

УДК 519.86

**В. В. Волкова, М. Р. Васютенко***Дніпропетровський національний університет імені Олеся Гончара, Україна***ВИЗНАЧЕННЯ ВИТРАТ НА ЗАБЕЗПЕЧЕННЯ  
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА  
НА ЗАСАДАХ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ**

Досліджується процес визначення оптимального обсягу грошових коштів та його розподіл між окремими напрямками захисту інформації підприємства на підставі застосування економіко-математичних моделей.

*Ключові слова:* інформаційна безпека підприємства, інформаційні загрози, напрями захисту інформації, оптимальний обсяг витрат, математичне моделювання.

Исследуется процесс определения оптимального объема денежных средств и его распределение по основным направлениям защиты информации предприятия на основе применения экономико-математических моделей.

*Ключевые слова:* информационная безопасность предприятия, информационные угрозы, направления защиты информации, оптимальный объем затрат, математическое моделирование.

**The article studies the process of determining the optimal volume of funds and their distribution between different areas of the enterprise information security through the use of mathematical economic models.**

*Keywords:* enterprise information security, information threats, areas of information protection, the optimal amount of expenditures, mathematical modeling.

У сучасних умовах інформація набуває все більшої ваги для функціонування та розвитку суб'єктів ринкової економіки. Вона є одним із найважливіших ресурсів у розвитку й виступає у вигляді нових ідей і технологій, комерційних та інноваційних проєктів, аналітичних розробок, виробничих планів та звітності, тому поряд із завданнями ефективної обробки й передачі інформації, забезпечення надійності захисту інформаційних ресурсів – однією з головних задач сучасного бізнесу є управління інформаційними ризиками [1].

Серйозна увага до питань захисту інформаційних систем спричинює проблеми оцінки рівня безпеки корпоративних інформаційних систем підприємств та організацій, визначення величини грошових коштів, які потрібно виділити на вирішення проблем інформаційної безпеки, розподілу грошових коштів між засобами, які забезпечують захист інформації, зниження інформаційних ризиків. Найчастіше зазначені проблеми розв'язують на інтуїтивному рівні, без обґрунтування фінансової доцільності рішень. Адже керівництво підприємств не завжди оцінює важливість цього питання та має інформацію про співвідношення витрат на забезпечення інформаційної безпеки та збитків від втрати інформації. Іноді на інформаційній безпеці економлять, хоч це найчастіше призводить до істотних фінансових і моральних втрат, які можуть бути причиною краху. Однією з проблем інформаційної безпеки підприємства є її кількісна оцінка, а також необхідність обґрунтування вартості створення корпоративної системи захисту інформації.

Про забезпечення інформаційної безпеки, проблему управління інформаційними ризиками йдеться в багатьох роботах зарубіжних та вітчизняних учених. Так, дослідження В. В. Домарева розкривають проблеми створення комплексних систем захисту інформації. У роботах [2; 3] він пропонує системний підхід до їхнього вирішення. У роботі [4] розглянуто поняття інформаційної безпеки бізнесу, моделі та практику розвитку служб інформаційної безпеки, технології аналізу інформаційного ризику, аудит інформаційної безпеки, проаналізовано захищеність інформаційних систем, основні поняття й методики, використовувані при аналізі інформаційних ризиків.

Основи управління захистом інформації, моделі та розв'язок відповідних задач щодо створення системи захисту інформації на підприємстві розглядають у своїх роботах В. А. Герасименко [5], А. М. Івашко, П. Д. Зегжда [6]. Проблеми забезпечення інформаційної безпеки корпоративних інформаційних систем дедалі більше приділяють уваги [1]. Це пов'язано з тим, що витрати на попередження інформаційних загроз є набагато меншими, ніж витрати на усунення їхніх наслідків.

Позитивно оцінюючи результати зазначених досліджень, необхідно підкреслити, що в науковій літературі недостатньо розроблено визначення оптимального обсягу грошових коштів та його розподіл між окремими напрямками захисту інформації організації на підставі застосування математичних моделей та методів, а також їх практичної реалізації.

Метою роботи є визначення витрат на забезпечення інформаційної безпеки підприємства на підставі математичного моделювання.

Функціонування будь-якої організації, і підприємства зокрема, супроводжується обробкою та переміщенням великої кількості інформації між певними структурними підрозділами, кожен з яких розв'язує відповідні завдання. Інформаційна система підприємства складається з комплексу апаратних та програмних засобів, які дозволяють автоматизувати процеси його діяльності, тобто кожен з відділів має у своєму розпорядженні певну кількість засобів обчислювальної техніки, за допомогою яких наявну на підприємстві в електронному вигляді інформацію зберігають, передають та обробляють. Зв'язок між підрозділами забезпечується за допомогою корпоративної мережі. Інформацію в паперовій формі зберігають у відповідних відділах структури підприємства. Як правило, функціонування корпоративної мережі та вихід в Інтернет забезпечує багатоцільовий сервер.

Пропонуємо такі етапи процесу оцінки витрат, необхідних для створення системи захисту інформації на підприємстві та здійснення їхнього оптимального розподілу між окремими заходами:

1. Проведення інвентаризації та класифікації інформаційних об'єктів підприємства для об'єднання їх в інформаційні блоки з метою зниження трудомісткості подальших обчислень. До одного блоку зараховують інформаційні об'єкти, схожі за видом носія, структурою, технологією обробки, тематикою, видом даних.

2. Складання переліку інформаційних загроз, актуальних для підприємства. Існує три основні загрози для інформації: загроза цілісності, загроза конфіденційності, загроза доступності. Оскільки рівень інформаційної загрози безпосередньо залежить від заходів, направлених на її попередження, та обсягу виділених на ці заходи грошових коштів, то необхідно визначити перелік контрзаходів, що можуть бути застосовані для захисту інформації. Кожному заходу щодо захисту інформації ставиться у відповідність стаття фінансування.

3. Визначення виду функції залежності ймовірності реалізації інформаційної загрози від обсягу грошових коштів, виділених на заходи щодо її попередження.

4. Визначення величин втрат, якщо буде реалізовано кожен з інформаційних загроз, для відповідного інформаційного блоку. Значення втрат для інформаційного блоку в цілому дорівнює сумі втрат за кожним з елементів, інформаційних об'єктів цього блоку.

5. Визначення середньої частоти проривів системи захисту інформації за певний період, тобто кількість випадків, коли відповідна інформаційна загроза може бути реалізована.

6. Знаходження економічно обґрунтованої кількості грошових коштів, необхідних для забезпечення інформаційної безпеки підприємства.

7. Здійснення оптимального розподілу грошових коштів між окремими напрямками захисту інформації.

Розгляньмо зміст кожного з етапів процесу визначення витрат на забезпечення інформаційної безпеки виробничого підприємства.

Етап 1. Оскільки на підприємствах циркулює інформація у паперовій та електронній формах, створення системи інформаційної безпеки направлене на зниження ризику втрати конфіденційності, цілісності, доступності інформації саме в цих формах. З точки зору змісту можна виділити такі основні типи інформаційних об'єктів, що мають місце на підприємстві: база персональних даних співробітників та трудові книжки; накази по підприємству; відомості нарахування та виплати заробітної плати; касові звіти; первісна бухгалтерська документація; бухгалтерські звіти (податкові та фінансові); оборотні відомості рахунків бухгалтерського обліку; журнали-ордера рахунків бухгалтерського обліку; оборотні баланси; статутні документи підприємства; договори з постачальниками, покупцями, книги реєстрації договорів; інформаційна база контрагентів; журнал реєстрації вихідної і вхідної кореспонденції; фінансовий план розвитку підприємства; технологічні карти; технічні умови та ін.

Оскільки захист інформації відбувається на рівні приміщення (середовища), де вона обробляється, будемо розглядати розподіл інформації за типами приміщень (відділів підприємства). Інформація в електронному вигляді зберігається, передається та обробляється на засобах обчислювальної техніки, тому інформацію також будемо розглядати з урахуванням її розміщення на комп'ютерах підприємства, які, у свою чергу, групуються відповідно до фізичного розташування. Інформаційні об'єкти об'єднують у блоки на основі місця обробки інформації та розташування. Наприклад, можна сформувати такі інформаційні блоки: Блок 1. Приміщення, де розташований сервер підприємства. Блок 2. Кабінет директора. Комп'ютер директора підприємства. Блок 3. Відділ бухгалтерії. Комп'ютери робітників відділу бухгалтерії та ін.

Етап 2. До переліку основних типів інформаційних загроз, що є актуальними для підприємства, можна віднести: впровадження шкідливого програмного забезпечення на робочі станції; впровадження шкідливого програмного забезпечення на сервер підприємства; збій програмного забезпечення на робочих станціях та на сервері підприємства внаслідок перепаду напруги в мережі; несанкціоноване копіювання конфіденційної інформації на зовнішні носії; несанкціонована передача конфіденційної інформації на зовнішні сервери Інтернету; загроза несанкціонованого доступу до конфіденційної інформації, що знаходиться на комп'ютерах технологічного відділу та на комп'ютері директора підприємства; зовнішні загрози корпоративній мережі підприємства; втрата, витік, викрадення документів підприємства у паперовій формі та ін.

До контрзаходів захисту інформації, які можуть бути використані для створення системи інформаційної безпеки на підприємстві, можна віднести встановлення антивірусного програмного забезпечення на робочі станції та на сервер підприємства; встановлення антивірусного програмного забезпечення захисту від перепадів напруги у мережі, шляхом придбання мережних фільтрів та джерел безперебійного живлення (UPS) для робочих станцій та для сервера підприємства; встановлення програми, що попереджує витік конфіденційної інформації шляхом несанкціонованого копіювання її на зовнішні носії; введення обмежень на користування Інтернет-ресурсами; встановлення апаратно-програмного засобу шифрування інформації для її захисту в технологічному відділі; встановлення програми захисту корпоративної мережі підприємства від несанкціонованого доступу; витрати на обладнання архіву для зберігання документів підприємства в паперовій формі та ін.

Кожний з запропонованих вище заходів захисту інформації відповідає статті фінансування інформаційної безпеки.

Етап 3. Необхідно оцінити ймовірність  $g_j(x_j)$  реалізації  $j$ -ї інформаційної загрози ( $j = 1, n$ ) для кожної з  $n$  визначених інформаційних загроз залежно від обсягу виділених грошових коштів  $x_j$  на заходи із попередження її реалізації. Ймовірність визначається в межах однієї небезпечної події. Інформацію про ймовірності реалізації загроз оцінюють експерти шляхом анкетування, оскільки подібна статистична інформація на підприємстві, як правило, відсутня. Оцінки експертів збираються у якісному вигляді. Якісні показники формалізують за допомогою теорії нечіткості.

На підставі проведеного аналізу пропонується такий вигляд функції залежності ймовірності реалізації інформаційної загрози від обсягу виділених грошових коштів:  $g(x) = ae^{-\beta x} + \gamma$ . Кожний параметр цієї функції має певне смислове навантаження. Параметр  $\gamma$  функції показує мінімальну ймовірність реалізації інформаційної загрози, до якої прагне функція  $g(x)$  при збільшенні обсягу виділених грошових засобів на заходи, що попереджують інформаційні загрози. Параметр  $\beta$  характеризує швидкість зниження ймовірності реалізації інформаційної загрози при збільшенні асигнувань на заходи з її попередження. Параметр  $\alpha$  є масштабним і обирається так, щоб значення функції  $g(0) = \alpha + \gamma$  відповідало ймовірності реалізації загрози у випадку, коли гроші на захист інформації не виділяють. При цьому повинні бути виконані умови:  $\alpha, \beta, \gamma \geq 0, \alpha + \gamma \leq 1$ .

Зауважимо, що параметри функції будуть різними для кожної інформаційної загрози і можуть бути визначені так. Параметр  $\gamma$  визначає експерт у запропонованій йому анкеті, оцінивши значення ймовірності реалізації інформаційної загрози при 100 % рівні фінансування. Параметр  $\alpha$  визначається як різниця між експертною оцінкою ймовірності реалізації загрози у випадку, коли гроші на інформаційну безпеку не виділяють, та значенням параметру  $\gamma$ . Параметр  $\beta$  оцінюють за допомогою методу найменших квадратів.

Етап 4. Велику увагу необхідно приділити оцінюванню втрат підприємства  $A_{ij}$  для кожного  $i$ -го інформаційного блоку ( $i = 1, m$ ) від реалізації кожної  $j$ -ї інформаційної загрози ( $j = 1, n$ ). Будемо вважати, що загрози реалізуються незалежно одна від одної.

Наприклад, оцінку втрат від упровадження шкідливого програмного забезпечення на комп'ютери у відділі бухгалтерії, тобто інформаційний блок 1 – загроза 1, можна знайти у вигляді суми:

$$A_{11} = L_{dt} + L_r + L_f,$$

де  $L_{dt}$  – втрати, пов'язані з простоем відділу бухгалтерії;

$L_r$  – витрати на відновлення втрачених даних;

$L_f$  – витрати на виплату штрафних санкцій за несвоєчасне подання звітності і сплати податків та зборів.

Суму втрат, пов'язаних із простоем відділу, розраховують за формулою:

$$L_{dt} = \frac{\sum_{i=1}^N S_i}{T} \cdot t_d,$$

де  $S_i$  – заробітна плата на місяць робітника відділу;

$N$  – кількість співробітників відділу;

$t_d$  – час простою відділу бухгалтерії;

$T$  – кількість робочих годин відділу на місяць.

Етап 5. Зазначимо, що ймовірність реалізації кожної інформаційної загрози оцінювалася в межах однієї небезпечної події. Оскільки необхідно оцінити значення інформаційного ризику за певний проміжок часу (рік), то потрібна інформація

про середню частоту атак  $\lambda_j$  за цей період, тобто математичне сподівання кількості небезпечних подій у межах  $j$ -ї інформаційної загрози ( $j = 1, n$ ). Величини  $\lambda_j$  визначають також на основі експертних оцінок.

Етап 6. Визначення оптимального обсягу грошових коштів, необхідного для мінімізації втрат від реалізації інформаційних загроз та витрат на заходи, направлені на попередження інформаційних загроз, здійснюється на основі наступної моделі оптимізації [7, с. 105]:

$$\sum_{j=1}^n (g_j(x_j) \cdot \lambda_j \cdot \sum_{i=1}^m A_{ij} + x_j) \rightarrow \min, \quad (1)$$

$$x_j \geq 0. \quad (2)$$

Складовою цільової функції (1) є інформаційний ризик  $\sum_{j=1}^n (g_j(x_j) \cdot \lambda_j \cdot \sum_{i=1}^m A_{ij})$

за умови, що значення втрат для інформаційного блоку в цілому дорівнює сумі втрат по кожному з елементів інформаційних об'єктів цього блоку. Інформаційні блоки не перетинаються один з одним, тому загальний обсяг втрат  $A_j$  для інформаційної системи від реалізації  $j$ -ї інформаційної загрози буде дорівнювати сумі втрат по конкретним інформаційним блокам  $i$ , у яких ця загроза може бути реалізована. Зауважимо, що втрати від реалізації  $j$ -ї інформаційної загрози будуть різними для кожного  $i$ -го інформаційного блоку. Тому величина втрат від реалізації кожної  $j$ -ї інформаційної загрози в рамках однієї небезпечної події

розрахована як сума втрат за кожним інформаційним блоком, тобто  $A_j = \sum_{i=1}^m A_{ij}$ .

Оскільки треба оцінити значення інформаційного ризику за певний період (рік), то необхідно врахувати середню частоту проривів системи захисту інформації за цей період, тобто кількість випадків  $\lambda_j$ , коли  $j$ -а інформаційна загроза може бути реалізована. Другою складовою цільової функції (1) є сума витрат  $x_j$  на проведення заходів захисту інформації від усіх видів інформаційних загроз.

Розв'язок задачі (1–2) дозволяє знайти оптимальний обсяг фінансування, яке доцільно виділити на інформаційну безпеку підприємства  $\sum_{j=1}^n x_j = D$ .

Етап 7. Оптимальний розподіл грошових коштів між окремими напрямками захисту інформації здійснюють на основі такої моделі оптимізації:

$$\sum_{j=1}^n (g_j(x_j) \cdot \lambda_j \cdot \sum_{i=1}^m A_{ij} + x_j) \rightarrow \min, \quad (3)$$

$$\sum_{j=1}^n x_j \leq D, \quad (4)$$

$$x_j \geq 0.$$

Розв'язок задачі (3–4) дозволяє знайти оптимальний розподіл грошових коштів між статтями фінансування, який забезпечує мінімальний рівень інформаційного ризику та витрат на проведення заходів захисту інформації, при зазначених обмеженнях на загальний обсяг фінансування інформаційної безпеки. Розрахунки в межах цієї задачі також дають змогу визначити очікувану величину грошових втрат при реалізації інформаційних загроз.

**Висновки.**

Проведені дослідження показали, що, незважаючи на різноманітність специфіки підприємств, існує єдність у підході до визначення витрат на створення системи захисту інформації. Тому в межах нашого дослідження класифіковано інформаційні об'єкти, складено перелік інформаційних загроз, що можуть бути актуальними для підприємств, розроблено перелік контрзаходів, необхідних для попередження реалізації визначених інформаційних загроз. За допомогою методу експертних оцінок, теорії нечіткості та регресійного аналізу виведено функцію залежності ймовірності реалізації інформаційної загрози від обсягу грошових коштів, направлених на заходи щодо їх попередження.

Визначення на основі моделі оптимізації (1–2) економічно обґрунтованого обсягу коштів, що доцільно виділити на інформаційну безпеку підприємства, спрощує процес прийняття рішень керівництвом підприємства. Розв'язок наступної задачі (3–4) оптимального розподілу коштів між окремими напрямками захисту інформації дозволяє підприємству забезпечити мінімально можливий у межах виділеної суми рівень інформаційного ризику та витрат на проведення заходів захисту інформації.

Апробація запропонованого підходу щодо визначення витрат на створення для підприємства системи захисту інформації дозволяє, складаючи порівняно невеликі витрати на заходи забезпечення інформаційної безпеки, значно зменшити рівень інформаційного ризику і, як наслідок, очікувані втрати від реалізації інформаційних загроз. Результати дослідження, подані в роботі, можуть бути застосовані у практичній діяльності зі створення системи захисту інформації на будь-якому підприємстві.

**Бібліографічні посилання**

1. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах» від 29 березня 2006 р. // Офіційний вісник України. – 2006. – № 13. – С. 878.
2. **Домарев В. В.** Безопасность информационных технологий. Системный подход / В. В. Домарев. – К. : ТИД Диа Софт, 2004. – 992 с.
3. **Домарев В. В.** Моделирование процессов создания и оценки эффективности систем защиты информации [Електронний ресурс] / В. В. Домарев // Режим доступу : [http://www.citforum.ru/sekurity/articles/model\\_proc](http://www.citforum.ru/sekurity/articles/model_proc)
4. **Петренко С. А.** Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Компания АйТи, 2005. – 278 с.
5. **Герасименко В. А.** Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 2000. – 537 с.
6. **Зегжда Д. П.** Как построить защищенную информационную систему / Д. П. Зегжда, А. М. Ивашко. – СПб. : Мир и семья, 2009. – 249 с.
7. **Немиткина В. В.** Применение методов оптимизации при анализе и управлении информационными рисками / В. В. Немиткина // Экономика и математические методы. – 2008. – № 2. – С. 105.

*Надійшла до редколегії 15.01.2014*