролем $П_i$; $\alpha$ – імовірність збою при виконанні команди (з урахуванням циклів); l – число машинних команд для реалізації одного пароля; L – додаткова пам'ять, що потрібна для реалізації методу паролів;

$$L = nl,$$

де n – число паролів; B – пам'ять, що захищена паролями

$$B = \sum_{i=1}^{n} b_i,$$

$q_i$ – умовна імовірність невизначення збою при передачі управління системою $П_1,...,П_n$ при умові, що збій був у блоці $M_i$; q – безумовна імовірність невизначення збою системою паролів $П_1,...,П_n$ (безвідносно до того або іншого блоку); C – обсяг пам'яті, не захищеної системою паролів (захищеної іншими системами); V – загальний обсяг пам'яті,

$$V = B + C + L.$$

Очевидно, що

$$q_i = \frac{(b_i + L + C)}{B + L + C} + p_i \frac{(b_i + L + C)}{B + L + C} + ... + p_i^n \frac{(b_i + L + C)}{B + L + C} = \frac{b_i + L + C}{V(1 - p_i)}. \quad (1)$$

Тут $p_i$ – сумісна імовірність того, що при випадковому збої в блоці $M_i$ управління передається іншому блоку, але збій не буде виявлений паролем, що відповідає черговому (після збою) блоку (до якого потрапило управління) через виникнення чергового збою у вказаному блоці.

$$p_i = \sum_{k \neq i} \frac{b_k}{V} \left( \frac{1}{b_k} \cdot \sum_{r=0}^{b_k} \left[ 1 - (1 - \alpha)^r \right] \right) = \frac{1}{V} \sum_{k \neq i} \left[ (b_k + 1) - \frac{1 - (1 - \alpha)^{b_k + 1}}{\alpha} \right]. \quad (2)$$

Формули можна спростити при припущеннях, що не протирічать практиці. При $\alpha \to 0$ маємо

$$q_i = \frac{b_i + L + C}{V - \sum_{k \neq i} \left( b_k + 1 - \frac{1 - \ell^{-\alpha(b_k + 1)}}{\alpha} \right)}. \quad (3)$$

При малих розмірах блоків ($\alpha b_k \to o$) після певних перетворень отримаємо

$$q_i = (b_i + L + C) \Big/ \left( V - \frac{\alpha}{2} \sum_{k \neq i} (b_k + 1)^2 \right). \quad (4)$$

Знайдемо мінімум $q_i$ при фіксованому значенні $b_i$. Очевидно, що задача знаходження оптимальних величин обсягів блоків $b_{k,k \neq i}$ при фіксованому $b_i$ може бути зведена до задачі знаходження опти-

 

мальних величин $b_{k,k\neq i}$, які мінімізують функцію

$$f(b_1,...,b_{k-1}) = \sum_{k=1}^{n-1}\left( b_{k+1} - \frac{1-\ell^{-\alpha(b_k+1)}}{\alpha}\right). \quad (5)$$

При обмеженнях

$$\sum_{k=1}^{n-1} b_k = B - b_i; b_k \geq 0. \quad (6)$$

Застосувавши заміну $y_k = b_k + 1$ і зробивши необхідні перетворення, отримаємо систему

$$y_k = B - b_i + (n-1) - (y_1 + y_2 + ... + y_{n-2}); \quad k = \overline{1, n-2} \quad (7)$$

Звідки випливає

$$y_1 = y_2 = ...y_{n-2} \quad (8)$$

і остаточно

$$b_{1l} = b_2 = ...b_{n-2}. \quad (9)$$

Таким чином, ми показали, що при фіксованих $n$ й $b_i$ мінімум $q_i$ досягається, якщо обсяги захищених блоків будуть рівними між собою.

Припускаючи

$$b_i = B/n, \overline{i, n.} \quad (10)$$

Отримаємо при $\alpha \to 0$

$$q_i = \frac{B/n + L + C}{V - (n-1)\left(B/n + 1 - \left(1-\ell^{-\alpha(B/n+1)}\right)/\alpha\right)}. \quad (11)$$

При $\alpha B/n \to o$:

$$q_i = \frac{B/n + L + C}{V - \alpha/2(n-1)(B/n+1)^2}. \quad (12)$$

Безумовна імовірність того, що випадковий збій не буде виявлений системою паролів $\{\Pi_i\}$, дорівнює

$$q = \frac{b_i}{B}\sum_{i=1}^{n} q_i.$$

Дійсно, оскільки відмови із імовірністю $\alpha$ являють собою рідкі події $(\alpha \to 0)$, ми можемо стверджувати (із посиланням на теорему Пуассона й особливості експоненційного закону розподілу), що момент появи збою має рівномірний розподіл, тобто імовірність появи випадкового збою в модулі $M_i$ при умові, що збій відбувся) дорівнює $b_i/B$.

Беручи до уваги (10), отримаємо

$$q = \frac{1}{n}\sum_{i=1}^{n} q_i = q_i. \quad (13)$$

**Нові наукові досягнення.** Знайдемо оптимальне число захищених блоків, при якому досягається найбільший ефект від захисту, тобто $q_i = q_{i\min}$.

Підставляючи $L = nl$ у (12), отримаємо

$$q_i = \frac{B/n + nl + C}{B + nl + C - (\alpha/2)(n-1)(B/n+1)^2} = \frac{an^3 + bn^2 + cn}{dn^3 + en^2 + fn + g},$$

де $a = 2l, b = 2C, c = 2B, d = 2l - \alpha, e = 2B + 2C + 2\alpha B + \alpha, f = 2\alpha B - \alpha B^2, g = \alpha B^2.$

Звідси оптимальне $n$ знаходиться із рівняння

$$a_4 n^4 + a_3 n^3 + a_2 n^2 + a_1 n + a_0 = 0, \quad (14)$$

де
$a_4 = 2l(2B + 4l + \alpha(2B+1)) - 2\alpha C,$
$a_3 = 4B(\alpha(l(2-B)+1) - 2l),$
$a_2 = 2B(\alpha(B(3l - C - 2) + 2C) - 2(B + C) - \alpha),$
$a_1 = 2\alpha B^2(2C - B - 2),$
$a_0 = 2\alpha B^2.$

При $\alpha \to 0$ маємо

$$q_i = \frac{B/n + nl + C}{B + C + (n-1)\left(B/n + 1 - \frac{1-\ell^{-\alpha(B/n+1)}}{\alpha}\right)}.$$

Зробивши декілька перетворень, отримаємо

$$n^* = 1 + \sqrt{1 + \frac{B+C}{l}}. \quad (15)$$

## Висновки

Розроблена математична модель дозволяє створити умови для знаходження оптимального числа захищених блоків ІСПР, при яких досягається найбільший ефект від захисту. Зазначене забезпечує оптимізацію процесу управління захистом інформації в ІСПР правоохоронної діяльності та підвищує функціональність системи для підтримки управлінських рішень в діяльності підрозділу ОВС.

## Список літератури

*1. Бойченко О.В. Модель корпоративного інформаційного захисту об'єкту інформатизації / О.В. Бойченко, Я.І. Торошанко // Наукові записки українського науково-дослідного інституту зв'язку. – К., 2011. – Вип. 4 (20). – С. 15-19.*

*2. Бойченко О.В. Проблеми інформаційної безпеки при використанні економічних систем управління / О.В. Бойченко // Вісник українського науково-дослідного інституту зв'язку. – К., 2010. – № 1. – С. 45-49.*

*3. Бойченко О.В. Оцінка якості та оптимізація функціонування інформаційних систем / О.В. Бойченко // Захист інформації: наук.-техн. ж. – К., 2011. – № 2 (51). – С. 105-107.*

*4. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О.В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009): Друга міжнар. наук.-пр. конф. 25-28 травня 2009 року. – К.: НАУ, 2009. – С. 230-232.*

*5. Бойченко О.В. Принципи відомчої політики у сфері захисту інформації в інформаційно-аналітичних системах ОВС / О.В. Бойченко // Наук.-пр. конф. «Захист в інформаційно-телекомунікаційних системах». – К.: НАУ, 2010. – С. 111-112.*

*6. Бойченко О.В. Інформаційна безпека телекомунікаційних систем спеціального призначення / О.В. Бойченко // Мат-ли доповідей 14-ї міжнар. наук.-пр. конф. «Новітні мережні технології в Україні». АР Крим, с. Партеніт, 23-25 вересня 2011 р. – К. УНДІЗ, 2011. – № 1. – С. 119-124.*

*Надійшла до редколегії 29.06.2012*

**Рецензент:** д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

## МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВЫБОРА РАЦИОНАЛЬНОГО РАЗМЕРА БЛОКОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ, КОТОРЫЕ ПОДЛЕЖАТ ЗАЩИТЕ

О.В. Бойченко, И.В. Пампуха, Н.М. Берназ

*Рассматривается вопрос моделирования выбора рационального размера блоков информационной системы, которые подлежат защите. Предложена математическая модель создания условий для нахождения оптимального числа защищенных блоков информационных систем поддержки решений (ИСПР), при которых достигается наибольший эффект от защиты.*

***Ключевые слова:*** *информационная система поддержки решений, система защиты.*

## MATHEMATICAL DESIGN OF CHOICE OF RATIONAL SIZE OF BLOCKS OF INFORMATIVE SYSTEM, WHICH ARE SUBJECT DEFENCE

O.V. Boychenko, I.V. Pampukha, N.M. Bernaz

*The question of design of choice of rational size of blocks of the informative system, which are subject to defence, is examined. The mathematical model of conditioning is offered for finding of optimum number of the protected blocks of ISSD, at which a most effect is arrived at from defence.*

***Keywords:*** *informative system of support of decisions, system of defence.*