

*Обґрунтовано актуальність урахування людського чинника при моделюванні систем захисту інформації в автоматизованих системах. Побудовано математичну модель для дослідження процесів впливу людського чинника на витік конфіденційної інформації*

*Ключові слова: людський чинник, захист інформації, конфіденційна інформація*

*Обоснована актуальность учета человеческого фактора при моделировании систем защиты информации в автоматизированных системах. Построена математическая модель для исследования процессов влияния человеческого фактора на утечку конфиденциальной информации*

*Ключевые слова: человеческий фактор, защита информации, конфиденциальная информация*

*The urgency of the human factor in the modeling of systems of information protection in automated systems is grounded. A mathematical model for studying the influence of human factor on the confidential information leakage is builded*

*Keywords: human factor, information security, confidential information*

# МАТЕМАТИЧНА МОДЕЛЬ ВИТІКАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ З УРАХУВАННЯМ ЛЮДСЬКОГО ЧИННИКА

**В.З. Табаков**

Кандидат технічних наук, доцент  
Кафедра інформаційних систем  
Інститут підготовки кадрів державної служби зайнятості  
України  
вул. Нововокзальна, 17, м. Київ, 03038  
Контактний тел.: 063-357-70-68, (044) 528-17-91

При управлінні інформаційними війнами часто використовується та обставина, що недбайливий або недобросовісний менеджер здатен перетворити контрольований ним чинник на ресурс суперника.

Проблемна ситуація пов'язана з ризиком просочування конфіденційної інформації до галузевих конкурентів [1]. Такий витік може привести до значних збитків як в бізнесі, так і в політиці.

Сьогодні захист інформації в автоматизованих системах конфіденційного діловодства на базі ПЕОМ, як правило, заснований на шифруванні і застосуванні електронних ідентифікаторів. Основним напрямом нейтралізації прихованих загроз і атак пов'язаних з неправомірними діями санкціонованих користувачів автоматизованих систем – осіб, що мають доступ на територію контрольованої зони і допущених до інформації, що захищається, є розробка і впровадження спеціальних програмно-апаратних комплексів захисту інформації [2].

Проте основною причиною витікання конфіденційної інформації залишається людський чинник, урахування якого вимагає розв'язання наступних задач: а) дослідження мотивів, що штовхають людей на порушення корпоративних угод і правопорушення; б) розробка механізмів управління секретносіями; в) розробка способів інформаційного впливу на санкціонованих користувачів автоматизованих систем і ін.

Для ефективного розв'язання перерахованих задач найбільш доцільним представляється створення математичної моделі витікання конфіденційної інформації з урахуванням людського чинника.

Розглянемо модель проблемної ситуації. Позначимо через  $i$  - номер оператора-секретноносія,  $i = \overline{1, N}$ , де  $N$  - загальне число операторів;  $q_i$  - об'єм блоку конфіденційної інформації, що знаходиться в користуванні  $i$ -го оператора;  $Q$  - повний об'єм конфіденційної інформації  $Q = \sum_{i=1}^N q_i$ ;  $C(q_i)$  - вартість блоку  $q_i$ , що складається з вартості його розробки, впровадження і експлуатації,  $k(q_i)C(q_i)$  - «продажна ціна» блоку  $q_i$  для конкурента, де  $C(q_i)$  - коефіцієнт корисності блоку  $q_i$  для конкурента,  $C(q_i) > 0$ .

Фрагмент  $q_i$  конфіденційної інформації тим цінніше для конкурента, чим більшою мірою він інформує про її повний об'єм  $Q$ . Чим більше об'єм фрагмента  $q_i$ , тим більше коефіцієнт його корисності для конкурента  $k(q_i)$  і його ціна  $k(q_i)C(q_i)$ . Передбачається, що  $k(q_i)$  монотонно зростає із збільшенням  $q_i$ , причому  $k(q_i) = 1$ , якщо  $q_i = Q$ . Тому  $0 < k(q_i) \leq 1$ . Типова залежність  $k(q_i)$  показана на рис. 1.

Приріст коефіцієнта корисності інформації для конкурента на ділянці від 0 до  $q_1$  незначний, оскільки після неї практично неможливо відновити необхідні відомості в повному об'ємі. На ділянці від  $q_2$  до

Q, приріст корисності інформації також невеликий, оскільки різко зростає вірогідність відновлення потрібних відомостей за вже придбаною інформацією.

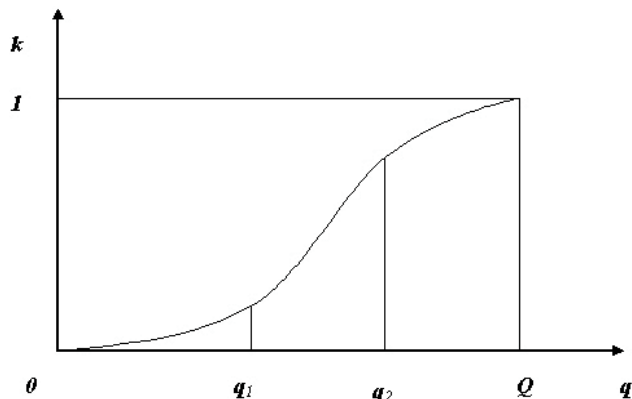


Рис. 1. Типова залежність коефіцієнта корисності інформації  $k(q_i)$  від її об'єму  $q_i$

У моделі виділяють п'ять класів порушників. Порушники 1-го класу не мають доступу в контрольовану зону. Їх пряму дію на елементи автоматизованої системи, що захищаються, виключено, але можливий зйом інформації по каналах ПЕОМ. Порушники з другого по п'ятий клас мають доступ в зону. Для порушників вищого класу характерні великі можливості доступу до ресурсів автоматизованої системи, починаючи від відсутності прямого фізичного доступу до АРМ, і закінчуючи необмеженими можливостями управління автоматизованою системою, в особі адміністратора.

Таким чином, система доступу до конфіденційної інформації має ієрархічну структуру. Оператор, що стоїть на нижньому рівні ієрархії доступу до конфіденційної інформації, контролює певний її фрагмент. Керівники підрозділів контролюють інформацію своїх підлеглих. Так, керівник  $j$ -го підрозділу контролює об'єм інформації, що дорівнює сумі об'ємів фрагментів, контрольованих його підлеглими:  $m_j = \sum_{i=1}^{M_j} q_i$ , де  $M_j$  - кількість операторів в  $j$ -му підрозділі,  $1 < j \leq K$ ,  $K$  - кількість підрозділів  $\sum_{j=1}^K M_j = N$ . Отже, вартість фрагмента інформації  $m$ , контрольованого керівником  $j$ -го підрозділу, дорівнює  $C(m_j)$ , а його «продажна ціна» -  $k(m_j)C(m_j)$ . Вартість конфіденційної інформації  $Q$ , контрольованої адміністратором автоматизованої системи, співпадає з її «продажною ціною», оскільки  $k(Q)=1$ .

Часто оператор продає інформацію нижче за її вартість, особливо якщо не знає останньої. Покупець інформації більш обізнаний про неї і пропонує ціну  $X$ . Прибуток  $V(q_i, X)$  продавця конфіденційної інформації, в ролі якого виступає  $i$ -й оператор, можна оцінити таким чином:

$$V(q_i, X) = X - p_{1i}(nD(q_i) + lB(q_i)) - p_{2i}R(q_i), \quad (1)$$

де  $p_{1i}$  - вірогідність викриття продавця;  $n$  - кількість місяців, які пропрацював би на фірмі продавець без правопорушення;  $D(q_i)$  - місячний оклад;  $l$  - кіль-

кість премій;  $B(q_i)$  - розмір премій;  $p_{2i}$  - вірогідність збитку у разі викриття;  $R(q_i)$  - розміри морального і матеріального збитку, виражені в грошах. Вираз (1) можна ускладнити, наприклад, враховуючи втрату викритим продавцем страховки, різниці в окладах після звільнення і переходу на менш оплачувану роботу. Проте дані уточнення у принципі не ускладнюють завдання.

Прибуток покупця  $\pi_i(q_i, X)$  можна оцінити таким чином:

$$\begin{aligned} \pi_i(q_i, X) &= k(q_i)C(q_i) - X - S(q_i) - p_{3i}U(q_i), \\ X &< k(q_i)C(q_i), \end{aligned} \quad (2)$$

де  $S(q_i)$  - засоби, витрачені на вербування продавця;  $p_{3i}$  - вірогідність викриття покупця;  $U(q_i)$  - матеріальні і моральні втрати внаслідок викриття, виражені в грошовій формі.

З (1) витікає, що для продавця прийнятна ціна за товар, що задовольняє вимозі:

$$X > p_{1i}(nD(q_i) + lB(q_i)) + p_{2i}R(q_i) \quad (3)$$

З (2) витікає, що для покупця прийнятна ціна за товар, що задовольняє вимозі:

$$X \leq k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i) \quad (4)$$

З (3) і (4) витікає, що для покупця прийнятна ціна за товар, що знаходиться в сегменті компромісу

$$\begin{aligned} [p_{1i}(nD(q_i) + lB(q_i)) + \\ + p_{2i}R(q_i), k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i)] \end{aligned} \quad (5)$$

Для операції необхідно, щоб сегмент компромісу (5) не був порожнім

$$\begin{aligned} p_{1i}(nD(q_i) + lB(q_i)) + \\ + p_{2i}R(q_i) \leq k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i) \end{aligned}$$

Звідси слідує важливий висновок: щоб виключити продаж конфіденційної інформації, досить виконати умову:

$$\begin{aligned} p_{1i}(nD(q_i) + lB(q_i)) + \\ + p_{2i}R(q_i) > k(q_i)C(q_i) - S(q_i) - p_{3i}U(q_i) \end{aligned}$$

Якщо як продавець конфіденційної інформації виступає керівник  $j$ -го підрозділу, то  $i$  і  $q_i$  слід замінити, відповідно на  $j$  і  $m_j$ . Якщо ж секретами автоматизованої системи торгує адміністратор, то  $q$  слід замінити на  $Q$ .

#### Література

1. Бухарин С.Н. Человеческий фактор в проблеме защиты информации от несанкционированного доступа в автоматизированных системах конфиденциального делопроизводства [Текст] / А.А. Кулемин // Стратегическая стабильность. - 2006.- №4. - С. 120 - 144.
2. Бухарин С.Н. Информационное противоборство. Книга 2. Теоретические основы [Текст] / А.Г. Глушков, И.Д. Ермолаев. - М.: Полиори, 2005. - 325 с.