

*О.Є. Архипов, доктор технических наук, профессор,  
С.А. Архипова, кандидат технических наук, доцент  
(Національний технічний університет України "КПІ", Україна)*

## **МОДЕЛЬ ЦІННОСТІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ**

*Розглянуто особливості визначення цінності конфіденційної інформації, зокрема, з урахуванням процесів старіння та фрагментації інформаційного ресурсу на окремі блоки. Наведено структуру моделей цінності інформації.*

Одним з базових положень побудови систем захисту інформації (СЗІ) є принцип розумної достатності, відповідно до якого витрати на побудову та супровід СЗІ мають співставлятися з можливими втратами, обумовленими реалізаціями загроз щодо інформації, яка підлягає захисту. Це дозволяє оптимізувати витрати на створення СЗІ, забезпечивши адекватність рівня захисту рівню цінності інформації. Тому визначення кількісного значення цінності інформації, яку треба захищати, є провідним моментом процедури оптимізації витрат на СЗІ.

Однак значення цінності інформації не можуть бути отримані шляхом прямого вимірювання, бо цінність інформації являє собою так звану латентну (приховану) властивість, яка є неспостережною й невимірною безпосередньо, оскільки до неї незастосовна процедура вимірювання еталонною одиницею. Для вимірювання латентної властивості необхідно виразити її через вимірювані властивості, які отримали назву індикаторів. Сукупність індикаторів, що заміняє латентну властивість (змінну), утворює операціональний референт або операціональний конструкт. Він використовується замість латентної змінної в усіх залежностях, в які вона входить. Операціональний конструкт повинен бути достатньо валідним відносно своєї латентної змінної, тобто має достатньо точно відтворювати її властивості, критичні для всіх застосувань, де задіяна латентна змінна.

В найпростішому випадку операціональним конструктом може бути окремий індикатор, зокрема, для латентної змінної "цінність інформації" їм може бути придатність інформації до практичного застосування. В цьому разі спосіб вимірювання значень обраного індикатора залежить від мети використання інформації у кожному конкретному практичному застосуванні, що в кінцевому підсумку й обумовлює появу множини підходів і методів оцінювання рівнів індикаторів.

Якщо у якості індикатора латентної змінної "цінність інформації" взяти корисність використання інформації у різних прикладних застосуваннях, та як одну з головних вимог визначити необхідність грошової форми представлення значень цього індикатора, отримуємо достатньо універсальний операціональний конструкт, незалежний від способу "вимірювання" (обчислення) рівня корисності у кожному конкретному застосуванні. Мається на увазі, що при оцінюванні рівня корисності, обумовленої зростанням ефективності виконанням несхожих прикладних завдань завдяки використанню певної допоміжної інформації, припустиме застосування відповідних не співпадаючих способів обчислення цієї корисності. Головне – щоб ці оцінки були обчислені в єдиній шкалі, що забезпечує можливість їх наступного порівняння та сумісного дослідження. Зауважимо, що аналіз літературних джерел дозволяє констатувати, що в більшості випадків оцінювання цінності інформації, за умов дотримання певних додаткових вимог, зводиться саме до оцінювання корисності прикладних застосувань цієї інформації. Це дозволяє сформулювати наступне положення: цінність інформації вимірюється рівнем максимальної корисності, отриманої від залучення оцінюваної інформації до оптимізації виконання певного завдання (виконання роботи, розв'язання задач та проблемних ситуацій, оптимізації параметрів виробничого процесу тощо) за умови найліпшого способу використання цієї інформації. Деякий екстремізм цього твердження, що його вносять звороти "максимальна користь", "найліпший спосіб використання", отримав назву принципу

(умов) екстремальності. Очевидно, що якість конкретного прикладного застосування інформації може бути різною. Відтак корисність цієї інформації може змінюватися в широких межах. Дотримання принципу екстремальності гарантує найвищу якість використання інформації, відповідно найвищу (максимальну) корисність її застосування. Кількісна оцінка цієї максимальної корисності визначає цінність інформації. Тобто саме наявність принципу екстремальності в наведеному тлумаченні цінності інформації є запорукою коректного однозначного кількісного визначення цінності.

Формально цінність інформації можна відповідно до викладеного вище визначити наступним чином:

$$V(I) = \Delta A_{extr}(I) - d(I), \quad (1)$$

де  $A$  – показник, що характеризує ступінь успішності виконання певного завдання, роботи, іншого виду діяльності (цим показником може бути вартість продукції, виготовленої за певний час чи з фіксованого обсягу вихідної сировини, виграш, обумовлений вибором вдалого рішення, загальна вартість послуг, наданих споживачам у певній сфері діяльності тощо);

$d(I)$  – витрати на одержання, обробку та використання інформації  $I$  у певному виді діяльності;

$\Delta A$  – покращення (зростання) показника  $A$  за рахунок отриманої інформації  $I$ :

$$\Delta A(I) = A(I) - A_0, \quad (2)$$

де  $A_0$  – вихідне значення показника (за відсутністю інформації  $I$ ),  $A(I)$  – зросло завдяки використанню інформації  $I$  значення показника  $A$ . Зокрема, значення  $A$  може збільшитись внаслідок застосування отриманої інформації для оптимізації параметрів виробничого процесу, зменшення можливих хибних або неперспективних варіантів рішення певної проблеми, зростання іміджевої привабливості даного виду професійної діяльності й т. п.

Дотримання принципу екстремальності обумовлює зростання показника  $A$  до його максимально можливого значення  $A_{extr}$ , то ж

$$\Delta A_{extr}(I) = A_{extr}(I) - A_0. \quad (3)$$

У кожному конкретному застосуванні інформації  $I$  спосіб її "споживання" буде різним: разове використання інформації  $I$  у задачах прийняття рішення для вибору найкращого рішення з множини можливих; розподілене у часі поточне використання інформації для налаштування параметрів виробничих процесів тощо. Очевидно, що найбільш прийнятна форма виміру значень  $V$ ,  $A$ ,  $d$  – грошова, хоча на практиці використовуються умовні одиниці, бали та інше. Крім того у більшості випадків величини  $V$ ,  $A$ ,  $d$  носять детермінований характер і їх значення можуть бути точно обчислені за існуючими нормативами та тарифами (виключення становить задача прийняття рішення на множині варіантів з відомою інформацією про розподіл ймовірностей їх реалізацій). Зазначимо, що наведений спосіб обчислення рівня корисності інформації, як і більшість традиційних методів та підходів до визначення цінності інформації, базуються на парадигмі позитивності наслідків залучення інформації до оптимізації певних видів робіт (прийняття рішень, розв'язання задач, виконання завдань). Однак в задачах захисту інформації (ЗІ) ця парадигма не спрацьовує, бо виникає відсутня раніше потреба в чіткому визначенні того суб'єкта інформаційних відносин (власника / споживача інформації чи зловмисника), для якого в цій ситуації визначається цінність інформації. Наприклад, для зловмисника несанкціонований доступ до конфіденційної інформації  $I$ , легітимне право на ознайомлення з якою у нього відсутнє, в більшості випадків стимулюється перспективою отримання певного прибутку, пов'язаного саме з використанням цієї конфіденційної інформації у своїх інтересах. Тому для зловмисника корисність цієї інформації  $I$  очевидна. Що стосується власника / споживача інформації  $I$ , то тут ситуація має подвійний характер. По-перше, ця інформація може бути корисна в традиційному сенсі. По-друге, компрометація інформації  $I$  здатна призвести до збитків, обсяг яких значне перевищуватиме корисність, ви-

значену за співвідношенням (1). Це є достатнім мотивуванням необхідності захисту цієї інформації, отже в певному розумінні визначає цінність інформації  $I$ . Тому питання визначення цінності інформації, яка підлягає захисту, потребує додаткового розгляду.

Як відомо [7,8], споживчі якості інформації в повному обсязі гарантуються за умов забезпечення трьох властивостей інформації:

- доступності (можливості отримання санкціонованим користувачем потрібної йому інформації не пізніше заданого (малого) проміжку часу, захищеність її від несанкціонованого блокування);
- цілісності (захищеність інформації від несанкціонованого знищення, модифікації);
- конфіденційності (неможливість отримання інформації неавторизованим користувачем, захищеність від несанкціонованого ознайомлення).

Розглянемо дещо детальніше ситуації, що виникають в разі реалізації загроз щодо трьох наведених властивостей інформації. Так, у випадку разового використання інформації  $I$  в задачі прийняття рішення, знищення або блокування цієї інформації обумовлює неможливість зростання показника  $A$ , тобто  $\Delta A = 0$ . Це означає, що споживач інформації задарма витратив гроші  $d(I)$  на підготовку та обробку вчасно невикористаної інформації  $I$ . Додавши сюди втрачену вигоду, максимальний обсяг якої складає  $\Delta A_{extr}(I)$ , отримуємо граничний обсяг збитку споживача:

$$l = \Delta A_{extr}(I) + d(I) \quad (4)$$

У випадку використання поточно оновлюваної інформації, надходження якої розподілене у часі, її блокування чи знищення призведе практично до такого самого збитку, але з деяким часовим запізненням (лагом), впродовж якого збиток зростатиме від 0 до  $l$ .

У разі модифікації інформації, при невиявленні факту модифікації, збитки споживача інформації можуть сягати суттєвих значень, перевищуючи як  $\Delta A(I)$ , так і  $A(I)$ , та мають, на відміну від (4), імовірнісний характер.

Однак найбільші збитки характерні для випадку порушення конфіденційності інформації. При їх оцінюванні слід зважати на існування множини можливих сценаріїв розвитку подій, тобто ці збитки мають принципово імовірнісний характер. Крім того, в разі виявлення факту компрометації конфіденційної інформації, до загального обсягу збитків слід додати витрати на відновлювальні роботи, пов'язані з ліквідацією наслідків компрометації інформації.

Загалом структура збитків, що їх несе власник/споживач конфіденційної інформації через її втрату, має чотири складові:

$$L(I) = l_1 + l_2 + l_3 + L_{\Sigma}(I) \quad (5)$$

де  $l_1$  – витрати на створення та обробку конфіденційної інформації  $I$  (близькі або співпадають з  $d(I)$ ),

$l_2$  – втрати можливого прибутку за рахунок використання конфіденційної інформації  $I$  (у ряді випадків співпадають з  $\Delta A(I)$ ),

$l_3$  – витрати на створення та експлуатації СЗІ,

$L_{\Sigma}(I)$  – інтегральна оцінка збитку, що є наслідком можливих результатів розвитку ряду негативних для власника/споживача сценаріїв подій, обумовлених втратою конфіденційної інформації.

За своїм характером  $l_1 - l_3$  – детерміновані величини, значення яких для діючої виробничої системи мають бути достеменно відомі. Складова  $L_{\Sigma}(I)$  – імовірнісна величина, яка для свого обчислення вимагає знання пар  $\langle p_j, L_j \rangle$  – ймовірностей розвитку кожного з можливих сценаріїв та результуючих збитків за кожним з них. Зважаючи на те, що в разі недосконалої СЗІ власник конфіденційної інформації  $I$  може понести максимальний збиток в розмірі  $L(I)$ , саме ця величина приймається у якості цінності  $V(I)$  конфіденційної інформації.

В семантичному розумінні найбільш адекватною реальній економічній ситуації, що настає після здійснення загрози, буде структура, яка включає такі три складові:

- втрачена цінність;
- збитки, обумовлені модифікацією чи розголошенням конфіденційної інформації;
- витрати на отримання та зберігання інформації.

Відповідно до викладеного вище, остання складова включає в себе витрати  $l_1$ ,  $l_3$ .

Доцільно більш детально розкрити зміст двох перших складових. Зокрема, обраховуючи втрачену цінність, зважатимемо на такі часткові показники:

а) корисність інформації як інформаційної складової забезпечення якості та ефективності певної діяльності;

б) "самостійну" корисність інформації з точки зору її необхідності для розв'язання ряду задач означеної вище діяльності.

Обчислення збитків теж базується на двох часткових показниках:

а) величині шкоди, обумовленої модифікацією чи розголошенням конфіденційної інформації;

б) витратах на проведення робіт з ліквідації наслідків розголошення конфіденційної інформації.

### **Висновки**

Проаналізовано відмінності підходу до визначення цінності конфіденційності інформації порівняно із традиційним підходом, що базується на парадигмі позитивності наслідків застосування інформації для підвищення ефективності різних видів діяльності. Запропоновано узагальнену структуру цінності конфіденційної інформації, розглянуто деякі особливості оцінювання цінності, пов'язані з процесом старіння інформації та фрагментацією її на окремі блоки.