УДК 004.056

*Д. О. Сікорський,*
*аспірант, Київський національний університет імені Тараса Шевченка, м. Київ*

# МЕТОДИКА ВИБОРУ ЗАСОБІВ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

*D. O. Sikorkyi,*
*PhD-student, Taras Shevchenko Kyiv National University, Kyiv*

## HOW TO CHOOSE INFORMATION RISKS MANAGEMENT TECHNIQUES

*У статті досліджена проблема удосконалення системи управління інформаційними ризиками. Запропоновано методику, яка передбачає на кожному кроці вибір одного з можливих засобів, що забезпечує отримання максимального ефекту.*

*The paper explores the problem of perfectibility of information risks management system. The methods, which provide the maximum effect, are proposed.*

***Ключові слова:*** *інформаційна безпека, інформаційний ризик, інформаційна система підприємства, система управління інформаційними ризиками.*

***Keywords:*** *information security, information risk, information system of enterprise, system of information risks management.*

**Постановка проблеми.** Використання інформаційних систем підприємства (ІСП) виникає необхідність вдосконалення системи управління інформаційними ризиками (СУІР), що обумовлене низкою причин, а саме: зростанням суми збитків від дії певного виду інформаційного ризику; появою нових інформаційних ризиків; видозміною існуючих ризиків; модернізацією ІСП; зміною масштабів та складності бізнес-процесів підприємства; змінами в суміжних чи інших складових інформаційної системи; природними явищами; появою нових нормативних документів та стандартів; змінами в політичному та економічному житті суспільства.

Удосконалення системи здійснюється за рахунок зміни існуючих або впровадження нових засобів управління інформаційними ризиками, що пов’язане з певними труднощами. У процесі модернізації СУІР повинні враховуватися вимоги національних стандартів до всіх об'єктів ІСП і, особливо, до механізмів СУІР. Підприємства, на яких здійснюється робота з інформацією, що становить державну таємницю, зобов'язані виконувати вимоги відповідних нормативних актів і стандартів. Механізми управління на таких підприємствах підлягають обов'язковій сертифікації. Державна регламентація управління інформаційними ризиками проводиться на підприємствах банківської системи, підприємствах з критичними виробничими процесами, що становлять загрозу населенню та навколишньому середовищу у разі аварійних ситуацій. Навіть якщо підприємство не підпадає під дію нормативних актів про обов'язкове регулювання заходів з управління окремими інформаційними ризиками, також доцільно використовувати сертифіковані засоби управління і застосовувати механізми управління, оскільки відповідність рекомендаціям стандартів дозволяє створити збалансовану, близьку до оптимальної СУІР.

**Аналіз останніх досліджень і публікацій.** У сучасній науковій літературі, в національних і міжнародних стандартах приділяється значна увага проблемам управління ризиками, а саме вдосконалення системи управління інформаційними ризиками. Разом з тим залишається невирішеним ціла низка проблем, головна з яких – відсутність методик вибору засобів управління інформаційними ризиками, що забезпечували б системний підхід до управління інформаційною безпекою.

**Метою статті** є розроблення методики вибору засобів протидії інформаційним ризикам, яка забезпечувала б мінімальний обсяг прогнозованих загальних витрат на управління інформаційними ризиками підприємства.

**Виклад основного матеріалу.** В процесі експлуатації СУІР адаптується до нових умов функціонування шляхом введення нових механізмів управління інформаційними ризиками, заміни механізмів на нові або вдосконалення механізмів, що вже перебували у використанні. Експлуатація нових засобів захисту, як правило, вимагає зміни організаційних методів.

Рішення про необхідність внесення змін до СУІР приймається керівництвом підприємства на основі аналізу повних витрат за минулий рік експлуатації ІСП і прогнозної інформації про ризики в наступному році.

Інформаційні ризики ранжуються в порядку спадання розміру збитків внаслідок впливу ризиків, що були понесені підприємством за певний період. Аналогічний процедура виконується і для ризиків, які не були реалізовані на підприємстві, але які можуть виникнути надалі. Такі ризики характеризуються показником «небезпека ризику», який обчислюється як добуток імовірності настання ризикової події в наступному році на величину передбачуваних збитків.

Обсяг збитків розраховується на підставі аналізу статистичних даних з урахування змін в ІСП та в суміжних системах. Очікуваний збиток від більшості інформаційних ризиків допускає його вираження в грошовій формі на основі песимістичних і оптимістичних прогнозів.

Найбільшу складність представляє визначення ймовірності настання ризикової події. В [5] показано, що більшість ризикових подій не можуть бути віднесені до статистичних. Тому методи математичної статистики здебільшого є обмеженими до застосування. У цьому випадку перевагу надають експертним методам визначення ймовірності ризикових подій.

Звичайно, можна представити ризикові події як статистичні. Скрипкін К.Г зазначає, що значна частина ризикових подій не відповідає вимогам однорідності і кількісної визначеності, що не дозволяє визначати ймовірність події статистичними методами [5]. Вимогу однорідності не задовольняє значна частина інформаційних ризиків, оскільки в одній ІСП отримати достатні для статистичної обробки дані за певним ризиком неможливо через його нечисленні реалізації.

Щоб інформаційні ризики були однорідними, пропонується фіксувати не саму подію ризику, а тільки її причину. Наявність причин ризиків мало пов'язано з особливостями певної ІСП. Для підприємств одного профілю ці причини, як правило, характеризуються схожими джерелами ризиків і механізмами реалізації.

Використання статистики подій, що є причинами ризикових подій, має ще одну істотну перевагу. На відміну від статистики подій ризику статистика причин ризиків не є конфіденційною інформацією для підприємства. Адже підприємство не розкриває інформацію про те, який відсоток подій-причин ризику призвели до інформаційних ризиків. А це суттєво спрощує збір статистики і підвищує достовірність отриманих даних.

За наявності інформації про ймовірність настання події, що є причиною ризику, і характеристику певної СУІР щодо блокування цього ризику можна визначити ймовірність події ризику для даної ІСП. Наприклад, існує статистика спроб злому системи захисту від несанкціонованого доступу. Знаючи ймовірність спроби злому та ймовірність успішного подолання системи захисту від несанкціонованого доступу, ймовірність даного ризику може бути визначена як добуток цих ймовірностей.

Необхідний рівень кількісної визначеності та однорідності можуть бути досягнуті, якщо отримати статистичні дані про ризики однієї галузі господарства. Кожна галузь характеризується своїм набором інформаційних ризиків, які мають найбільший вплив на якість інформації. Так в банківській сфері основними є інформаційні ризики, що впливають на безперервність обслуговування клієнтів, отримання достовірних даних про клієнтів і партнерів, конфіденційність банківської інформації, дистанційне обслуговування клієнтів. У виробничій сфері в першу чергу необхідно запобігти інформаційним ризикам, що пов'язані з процесом отримання сировини, енергоресурсів та комплектуючих елементів, з виробництвом і збутом продукції, зі збереженням конфіденційності інформації.

Реальний збиток від інформаційного ризику, що був визначений за кілька років, доцільно порівняти з розрахунковим збитком внаслідок впливу цього ж ризику, який визначений для року, що аналізується. Це дозволить визначити точність розрахунків і, можливо, відкоригувати методику визначення величини розрахункового збитку. Отримані дані про збитки в минулому році слід відкоригувати з урахуванням тенденцій розвитку ІСП і всіх пов'язаних з нею елементів. Для цих цілей можуть бути застосовані такі методи прогнозування: екстраполяції та інтерполяції, регресії і кореляції, факторні моделі.

В роботі [4] пропонується приймати рішення про вдосконалення СУІР на основі аналізу тільки збитків від інформаційних ризиків, які понесло підприємство за підсумками року, без урахування ймовірних збитків. Вважаємо, що такий підхід неприпустимий зважаючи на стохастичний характер ризикових подій і динамічність інформаційних ризиків.

Пропонується створювати і аналізувати єдиний набір збитків, який був отриманий шляхом об'єднання обох наборів збитків від інформаційних ризиків на підставі обробки статистичних даних експлуатації і прогнозної інформації.

Повні поточні витрати приводяться до одного року експлуатації. Це означає, що витрати на придбання, створення і впровадження нового або модифікованого механізму управління інформаційними ризиками рівномірно розподіляються на всі роки передбаченої експлуатації цього механізму. Розрахункові терміни служби механізмів управління визначаються часом експлуатації відповідних елементів ІСП.

Завдання оптимізації витрат на вдосконалення СУІР полягає у визначенні такої множини засобів протидії інформаційним ризикам, яка забезпечувала б мінімальний об’єм прогнозованих загальних витрат на управління інформаційними ризиками. Вирішення цього завдання зводиться до визначення тих засобів управління, які підлягають заміні або модернізації, а також до вибору (створення) нових механізмів для введення їх в СУІР з метою отримання оптимальної системи управління інформаційними ризиками. Частковим вирішенням завдання є отримання порожньої множини механізмів, що підлягають модернізації і заміні, оскільки це свідчить про оптимальність існуючої системи.

Розглянемо розв’язання задачі управління інформаційними ризиками без застосування механізмів страхування інформаційних ризиків. Формальна постановка задачі може бути представлена в наступному вигляді.

Нехай $R=\{r_1,r_2,\ldots,r_N\}$ – множина значущих ризиків. Для кожного ризику $r_i$ визначено збиток у грошовій формі $u_{r_i}$. Тоді множина збитків має вигляд $U=\{u_{r_1},u_{r_2},\ldots,u_{r_N}\}$ у порядку спадання значення розміру збитків. Кожен збиток $u_{r_i}$ визначений за умови, що по відношенню до $i$-го ризику не застосовуються ніякі засоби управління. Визначено множину засобів управління інформаційними ризиками $M=\{m_1,m_2,\ldots,m_K\}$, елементи якої можуть використовуватися в СУІР. Кожен $k$-й засіб управління характеризується множинами параметрів $R_k$ і $E_k$, а також параметром $c_k$. Множину $R_k=(r_1,r_2,...,r_j)$ складають інформаційні ризики, яким протидіє $k$-й засіб управління інформаційними ризиками.

З допомогою множини показників $E_k=(e_{k1},e_{k2},...,e_{kN})$ оцінюється ефективність $k$-го засобу управління. Елемент множини $e_{kn}$, $(n=\overline{1,N})$ показує яку частину збитку від $n$-го інформаційного ризику буде попереджено при використанні $k$-го засобу управління. Слід зазначити, що величина $e_{kn}$ змінюється в межах $0\le e_{kn}\le 1$. Ефективність всіх засобів управління інформаційними ризиками може характеризуватися за допомогою матриці $E$:

$$E=\begin{vmatrix} e_{11} & e_{12} & \ldots & e_{1N} \\ e_{21} & e_{22} & \ldots & e_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ e_{K1} & e_{K2} & \ldots & e_{KN} \end{vmatrix}.$$

На практиці як правило, кілька засобів управління мають вплив на один ризик. Формально це означає, що в стовпцях матриці $E$ може бути декілька елементів, відмінних від нуля. Ефект від впливу декількох засобів на ризик $n$ не може визначатися як адитивний показник $\sum_{k=1}^{K} e_{kn}$, оскільки в даному випадку сумарний показник може бути рівним чи більшим за 1. При визначенні загальної ефективності зниження збитку від ризику $n$, за умови включення в СУІР всіх $K$ засобів, що розглядаються, може використовуватися мультиплікативний показник:

$$\prod_{k=1}^{K}(1-e_{kn})=(1-e_{1n})(1-e_{2n})\ldots(1-e_{Kn}). \qquad (1)$$

Цей показник характеризує загальну частину збитку від ризику $n$, яка збережеться у випадку застосування всіх $K$ засобів управління інформаційними ризиками [2].

Параметр $c_k$ характеризує витрати підприємства на придбання чи заміну, розробку, створення, а також на впровадження та експлуатацію $k$-го засобу. У випадку, коли керівництво підприємства обмежене у витратах грошових коштів на вдосконалення СУІР, показник $c_{\max}$ визначає таке обмеження.

Відомі також елементи матриці сумісності засобів управління інформаційними ризиками:

$$D=\begin{vmatrix} d_{11} & d_{12} & \ldots & d_{1K} \\ d_{21} & d_{22} & \ldots & d_{2K} \\ \ldots & \ldots & \ldots & \ldots \\ d_{K1} & d_{K2} & \ldots & d_{KK} \end{vmatrix}.$$

Значення елемента матриці $d_{ij}$ визначається з наступної умови:

$$d_{ij} = \begin{cases} 1, & якщо\ i-й\ та\ j-й\ засоби\ сумісні; \\ 0, & в\ інших\ випадках. \end{cases}$$

Несумісними вважаються засоби, які не передбачено або заборонено до спільного використання в одній системі управління інформаційними ризиками. Наприклад, не можуть використовуватися в СУІР програмні засоби, що розроблені для використання в комп'ютерних системах з різними операційними системами. Несумісними слід вважати також засоби, що виконують однакові функції, і спільне використання яких не призводить до підвищення продуктивності системи. Такі засоби побудовані, як правило, на одних і тих же принципах, з використанням подібних технологій. Наприклад, не має сенсу використовувати в одній СУІР різні системи шифрування даних, що зберігаються на зовнішніх запам'ятовуючих пристроях. У той же час використання програмних фільтрів і контроль оператором введеної інформації є сумісними механізмами, що підвищують достовірність інформації, що вводиться. Сумісні механізми можуть використовуватися спільно в різних поєднаннях для комплексної протидії ризику.

Множина засобів, що входять до складу СУІР, задається за допомогою бінарного вектора конфігурації:

$$X = (x_1, x_2, \ldots, x_K).$$

Компоненти вектора приймають такі значення:

$$x_k = \begin{cases} 1, & якщо\ k-й\ засіб\ включено\ до\ складу\ СУІР; \\ 0, & в\ інших\ випадках. \end{cases}$$

Засоби управління $x_i, x_j \in X$ сумісні, якщо виконується умова:

$$x_i x_j \le d_{ij}, i = \overline{1,K},\ j = \overline{1,K}.$$

Загальний збиток $U^0$, який очікується після введення в СУІР засобів управління, назвемо залишковим. Залишковий збиток визначається бінарним вектором конфігурації. З врахуванням введених позначень, вираз для обчислення залишкового збитку може бути представлено в наступному вигляді:

$$U^0(x_1, x_2, \ldots, x_K) = \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K} (1 - e_{kn} x_k). \qquad (2)$$

З урахуванням введених позначень та залежностей постановка задачі оптимального вибору механізмів управління інформаційними ризиками може бути представлена наступним чином.

Визначити бінарний вектор $X^* = (x_1^*, x_2^*, \ldots, x_K^*)$, що відповідає такій множині засобів управління інформаційними ризиками, які забезпечують мінімальну суму витрат на використання цих засобів та мінімальне значення залишкового збитку від всіх значущих ризиків:

$$\sum_{k=1}^{K} c_k x_k + \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K} (1 - e_{kn} x_k) \qquad (3)$$

при виконанні умов:

$$x_i x_j \le d_{ij}, i = \overline{1,K},\ j = \overline{1,K}; \qquad (4)$$

$$\sum_{k=1}^{K} c_k x_k \le c_{\max}. \qquad (5)$$

Задача визначення засобів управління інформаційними ризиками, які необхідно ввести в СУІР додатково

або для заміни існуючих, відноситься до нелінійних дискретних бінарних задач переборного типу [3]. Розв'язання таких задач здійснюється методами повного перебору, гілок і границь, динамічного програмування, евристичними методами [1, 3].

Для вирішення поставленого завдання використовується метод, який може бути віднесений до класу «жадібних» алгоритмів. Суть методу полягає у виборі на кожному кроці одного з можливих засобів, що забезпечує отримання максимального ефекту. Ефект визначається величиною зниження витрат на управління ризиками в результаті застосування наступного засобу і втраченою вигодою внаслідок відсутньої можливості використання на наступних кроках засобів, що є несумісними з включеним в систему наступним засобом. Таким чином, на кожному кроці, на відміну від класичного «жадібного» алгоритму, аналізується не тільки локальний ефект від включення в систему засобу, але й розглядаються наслідки цього кроку в подальшій роботі алгоритму. У роботі алгоритму враховуються обмеження на витрати, пов'язані із застосуванням засобів управління інформаційними ризиками.

Для формального подання алгоритму вводяться такі позначення: $h$ – номер виконаного кроку алгоритму; $X_h = (x_{h1}, x_{h2}, \ldots, x_{hK})$ – стан вектора конфігурації після $h$-го кроку алгоритму; $W^1(h)$ – множина засобів, які використовуються на $h$-ому кроці алгоритму; $S^1(h)$ – множина засобів, які ще не використовуються на $h$-ому кроці алгоритму, але сумісні із засобами множини $W^1(h)$; $\Omega^1(h)$ – множина засобів, що є несумісними з множиною $W^1(h)$, тобто підлягають виключенню з подальшого розгляду; $U_n^0(h)$ – залишкова величина збитку від $n$-го ризику після вибору засобів на перших $h$ кроках.

Таким чином, значення $x_{hk} = 1$ відповідають засобам, що вже відібрані на перших $h$ кроках алгоритму, тобто належать множині $W^1(h)$.

Нехай $m_{h+1} \in S^1(h)$ – засіб, який обирали на $h+1$-му кроці з множини $S^1(h)$. Вибір механізму $m_{h+1}$ означає, що відповідний компонент в $(x_{h1}, x_{h2}, \ldots, x_{hK})$ стає рівним одиниці. Припустимо, що обраному засобу $m_{h+1}$ у векторі $X_h$ відповідає компонент з номером $k$. Тоді величина, на яку зменшиться збиток від $n$-го ризику при виборі на кроці $h+1$ засобу $m_{h+1}$ з номером $k$, є рівною $\Delta U_n(h+1,k)$ і визначається наступним чином:

$$\Delta U_n(h+1,k) = U_n^0(h) e_{hn}. \qquad (6)$$

Залишок величини збитків від $n$-го ризику при цьому дорівнює:

$$\Delta U_n^0(h+1,k) = U_n^0(h)(1 - e_{hn}). \qquad (7)$$

Сумарне зменшення збитків від ризиків всіх видів при виборі на $h+1$-му кроці $k$-го засобу $\Delta U(h+1,k)$, дорівнює:

$$\Delta U(h+1,k) = \sum_{n=1}^{N} \Delta U_n(h+1,k) = \sum_{n=1}^{N} \Delta U_n^0(h) e_{kn} \qquad (8)$$

Втрачена можливість зниження величини збитків на наступних кроках алгоритму $\Delta U_\tau^-(h+1,k)$ обумовлена виключенням із розгляду на наступних кроках засобу $\tau \in \Omega^1(h)$, що є несумісним із засобом $k$.

Вираз для обчислення величини $\Delta U_\tau^-(h+1,k)$ має вигляд:

$$\Delta U_\tau^-(h+1,k) = \sum_{n=1}^{N} U_n^0(h)(1 - e_{kn}) e_\tau \overline{d_{k\tau}} s_{h\tau}^1, \qquad (9)$$

де $\overline{d_{k\tau}}$ – інверсне значення $d_{k\tau}$ з матриці сумісності $D$ (якщо $d_{k\tau} = 1$, то $\overline{d_{k\tau}} = 0$ і навпаки);

множник $s_{h\tau}^1 = 1$, якщо $\tau \in S^1(h)$ і $s_{h\tau}^1 = 0$ в протилежному випадку.

Присутність множника $s_{h\tau}^1$ у виразі дозволяє враховувати на кроці $h+1$ засіб $\tau$, який став несумісним тільки на кроці $h+1$ в результаті включення засобу $k$. Величина $U_n^0(h)(1-e_{kn})$ визначає залишковий збиток від $n$-го ризику після застосування засобу $k$ на кроці $h+1$.

Сумарна величина втраченої можливості зниження збитків, у випадку вибору на $h+1$-му кроці $k$-го механізму, за рахунок виключення несумісних з ним засобів, рівна:

$$\Delta U^-(h+1,k) = \sum_{\tau=1}^{K}\sum_{n=1}^{N} U_n^0(h)(1-e_{kn})e_{\tau n}\overline{d_{k\tau}}s_{h\tau}^1 . \qquad (10)$$

Для оцінювання ефекту від включення на $h+1$-му кроці $k$-го засобу управління введемо величину $Q(h+1,k)$:

$$Q(h+1,k) = \Delta U(h+1,k) - (\Delta U^-(h+1,k) + c_k) . \qquad (11)$$

Ефект від включення засобу $k$ в СУІР визначається як різниця між сумарною величиною зниження збитків за рахунок використання механізму $k$ і сумою витрат на $k$-й засіб і загальної величини збитку, на яку не може бути зменшений збиток підприємства через неможливість використання засобів, що несумісні з механізмом $k$. Зручно використовувати величину, що характеризує питомий ефект:

$$Q_y(h+1,k) = Q(h+1,k) / c_{\max} . \qquad (12)$$

Відповідно до введених позначень алгоритм складається з наступних кроків. На кожному кроці $h$ для $m \in S_1(h)$ обчислюється $Q_y(h+1,k)$ і обирається такий засіб $m^*$ з номером $k^*$, для якого питомий ефект $Q_y(h+1,k^*)$ має найбільше значення і при цьому не вичерпуються виділені засоби, тобто виконується умова (5). Якщо такого засобу немає, то робота алгоритму припиняється і в якості оптимального складу засобів приймається вектор $X^* = (x_1^*, x_2^*, \ldots, x_K^*)$.

Проведені випробування точності моделі показали, що зі збільшенням кількості змінних точність методу знижується. Це пояснюється тим, що величина $\Delta U^-(h+1,k)$ обчислюється для всіх засобів, які ще не включені до складу оптимальної підмножини засобів. При цьому враховуються і ті засоби, які не потраплять в остаточну оптимальну підмножину засобів.

Для підвищення точності алгоритму змінено порядок обчислення величини $\Delta U^-(h+1,k)$. При її обчисленні використовується величина $gl$, яку назвемо «глибина перегляду». Вона визначає максимальну кількість засобів, що використовуються при обчисленні величини $\Delta U^-(h+1,k)$. На кожному кроці визначається $gl$ засобів, які можуть стати несумісними після вибору механізму $k$. При цьому до складу засобів, характеристики яких будуть використовуватися при обчисленні величини $\Delta U^-(h+1,k)$, включаються не більше $gl$ засобів з найкращими значеннями $\Delta U(h+1,k) - c_k$. Глибина перегляду обмежує зверху кількість засобів, що підлягають аналізу. При виконанні алгоритму кількість несумісних з $k$ засобами може бути менше $gl$.

Змінна величина $gl$ залежить від кількості засобів управління $K$. Експериментально було встановлено, що найвища точність методу досягається, якщо величина $gl$ знаходиться в інтервалі $\frac{1}{4}K < gl < \frac{1}{3}K$.

Запропонований метод забезпечує час реалізації моделі менше ніж за хвилину при кількості засобів 100. При моделюванні в області застосовності методу повного перебору (до 30 засобів) максимальна відносна похибка

не перевищила 7 %, а середня відносна похибка дорівнювала 0,84 %. Максимальна відносна похибка методу не перевищує 15 % на інтервалі вихідних даних від 10 до 100 засобів.

На ринку засобів управління інформаційними ризиками часто пропонуються готові підсистеми, що включають в свій склад комплекс засобів управління. Нехай для створення СУІР може бути використано множину комплексних засобів $KZ = (kz_1, kz_2, ..., kz_L)$, а також множину окремих автономних засобів $Z = (z_1, z_2, ..., z_K)$. Частина автономних засобів може входити до складу комплексних засобів управління.

Припустимо, що ефективність автономних засобів при включенні їх до складу комплексних засобів не змінюється. Тоді завдання оптимального вибору засобів управління інформаційними ризиками, з врахуванням раніше введених позначень, може бути формально представлене наступним чином.

Визначити загальний бінарний вектор конфігурації автономних і комплексних засобів $X_0^* = (x_1^*, x_2^*, \ldots, x_K^*, x_{K+1}^*, x_{K+2}^*, ..., x_{K+L}^*)$, який забезпечує мінімум цільової функції

$$\sum_{k=1}^{K+L} c_k x_k + \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K+J} (1 - e_{kn} x_k),$$

при виконанні умов:

$$x_i x_j \le d_{ij}, \quad i = \overline{1, K+L}, \quad j = \overline{1, K+L}, \quad \sum_{k=1}^{K+L} c_k x_k \le c_{\max}.$$

Для розв'язання задачі можуть бути використані ті ж методи, що і для вирішення завдання (3–5). Обчислювальна складність алгоритмів при цьому зростає, оскільки розмірність вектора $X_0$ більше розмірності вектора $X$.

При вирішенні задачі вибору засобів може бути поставлена умова обов'язкового включення в систему засобів певного типу. Наприклад, вимога обов'язкового використання антивірусних засобів, системи розмежування доступу, програми первинної обробки даних може бути висунута за результатами аналізу можливих інформаційних ризиків.

Для вирішення завдання в такій постановці пропонується множину ризиків $M = \{m_1, m_2, \ldots, m_K\}$ представити у вигляді об'єднання двох підмножин $M = M^1 \cup M^2$. До підмножини $M^2$ віднесені засоби, які можуть не включатися в СУІР. Підмножина $M^1$ включає в себе підмножини засобів $M_1^1, M_2^1, ..., M_G^1 \subseteq M^1$, де $G$ – кількість підмножин. Підмножина $M_g^1$ складається з альтернативних засобів $m_{g1}^1, m_{g2}^1, ..., m_{gZ_g}^1 \in M_g^1$, один з яких повинен бути вибраний в обов'язковому порядку для включення в СУІР. Кожна підмножина $M_g^1$ складається із $Z_g$ засобів.

Відповідність нумерації засобів в підмножині $M^1$ та нумерації компонент в бінарному векторі $X = (x_1, x_2, \ldots, x_K)$ встановлюється наступним чином. Підмножини $M_g^1$ розміщуються у порядку зростання $g$. За таким же принципом у вигляді кортежу формується і перелік засобів всередині підмножин $M_g^1$. Відповідність індексу $k$ біля бінарної змінної $x_k$ вектора $X = (x_1, x_2, \ldots, x_K)$ та індексів в підмножині $M_g^1$ визначається наступним чином:

$$k = \begin{cases} z_g, & якщо\ g = 1; \\ \sum_{i=1}^{g-1} Z_i + z_g, & якщо\ g > 1. \end{cases}$$

З урахуванням прийнятих вище позначень і введених залежностей постановка задачі вибору засобів управління інформаційними ризиками може бути представлена наступним чином.

Визначити бінарний вектор $X^* = (x_1^*, x_2^*, \ldots, x_K^*)$, що забезпечує мінімум суми витрат на застосування засобів управління та залишкового збитку від всіх значущих ризиків:

$$\sum_{k=1}^{K} c_k x_k + \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K} (1 - e_{kn} x_k),$$

при виконанні умов:

$$x_i x_j \le d_{ij}, \quad i = \overline{1, K+L}, \quad j = \overline{1, K+L};$$

$$\forall M_g^1 \subseteq M^1 \; \exists x_k = 1 \wedge \forall x_\mu = 0, \partial e \, \mu \ne k \wedge (k = \sum_{i=1}^{g-1} Z_i + z_g \wedge \sum_{i=1}^{g-1} Z_i < \mu \le \sum_{i=1}^{g-1} Z_i + Z_g$$

$$при \; g > 1) \vee (k = z_g \wedge 0 < \mu \le Z_g \; при \; g = 1);$$

$$\sum_{k=1}^{K} c_k x_k \le c_{\max}.$$

Завдання розв’язується в два етапи. На першому етапі вибираються обов'язкові засоби з підмножини $M^1$, а на другому – з підмножини $M^2$. Перший етап вибору може бути представлений у вигляді наступної послідовності кроків.

1. Обчислюються значення ефекту $Q(k)$ для кожного засобу, що входить до кожної підмножини $M_g^1$ (відповідність індексу $k$ вектора $X^* = (x_1^*, x_2^*, \ldots, x_K^*)$ та індексів засобів з підмножини $M_g^1$ задана в постановці задачі). При обчисленні $Q(k)$ враховується сумісність із засобами всіх інших підмножин $M_g^1$ і з засобами підмножини $M^2$. Глибина перегляду складає до трьох несумісних засобів з найбільшим ефектом.

2. Вибирається засіб $m_{gz_g}^{1*}$, для якого $Q(k) = \max$.

3. Якщо вибір здійснений з усіх $G$ підмножин, то відбувається перехід до другого етапу.

4. Уточнюються значення $Q(k)$ для всіх засобів підмножин $M_g^1$ множини $M^1$, серед яких ще не обрано засіб. При цьому сумісність розглянутих засобів із засобами підмножин з вибраними засобами перевіряється тільки стосовно вже обраних засобів $m_{gz_g}^{1*}$.

На другому етапі алгоритму вибираються механізми підмножини $M^2$, які не є обов'язковими до використання в СУІР. Вибір здійснюється відповідно до методики розв’язання задачі вибору засобів управління без поділу їх на обов'язкові до включення в СУІР та необов'язкові. При цьому враховується, що на першому етапі вже вибрано по одному з альтернативних засобів з кожної підмножини $M_g^1$.

**Висновки.** В статті розроблено метод вибору засобів управління інформаційними ризиками на підґрунті модифікованого жадібного алгоритму. На відміну від класичного жадібного алгоритму, аналізується не тільки локальний ефект від включення в систему конкретного засобу, але й розглядаються наслідки цього кроку в подальшій роботі алгоритму з урахуванням сумісності засобів. Точність методу підвищена за рахунок обмеження «глибини пошуку» перспективних засобів.

**Література.**

1. Гэри М. Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон – М.: Мир, 1982. – 416 с.

2. Завгородний В.И. Управление информационными рисками предприятия / В.И. Завгородний. – М.: ИНИОН РАН, 2009. – 174 с.

3. Пападимитриу Х. Комбинаторная оптимизация / Х. Пападимитриу, К. Стайглиц. – М.: Мир, 1985. – 512

с.

4. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: АйТи-Пресс, 2004. – 384 с.

5. Скрипкин К.Г. Финансовая информатика: учебное пособие / К.Г. Скрипкин. – М.: ТЕИС, 1997. – 160 с.

**References.**

1. Gjeri, M. (1982), *Vychislitel'nye mashiny i trudnoreshaemye zadachi* [Computers and Intractability ], Mir, Moscow, USSR.

2. Zavgorodniy, V. I. (20090, *Upravlenie informatsionnymi riskami predpriiatiia* [Information Risk Management Company], INION RAN, Moscow, USSR.

3. Papadimitriu, X. (1985), *Kombinatornaja optimizacija* [Combinatorial optimization], Mir, Moscow, USSR.

4. Petrenko, S.A. and Simonov, S.V. (2004), *Upravlenie informacionnymi riskami. Jekonomicheski opravdannaja bezopasnost'* [Information Risk Management. Economically justified security], AjTi-Press, Moscow, Russia.

5. Skripkin ,K.G.(1997), *Finansovaja informatika: uchebnoe posobie* [Financial Informatics: Textbook], TEIS, Moscow, Russia.

*Стаття надійшла до редакції 20.11.2015 р.*