МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

В. К. Задірака,* О. С. Олексюк, Р. П. Смоленюк,*** П. І. Штабалюк******

ФІНАНСУВАННЯ ВИТРАТ НА ЗАХИСТ ІНФОРМАЦІЇ В ЕКОНОМІЧНІЙ ДІЯЛЬНОСТІ

Швидкі темпи інформатизації діяльності людини в різних сферах, зокрема, в фінансовій, господарській, економічній, супроводжуються ще швидшими темпами зростання кількості та витонченості загроз комп'ютерним мережам. Тому перед суб'єктами господарювання, які принаймні заради власного іміджу бажають мати в Інтернеті власний сайт, а тим більше перед тими, хто розвиває електронний бізнес, постає проблема надійної протидії атакам зловмисників. Зрозуміло, що заходи, необхідні для гарантування безпеки інформації, не можуть бути безкоштовними, їх здійснення потребує певних фінансових витрат. Однак, не зважаючи на актуальність, питання визначення розмірів витрат, необхідних на захист інформації, і досі залишається мало дослідженим.

У відомих нам літературних джерелах розглядаються різні аспекти захисту інформації, — правові, організаційні, технічні, криптографічні, стеганографічні і т. п .[1] Проте питання економічної

* *завідувач відділу Інституту кібернетики ім. В. М. Глушкова НАН України, доктор фізико-математичних наук, член-кореспондент НАН України*

** *завідувач кафедри фінансів Хмельницького економічного університету, доктор економічних наук, професор*

*** *проректор з наукової роботи Хмельницького економічного університету, кандидат економічних наук*

**** *доцент кафедри фінансів Хмельницького економічного університету, кандидат фізико-математичних наук*

[1] *Андрощук Г. А., Крайнев П. П.* Экономическая безопасность предприятия: защита коммерческой тайны: Монография. — К.: Издательский дом "Ин Юре", 2000. — 400 с.; *Богуш В. М. Кудін А. М.* Інформаційна безпека "від А до Я". 3000 термінів та понять. — К.: АСК, 2001. — 380 с.; *Вербіцький О. В.* Вступ до криптології. — Львів: Вид-тво наук.-тех. л-ри, 1998. — 248 с.; Введение в криптографию / Под. общ. ред. В. В. Ященко. — 2-е изд. Испр. — М.: МЦНМО: "ЧеРо", 1999. — 272 с.; ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хеширования.; *Задірака В. К., Олексюк О. С.* Методи захисту фінансової інформації: Навчальний посібник. — Тернопіль: Збруч, 2000. — 460 с.; *Задирака В. К., Абдикаликов К. А.* Элементы современной криптологии и методы защиты банковской информации: Учебное пособие. — Алматы: Республиканский издательский кабинет Казахской академии образования им. Н. Алтынсарина, 1999. — 336 с.; *Конхейм А. Г.* Основы криптографии / Пер. с анг. — М.: Мир, 1987. — 412 с.

Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490. www.univer.km.ua

доцільності впровадження засобів захисту інформації, фінансування витрат на такі заходи поки що майже не вивчалося[2].

Метою статті є запропонувати варіант моделі визначення розмірів витрат на захист інформації, який міг би знадобитись суб'єктам господарювання для побудови чи вдосконалення власної системи безпеки інформації.

Позначимо через S розмір фінансування витрат на захист інформації певного суб'єкта господарювання, а через $b(S)$ — розмір сподіваних втрат від ризику порушення безпеки інформації. Тоді загальний сподіваний розмір втрат на безпеку інформації V можна виразити як суму витрат S та можливих втрат $b(S)$:

$$V = S + b(S). \quad (1)$$

Отже, функцію (1) можна розглядати як цільову, яку потрібно мінімізувати:

$$V(S) = S + b(S) \to \min. \quad (2)$$

Проаналізуємо задачу (2). Перше питання, яке може виникнути у керівництва суб'єкта господарювання, коли мова йде про доцільність фінансування заходів безпеки інформації — це чи не можна без таких витрат обійтися взагалі, тобто чи не може виконуватися рівність

$$S = 0 \; ? \quad (3)$$

Взагалі кажучи, постановка такого питання не позбавлена сенсу, оскільки ведення підприємницької діяльності і так супроводжується видатками на різні види безпеки, причому багато з них обов'язкові і немалі, — це видатки на протипожежну безпеку, на дотримання санітарно-гігієнічних норм і приписів, на охорону праці, виплати у соціальні фонди. Тим більше, що витрати на захист інформації не вважаються загальнообов'язковими, практично не регламентуються ні державними, ні міжнародними стандартами бухгалтерського обліку, викликає труднощі обґрунтування врахування цих витрат із метою зниження розміру прибутку як бази оподаткування.

Якщо при $S=0$ сподіваний розмір втрат від ризику порушення безпеки інформації теж нульовий, тобто

$$b(0) = 0, \quad (4)$$

тобто вважається, що інформація суб'єкта господарювання, розміщена ним у комп'ютерній мережі, може бути відкритою і розголошення її ніяк не впливає на фінансовий стан підприємства, то задача (2) мінімізації загального сподіваного розміру втрат на безпеку інформації стає тривіальною і подальший її аналіз втрачає сенс.

Тому надалі припускаємо, що при $S=0$ сподіваний розмір втрат від ризику порушення безпеки інформації приймає своє найбільше можливе відмінне від нуля значення

$$b(0) = B > 0. \quad (5)$$

На жаль, в економічній літературі відсутня єдина загальновизнана методика оцінки максимального розміру можливих втрат від порушення безпеки інформації.

Відсутність загальноприйнятої методики оцінки втрат від ризику порушення безпеки інформації частково пояснюється різноманітністю способів і видів порушень.

Серед способів загроз комп'ютерним мережам, крім загальновідомих "вірусів", тобто програм, які заражають файли комп'ютерів вкрапленням у них своїх копій, розрізняють такі способи загроз[3]:

[2] *Олексюк О. С.* Моделювання оптимізації витрат на захист систем обробки інформації від ризику їх безпеки // Ризикологія в економіці та підприємництві. — К.: КНЕУ, Академія ДПС України, 2001. — С. 300, 301; *Задірака В. К., Олексюк О. С., Штабалюк П. І.* Способи вимірювання ризику розшифрування інформації // Праці міжнародної конференції "Питання оптимізації обчислень (ПОО — XXXII)", присвяченої пам'яті академіка В. С. Михалевича. — К.: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2005. — С. 84, 85.

[3] *Олексюк О. С.* Моделювання оптимізації витрат на захист систем обробки інформації від ризику їх безпеки // Ризикологія в економіці та підприємництві. — К.: КНЕУ, Академія ДПС України, 2001. — С. 300, 301.

www.univer.km.ua Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490.

- "черв'як", тобто програма, яка розповсюджується через мережу і не залишає свої копії в пам'яті комп'ютера, останнім часом найчастіше поширюється через електронну пошту;

- "троянський кінь", тобто програма, яка виконує в доповнення до основних, проектних та документованих, додаткові, але не описані в документації дії: труднощі діагностики таких програм полягають у тому, що їх дія може проявлятися лише в певні діапазони системного часу, залишаючись законсервованими в решті системного часу;

- "жадібна програма", яка при виконанні намагається монополізувати певний ресурс комп'ютера, наприклад, пам'ять, не даючи його використовувати основним програмам;

- "збирання сміття", тобто опрацьованої інформації, яка не повністю знищена в пам'яті комп'ютера;

- "загарбник паролів", тобто програма, призначена для викрадення паролів; здебільшого його використовують для несанкціонованого доступу, що полягає в отриманні порушником доступу до об'єкта, на який у нього відсутній дозвіл відповідно до прийнятої у суб'єкта господарювання політики безпеки;

- незаконне використання привілеїв; така загроза буває здебільшого від користувачів, які мають деякий рівень прав доступу до мережі, але хочуть здобути вищий привілей із метою несанкціонованого використання певної функції засобами штатного програмного забезпечення;

- "маскарад", тобто виконання якихось функцій одним користувачем від імені іншого;

- атаки "салямі" зазнають системи, що опрацьовують грошові рахунки; у цьому випадку програміст, котрий нараховує відсотки на банківські рахунки чи акційні знижки на ціни в супермаркетах, похибки заокруглення записує на власний рахунок на нашу думку такі атаки можна розцінювати як найбільш безневинні;

- "приховані канали", тобто шляхи передачі інформації між процесами системи, які порушують системну політику безпеки;

- "злам системи", тобто зумисне проникнення в систему з несанкціонованими параметрами входу;

- "люки", тобто приховані, недокументовані точки входу в програмні модулі, інформацією про які можуть володіти розробники чи постачальники програмного забезпечення;

- "шкідливі програми", які дезорганізовують процес обробки інформації, причому інколи навіть за рахунок некоректного виконання арифметичних операцій. Ці програми можуть не лише спотворювати інформацію, а й сприяти її витоку.

В будь-якому випадку величину B краще переоцінити, ніж недооцінити, оскільки порушення безпеки інформації може спричинити тривале неправомірне використання комерційної таємниці і цим самим поставити "під загрозу саме існування підприємства"[4]. Це означає, що величина B може дорівнювати навіть ринковій ціні підприємства.

Фінансування витрат S на захист інформації повинно зменшувати розмір сподіваних втрат $b(S)$ від порушення безпеки, причому більшим значенням S відповідають менші значення $b(S)$:

$$0 < S_1 < S_2 \Rightarrow b(S_2) < b(S_1) < b(0) = B. \quad (6)$$

Формула (6) означає, що функція $b(S)$ монотонно спадна, а тому швидкість $b'(S)$ зміни сподіваних втрат від обсягу витрат від'ємна:

$$b'(S) < 0. \quad (7)$$

Припустимо, що швидкість $b'(S)$ прямо пропорційна розміру сподіваних втрат із деяким від'ємним коефіцієнтом $(-k)$,

$$k > 0, \quad (8)$$

[4] *Дерінгер А.* Коментар до Закону України "Про захист від недобросовісної конкуренції" // В кн. *Андрощук Г. О.* Конкурентне право: захист від недобросовісної конкуренції. — К.: ЗАТ "Інститут інтелектуальної власності і права", 2003. — С. 246-284.

Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490. www.univer.km.ua

тобто, виконується рівність

$$b'(S) = -kb(S). \quad (9)$$

Розв'яжемо диференціальне рівняння (9) з умовою (5):

$$b'(S) = Be^{-ks} \quad (10)$$

З урахуванням формули (10) задача мінімізації (2) набирає вигляду

$$V(S) = S + Be^{-ks} \to \min \quad (11)$$

Вираз (11) набуває мінімального значення за умови

$$V'(S) = 0, \quad (12)$$

тобто при виконанні рівності

$$1 - kBe^{-ks} = 0 \quad (13)$$

Розв'язавши рівняння (13) щодо S, отримаємо

$$S = \frac{1}{k}\ln(kB). \quad (14)$$

Для того, щоб переконатися, що вираз (14) надає цільовій функції $V(S)$ мінімальне значення, обчислимо її похідну другого порядку:

$$V''(S) = Bk^2e^{-ks}. \quad (15)$$

За умов (5) та (8) вираз (15) набуває додатніх значень для всіх дійсних аргументів S, у тому числі і при S, що виражається формулою (14),

$$Bk^2e^{-ks} > 0, \quad (16)$$

що є достатньою умовою локального мінімуму функції $V(S)$ при S за формулою (14). З урахуванням того, що критична точка (14) єдина для функції $V(S)$, то можна стверджувати, що ця точка локального мінімуму є одночасно і точкою її глобального мінімуму.

З'ясуємо тепер, за якої умови вираз (14) набуває додатних значень, тобто насправді виражає оптимальний розмір витрат на захист інформації:

$$\frac{1}{k}\ln(kB) > 0 \Rightarrow \ln(kB) > 0 \Rightarrow kB > 1 \Rightarrow k > \frac{1}{B}. \quad (17)$$

Якщо умова (17) порушується, тобто виконується нерівність

$$k \le \frac{1}{B}, \quad (18)$$

то виконується нерівність

$$\frac{1}{k}\ln(kB) \le 0. \quad (19)$$

Взаємопов'язані нерівності (18) та (19) означають, що якщо коефіцієнт пропорційності між модулем швидкості зміни втрат від порушення безпеки інформації та найочікуванішим розміром можливих втрат ($k=|b'(S)|/b(S)$) не перевищує величини, оберненої до максимально можливого розміру втрат, то фінансування витрат на безпеку інформації недоцільне. При цьому зауважимо, що чим більша величина B, тим менша обернена до неї величина $(1/B)$ і тим менша ймовірність виконання умови (18), а, отже, відсутності потреби фінансування заходів безпеки інформації.

Дослідимо тепер характер залежності оптимального розміру витрат на захист інформації S, що за умови (17) виражається формулою (14).

Як видно з формули (14), розмір витрат S залежить від параметра B за нелінійним, а саме логарифмічним законом. Ця залежність монотонно зростаюча

$$B_1 < B_2 \Rightarrow \frac{1}{k}\ln(kB_{1)}) < \frac{1}{k}\ln(kB_2),$$

оскільки частинна похідна $\frac{\partial S}{\partial B}$ додатна

$$\frac{\partial S}{\partial B} = \frac{1}{kB} > 0.$$

www.univer.km.ua Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490.

Залежність витрат S від коефіцієнта пропорційності k також нелінійна, однак має дещо складніший характер, ніж залежність від величини B.

При спрямуванні коефіцієнта пропорційності k до нижньої межі допустимих значень, яка визначається умовою (17), оптимальний розмір витрат S прямує до нуля:

$$\frac{1}{k}\ln(kB)\xrightarrow[k\to\frac{1}{B}]{}0. \quad (20)$$

Умова (17) не встановлює обмежень зверху на коефіцієнт пропорційності k, тому можна умовно припустити, що цей коефіцієнт може прямувати навіть до плюс нескінченності. Однак і в цьому випадку величина S прямує до нуля:

$$\frac{1}{k}\ln(kB)\xrightarrow[k\to+\infty]{}0. \quad (21)$$

Враховуючи додатність величини S для допустимих значень k з нескінченного інтервалу $(\frac{1}{k};+\infty)$ та прямування її до нуля при підході до меж цього діапазону, можна стверджувати, що залежність S від k не має ні монотонно зростаючого, ні монотонно спадного характеру, єдиного для всього діапазону, при фіксованих значеннях B.

Обчислимо частинну похідну $\frac{\partial S}{\partial k}$:

$$\frac{\partial S}{\partial k}=\frac{1-\ln(kB)}{k^2}. \quad (22)$$

Вираз (22) може приймати як додатні, так і від'ємні значення при різних k, що підтверджує немонотонність залежності S від k.

З'ясуємо, при якому значенні k вираз (22) перетвориться в нуль:

$$\frac{1-\ln(k\hat{a})}{k^2}=0\Rightarrow\ln(k\hat{a})=1\Rightarrow \quad (23)$$

$$k\hat{a}=e;\quad k=\frac{e}{B}$$

де $e\approx 2{,}72$ — основа натуральних логарифмів. Обчислимо частинну похідну другого порядку

$$\frac{\partial^2 s}{\partial k^2}=\frac{-k-2k(1-\ln(k\hat{a}))}{k^4}. \quad (24)$$

Підставивши у формулу (24) значення k за виразом (23), отримаємо

$$\left.\frac{\partial^2 s}{\partial k^2}\right|_{k=\frac{e}{B}}=-\left(\frac{e}{B}\right)^{-3}\le 0. \quad (25)$$

Від'ємність виразу (25) є достатньою умовою того, що значення за формулою (23) надає виразові (14) максимального значення, яке дорівнює

$$S_{max}=\frac{B}{e}\approx 0{,}37B. \quad (26)$$

Формула (26) означає, що оптимальний розмір фінансування безпеки інформації не повинен перевищувати 37 % розміру максимально можливих втрат від порушень безпеки, якщо при цьому є достатні підстави вважати, що модуль швидкості зміни втрат пропорційний до самого розміру можливих втрат, навіть при відсутності достовірної інформації про коефіцієнт пропорційності. При наявності відомостей про коефіцієнт пропорційності, якщо він відрізняється від значення за формулою (23), тобто

$$k\neq\frac{e}{B},$$

Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490. www.univer.km.ua

оптимальний розмір витрат S_{opt} буде меншим від S_{max}, що виражається формулою (26),

$$Sopt \le \frac{B}{e} . \quad (27)$$

Розглянемо тепер випадок, коли швидкість зміни втрат $b'(S)$ пропорційна не до самого розміру $b(S)$ сподіваних витрат, а до деякого її степеня з показником $v > 1$:

$$\hat{a}'(S) = -k_1 b^v(S), \quad (28)$$

де $k_1 > 0$.

При цьому вважаємо, що для рівняння (28), як і для рівняння (9), виконується умова (5).

Рівняння (28) розв'яжемо способом відокремлювання змінних:

$$\frac{db}{b^v} = -k_1 \, dS .$$

У результаті інтегрування останнього рівняння знаходимо його загальний інтеграл (розв'язок)

$$\frac{b^{-v+1}}{1-v} = -k_1 S + C , \quad (29)$$

де C — деяка поки що невизначена стала.

З рівняння (29) виразимо в явному вигляді

$$b = ((1-v)(-k_1 S + C))^{\frac{1}{1-v}} . \quad (30)$$

Підставимо в загальний розв'язок (30) умову (5):

$$((1-v)C)^{\frac{1}{1-v}} = B ,$$

звідки виразимо константу C:

$$C = \frac{B^{1-v}}{1-v} . \quad (31)$$

Підставивши константу (31) в (30), отримаємо в явному вигляді закон залежності можливих втрат b від обсягів фінансування заходів безпеки:

$$b = (B^{1-v} + (v-1)k_1 S)^{\frac{1}{1-v}} . \quad (32)$$

Додавши до втрат (32) розмір витрат S, знайдемо загальну суму V, значення якої потрібно мінімізувати:

$$V = S + (B^{1-v} + (v-1)k_1 S)^{\frac{1}{1-v}} . \quad (33)$$

Щоб знайти точки екстремуму функції (33), яка визначена для невід'ємних значень S ($S \ge 0$), обчислимо її похідну:

$$\frac{dV}{dS} = 1 - k_1 (B^{1-v} + (v-1)k_1 S)^{\frac{v}{v-1}} , \quad (34)$$

прирівняємо її до нуля:

$$1 - k_1 (B^{1-v} + (v-1)k_1 S)^{\frac{v}{1-v}} = 0 , \quad (35)$$

і розв'яжемо отримане рівняння (35) відносно S:

$$S = \frac{k_1^{\frac{v-1}{v}} - B^{1-v}}{(v-1)k_1} . \quad (36)$$

З'ясуємо, за якої умови величина S, що виражається формулою (36) додатна:

$$\frac{k_1^{\frac{v-1}{v}} - B^{1-v}}{(v-1)k_1} > 0 \Rightarrow k_1 > B^{-v} . \quad (37)$$

www.univer.km.ua Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490.

Порівнюючи умову (37) з аналогічною умовою (17) на коефіцієнт пропорційності, що розглянутий у попередньому випадку, переконуємося, що умова (37) менш обмежувальна, оскільки при $\upsilon>1$ виконується нерівність

$$B^{-\nu} < B^{-1}. \quad (38)$$

Щоб з'ясувати тип критичної точки (36), знайдемо похідну другого порядку, ще раз диференціюючи похідну (34):

$$\frac{d^2V}{dS^2} = \nu k_1^2 (B^{1-\nu} + (\nu-1)k_1 S)^{\frac{2\nu-1}{1-\nu}}. \quad (39)$$

При невід'ємних аргументах S похідна другого порядку (39) набуває лише додатних значень

$$\nu k_1^2 (B^{1-\nu} + (\nu-1)k_1 S)^{\frac{2\nu-1}{1-\nu}} > 0, \quad (40)$$

що є достатньою умовою того, що аргумент (36) надає мінімального значення цільовій функції V.

Дослідимо тепер характер залежності оптимального розміру фінансування витрат на безпеку інформації (36) від параметрів розглядуваного варіанту моделі.

Якщо коефіцієнт пропорційності k_1 прямує до нижньої межі своїх допустимих значень, тобто до $B^{-\upsilon}$, то згідно з формулою (36) S прямує до нуля:

$$S \to \frac{B^{1-\nu} - B^{1-\nu}}{(\nu-1)B^{-\nu}} = 0 \quad (41)$$

Як бачимо, властивість (41) аналогічна до властивості (20), встановленої для випадку пропорційності швидкості зміни витрат до розміру очікуваних втрат. І це попри те, що функція (14) має логарифмічно-раціональний характер залежно від коефіцієнта пропорційності k, а функція (36) має степенево-раціональний характер залежності від свого коефіцієнта пропорційності k_1. Більше того, при спрямуванні коефіцієнта пропорційності до плюс нескінченності величина S за формулою (36) теж прямує до нуля.

$$\frac{k_1^{\frac{\nu-1}{\nu}} - B^{1-\nu}}{(\nu-1)k_1} \xrightarrow[k_1 \to +\infty]{} 0, \quad (42)$$

що також аналогічно властивості (21).

Проте припущення про повну якісну аналогію залежностей величин (36) та (14) від своїх параметрів було би передчасним, хоча б з тієї причини, що розмір витрат на безпеку інформації (36) залежить від трьох параметрів (B, k_1, υ), тоді як величина (14) залежить тільки від двох параметрів B та k.

Проаналізуємо тепер залежність витрат (36) від параметра υ, якого немає у виразі (14).

Обчислимо спочатку границю, до якої прямує вираз (36) при спрямуванні параметра υ до своєї нижньої межі допустимих значень, тобто до 1:

$$\lim_{\nu \to 1} \frac{k_1^{\frac{\nu-1}{\nu}} - B^{1-\nu}}{(\nu-1)k_1}. \quad (43)$$

При безпосередній підстановці у вираз (43) значення $\upsilon=1$ переконуємося, що ця границя зводиться до невизначеності типу $\frac{0}{0}$. Тому для її обчислення скористаємося правилом Лопіталя

$$\lim_{\nu \to 1} \frac{k_1^{\frac{\nu-1}{\nu}} - B^{1-\nu}}{(\nu-1)k_1} = \lim_{\nu \to 1} \frac{\left(k_1^{\frac{\nu-1}{\nu}} - B^{1-\nu}\right)'_\nu}{\left((\nu-1)k_1\right)'_\nu} = \lim_{\nu \to 1} \frac{k_1^{1-\frac{1}{\nu}} \ln(k_1) \cdot \frac{1}{\nu^2} + B^{1-\nu} \ln B}{k_1} = \frac{\ln(k_1 B)}{k_1}. \quad (44)$$

Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490. www.univer.km.ua

За своєю структурою останній вираз у ланцюжку рівностей (44) аналогічний виразу (14), що свідчить про узгодженість даного варіанту моделі з тим, що розглядався вище.

При умовному спрямуванні параметра ν до плюс нескінченності вираз (36) прямує до нуля:

$$\frac{k_1^{\frac{\nu-1}{\nu}} - B^{1-\nu}}{(\nu-1)k_1} \xrightarrow[\nu\to+\infty]{} 0 \,. \quad (45)$$

На основі формул (44) та (45) може виникнути запитання: чи вираз (36) як функція від ν монотонно спадає на проміжку $(1;+\infty)$? Однак, як показує числовий приклад, таке припущення, взагалі кажучи, насправді хибне. Якщо $B = 1$, а $k_1 = e$, то згідно формули (44)

$$\lim_{\nu\to 1} S = \frac{1}{e} \,, \quad (46)$$

а згідно формули (36) при ν=2

$$S = \frac{e^{1/2} - 1}{e} > \frac{1}{e} \,,$$

що спростовує припущення про монотонно спадний характер залежності витрат S від параметра υ, якщо параметри B та k_1, при цьому довільні, однак фіксовані.

Проте при деяких наборах значень параметрів B та k_1 припущення про монотонно спадний характер залежності витрат S від параметра υ підтверджується. Справді, якщо взяти k_1=1, а B>1, то при $1<\nu_1<\nu_2$ виконується нерівність

$$1-\nu_1 > 1-\nu_2 \,.$$

З цієї нерівності випливає істинність нерівності

$$B^{1-\nu_1} > B^{1-\nu_2} \,.$$

З останньої нерівності випливає монотонно зростаючий характер чисельника правої частини формули (36) (при k_1=1):

$$1 - B^{1-\nu_1} < 1 - B^{1-\nu_2} \,.$$

З іншого боку, знаменник правої частини формули (36) теж монотонно зростає

$$\nu_1 - 1 < \nu_2 - 1 \,.$$

Враховуючи те, що при ν=1 і чисельник, і знаменник правої частини формули (36) перетворюється в 0, то висновок про монотонність виразу (36) можна зробити на основі порівняльного аналізу швидкостей зростання чисельника і знаменника. Знаменник зростає з постійною швидкістю, що дорівнює:

$$(\nu - 1)'_\nu = 1 \,. \quad (47)$$

При цьому швидкість зростання чисельника змінна і виражається формулою:

$$\left(1 - B^{1-\nu}\right)'_\nu = B^{1-\nu} \ln B \,. \quad (48)$$

Зокрема, при $B = e$ швидкість зростання чисельника (48) менша від швидкості зростання знаменника (47):

$$e^{1-\nu} \ln e = e^{1-\nu} < 1 \text{ при } \nu > 1 \,. \quad (49)$$

На основі порівняння швидкостей зростання (49) отримуємо висновок, що при k_1=1 та B=e витрати S за формулою (36) мають монотонно спадний характер залежності від параметра ν.

www.univer.km.ua Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490.

Повертаючись до дослідження залежності витрат S від коефіцієнта пропорційності k_1, обчислимо швидкість зміни витрат S при зміні цього параметра та фіксованих параметрах B і υ, тобто обчислимо частинну похідну $\frac{\partial S}{\partial k_1}$:

$$\frac{\partial S}{\partial k_1} = \left(\frac{k_1^{1-\frac{1}{\nu}} - B^{1-\nu}}{(\nu-1)k_1} \right)'_{k_1} = \frac{1}{\nu-1} * \left(k_1^{-\frac{1}{\nu}} - B^{1-\nu} k_1^{-1} \right)'_{k_1} = \frac{1}{\nu-1}\left(-\frac{1}{\nu} k_1^{-1-\frac{1}{\nu}} + B^{1-\nu} k_1^{-2}\right) \quad . (50)$$

Прирівняємо похідну (50) до нуля:

$$\frac{1}{\nu-1}\left(-\frac{1}{\nu} k_1^{-1-\frac{1}{\nu}} + B^{1-\nu} k_1^{-2}\right) = 0 , (51)$$

і розв'яжемо рівняння (51) відносно k_1:

$$-\frac{1}{\nu} k_1^{-1-\frac{1}{\nu}} + B^{1-\nu} k_1^{-2} = 0 \Rightarrow$$

$$-\frac{1}{\nu} k_1^{1-\frac{1}{\nu}} + B^{1-\nu} = 0 \Rightarrow$$

$$k_1^{1-\frac{1}{\nu}} = \nu B^{1-\nu} \Rightarrow k_1 = (\nu B^{1-\nu})^{\frac{\nu}{\nu-1}} \quad . (52)$$

Зокрема, при υ=2 формула (52) набуває дещо простішого вигляду

$$k_1 = \frac{4}{B^2} \quad . (53)$$

Враховуючи, що на основі формули (37) точна нижня грань коефіцієнта k_1 при υ=2 визначається квадратом величини, оберненої до максимально можливого розміру втрат,

$$\inf(k_1) = B^{-2} ,$$

переконуємося, що критична точка (53) належить області визначення функції (36), оскільки виконується нерівність:

$$\frac{4}{B^2} > \frac{1}{B^2} .$$

Отриманий висновок узагальнюється на випадок довільного значення параметра υ, оскільки виконується нерівність:

$$V^{\frac{\nu}{\nu-1}} B^{-\nu} > B^{-V} .$$

Щоби з'ясувати тип критичної точки (52), обчислимо частину похідну другого порядку $\frac{\partial^2 S}{\partial k_1^2}$:

$$\frac{\partial^2 S}{\partial k_1^2} = \frac{1}{\nu-1}\left(\frac{\nu+1}{\nu^2} k_1^{-2-\frac{1}{\nu}} - 2B^{1-2} k_1^{-3}\right), (54)$$

і підставимо в отриманий вираз (54) значення k_1 за формулою (52):

$$\left.\frac{\partial^2 S}{\partial k_1^2}\right|_{k_1 = V^{\frac{\nu}{\nu-1}} B^{-\nu}} = \frac{1}{\nu-1}\left(\frac{\nu+1}{\nu^2}\left(V^{\frac{\nu}{\nu-1}} B^{-\nu}\right)^{-2-\frac{1}{\nu}} - 2B^{1-\nu}\left(V^{\frac{\nu}{\nu-1}} B^{-\nu}\right)^{-3}\right) = \frac{1}{\nu-1} B^{2\nu+1}\left(\frac{\nu+1}{\nu^2} V^{\frac{-2\nu-1}{\nu-1}} - 2V^{\frac{-3\nu}{\nu-1}}\right) =$$

$$= \frac{1}{\nu-1} B^{2\nu+1} V^{-\frac{3\nu}{\nu-1}}\left(\frac{(\nu+1)\nu}{\nu^2} - 2\right) = \frac{1}{\nu-1} B^{2\nu+1} V^{-\frac{3\nu}{\nu-1}}\left(\frac{1}{\nu} - 1\right) \quad (55)$$

При ν>1 вираз (55) набуває лише від'ємних значень:

$$\frac{1}{\nu-1} B^{2\nu+1} V^{-\frac{3\nu}{\nu-1}}\left(\frac{1}{\nu} - 1\right) < 0 ,$$

Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490. www.univer.km.ua

а це означає, що критична точка (52) є точкою максимуму функції (36).

Саме максимальне значення S отримаємо, підставивши вираз (52) у формулу (36):

$$S_{max} = \frac{vB^{1-v} - B^{1-v}}{(v-1)(vB^{1-v})^{\frac{v}{v-1}}} = \frac{\left(B^{1-v}\right)^{\frac{1}{v-1}}}{v^{\frac{v}{v-1}}} = \frac{B}{v^{\frac{v}{v-1}}} \quad . \quad (56)$$

Зокрема, при $v=2$ максимально можливий обсяг оптимальних витрат становить чверть величини B :

$$S\max\big|_{v=2} = B/4 \quad . \quad (57)$$

Порівнюючи вираз (57) з аналогічним до нього виразом (26), отриманим у попередньому варіанті моделі, бачимо, що витрати за формулою (57) менші від витрат (26):

$$\frac{B}{4} < \frac{B}{e} \quad .$$

З'ясуємо до якої величини прямує розмір витрат (56) при спрямуванні параметра v до його нижньої межі допустимих значень, тобто до одиниці. Для цього знайдемо границю:

$$\lim_{v\to 1} \frac{B}{v^{\frac{v}{v-1}}} \quad . \quad (57)$$

При безпосередній постановці значення $v=1$ у вираз (57) переконуємося, що ця границя зводиться до невизначеності виду

$$B \cdot 1^{-\infty}$$

Тому для обчислення границі (57) зробимо спочатку заміну:

$$v - 1 = x \quad . \quad (58)$$

Підставляючи формулу (58) у границю (57) отримуємо:

$$\lim_{v\to 1} \frac{B}{v^{\frac{v}{v-1}}} = \lim_{x\to 0} \frac{B}{(1+x)^{\frac{1+x}{x}}} = \lim_{x\to 0} \frac{B}{(1+x)^{\frac{1}{x}+1}} = \lim_{x\to 0} \frac{B}{(1+x)^{\frac{1}{x}} \cdot (1+x)} = \lim_{x\to 0} \frac{B}{(1+x)^{\frac{1}{x}}} \cdot \lim_{x\to 0} \frac{1}{x+1} = \lim_{x\to 0} \frac{B}{(x+1)^{1/x}} \quad (59)$$

Зробивши ще одну заміну $x = \frac{1}{n}$ отримаємо:

$$\lim_{x\to 0} \frac{B}{(x+1)^{1/x}} = \lim_{n\to\infty} \frac{B}{(1+\frac{1}{n})^n} = \frac{B}{\lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n} \quad . \quad (60)$$

Знаменник в останньому виразі подвійної рівності (60) є другою чудовою границею, яка, як відомо, дорівнює числу e — основі натуральних логарифмів:

$$\lim_{n\to\infty}(1+\frac{1}{n})^n = e \quad .$$

З урахуванням цього факту отримуємо:

$$\lim_{v\to 1} \frac{B}{v^{\frac{v}{v-1}}} = \frac{B}{e} \quad . \quad (61)$$

Порівнюючи формулу (61) з формулою (21) бачимо, що їх праві частини рівні між собою, що додатково підтверджує узгодженість розглядуваного варіанту моделі з проаналізованим вище.

При прямуванні параметра v до плюс нескінченності вираз (56), як і вираз (36), прямує до нуля:

$$\frac{B}{v^{\frac{v}{v-1}}} \xrightarrow[v\to+\infty]{} 0. \quad (62)$$

www.univer.km.ua Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490.

Принагідно відзначимо ще одну спільну властивість виразів (56) та (26) — це лінійна, а точніше прямо пропорційна залежність від параметра B. І це при тому, що вираз (56) є наслідком з виразу (36), який від параметра B залежить нелінійно, так само як вираз (36), що є наслідком виразу (14), який також нелінійно залежить від величини B.

Щодо залежності верхньої межі витрат (56) від параметра v, то пам'ятаючи про можливість відсутності монотонно спадного характеру витрат (36) від цього параметру, виникає питання, чи не може і тут мати місце подібна ситуація, тобто чи не може верхня межа витрат при незмінних значеннях максимально можливих розмірах втрат B збільшитися при збільшенні параметра , нехай лише і в окремих невеликих діапазонах зміни цього параметра, і чи не може, зокрема, внаслідок цього верхня межа витрат перевищити 37% від можливих максимальних витрат, тобто верхньої межі, отриманої за формулою (26) при v=1.

Однак насправді вираз (56), як функція v, є монотонно спадним, в чому можна переконатися шляхом логарифмічного диференціювання:

$$\ln S_{max} = \ln B - \frac{v}{} \ln v$$

$$\frac{(S_{max})'_v}{S_{max}} = \frac{1}{(v-1)^2}(\ln v - v + 1) < 0 \text{ при } v>1 \ ,$$

що і доводить монотонно спадний характер величини (56) від параметра v, тобто

$$v_1 < v_2 \Rightarrow \frac{B}{v_2^{\frac{v_2}{v_2-1}}} < \frac{B}{v_1^{\frac{v_1}{v_1-1}}}.$$

На основі аналітичного виразу (56) наведемо таблицю 1 залежності максимального розміру доцільних витрат від параметра v у відсотках від максимуму можливих втрат, прийнятого за 100%.

Таблиця 1.

Залежність максимально доцільного відсотку витрат на безпеку інформації від показника степеня v можливих втрат, за умови $|b'|=k_1 b^v$.

Показник V	Відсоток витрат S/ B (%)	Показник V	Відсоток витрат S/ B (%)
1,044	36	2,286	23
1,103	35	2,45	22
1,166	34	2,632	21
1,234	33	2,833	20
1,306	32	3,057	19
1,384	31	3,309	18
1,467	30	3,592	17
1,558	29	3,913	16
1,665	28	4,279	15
1,761	27	5,771	12
1,875	26	7,293	10
2	25	16,72	5
2,136	24	45,91	2

На завершення цього фрагменту дослідження зауважимо, що задача гарантування безпеки інформації багатоаспектна, багатогранна, складається з комплексу окремих підзадач. Неврахування однієї з граней, чи недофінансування однієї з підзадач може звести нанівець всю роботу з вирішення решти підзадач.

Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490. www.univer.km.ua

Як ілюстрацію наведемо приклад, що стосується гарантій безпеки електронного підпису[5]:

"Захищені пристрої для створення підписів повинні за допомогою технологічних та процедурних засобів забезпечити таке:

- дані щодо створення підпису, що використовуються для проставлення підпису, можуть з'явитись практично лише один раз і що секретність цих даних забезпечена належним чином;

- дані щодо створення підпису, що використовується для проставлення підпису, з достатньою певністю не можуть бути здобуті повторно, а підпис є захищеним від підробки з використанням сучасної технології;

- дані щодо створення підпису, що використовується для проставлення підпису, повинні бути надійно захищені законним власником підпису від використання іншими особами;

Захищені пристрої для створення підписів не повинні змінювати дані, які вимагають підпису, або перешкоджати представленню цих даних власникові підпису до процесу проставлення підпису".

Як видно з процитованих вище вимог до безпеки електронного підпису, задача гарантування його безпеки складається принаймні з чотирьох підзадач, вирішення кожної з яких вимагає фінансування. Однак питання, як оптимально розподілити бюджет всієї задачі на окремі підзадачі, залишається поки що недослідженим.

www.univer.km.ua Університетські наукові записки, 2006, № 3-4 (19-20), с. 479-490.

[5] *Davydov M. V.* Organization of the application of the electronic signature system in banking // Актуальні проблеми економіки. — 2004. — № 8. — С. 183-190.