УДК 625.05.31

О.А. ЗАМУЛА, В.І. ЧЕРНИШ, К.І. ІВАНОВ, Б.В. ВОЛОБУЄВ

Харківський національний університет радіоелектроніки, Україна

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ КОМПАНІЙ

Розроблена модель системи управління інформаційними ризиками. В статті розглянуто приклад рішення задачі управління інформаційними ризиками без застосування страхування ризиків. Запропонована методика дозволяє знайти оптимальну множину механізмів захисту від інформаційних ризиків. Ця методика може бути покладена в основу методики оптимізації системи управління інформаційними ризиками та впроваджена в інформаційні системи компаній. Розвитком методики може служити створення ітеративного алгоритму оптимізації за участю особи, яка приймає рішення на етапах реалізації методики.

Ключові слова: *інформаційна безпека, інформаційний ризик, механізми захисту.*

Вступ та мета роботи

На сьогодні управління інформаційними ризиками (ІР) є одним з найбільш актуальних і динамічно розвиваючих напрямків стратегічного і оперативного менеджменту в галузі захисту інформації. Основне завдання управління ІР – об'єктивно ідентифікувати і оцінити найбільш значущі для бізнесу ІР компанії, а також необхідність використання засобів контролю ризиків для збільшення ефективності і рентабельності економічної діяльності компанії. Тому під терміном «управління інформаційними ризиками» зазвичай розуміється системний процес ідентифікації, контролю і зменшення ІР компаній у відповідності з певними обмеженнями української нормативної бази в галузі захисту інформації.

Вважається, що якісне управління ризиками дозволяє використовувати оптимальні за ефективністю і витратам засоби контролю ризиків і засоби захисту інформації, що адекватні поточним цілям і завданням бізнесу компанії [1].

Функціонування інформаційних систем підприємства (ІСП) пов'язане з інформаційними ризиками. Інформаційний ризик – це можливість надходження випадкової події в ІСП, що приводить до порушення її функціонування, зниження якості інформації, в результаті чого завдається шкода підприємству [2].

Метою роботи є розробка моделі та обґрунтування застосування системи управління інформаційними ризиками (СУІР).

Актуальність проблеми

Сьогодні спостерігається посилення залежності успішної бізнес-діяльності вітчизняних компаній від використовуваних організаційних заходів і технічних засобів контролю та зменшення ризику. Для ефективного управління ІР розроблені спеціальні методики, що наведені в міжнародних стандартах ISO 15408, ISO 17799 (BS7799), BSI, а також національних та регіональних стандартах відповідно [2].

У відповідності до міжнародних стандартів управління ІР будь-якої компанії передбачає таке:

1) визначення основних цілей і завдань захисту інформаційних активів компанії;

2) створення ефективної системи оцінки та управління ІР;

3) розрахунок сукупності деталізованих не лише якісних, а й кількісних оцінок ризиків;

4) застосування спеціального інструментарію оцінювання та управління ризиками.

Для зниження шкоди від ІР на підприємстві створюється система управління інформаційними ризиками (СУІР). Під СУІР розуміється єдиний комплекс правових норм, економічних та організаційних заходів, технічних, програмних і криптографічних засобів, що забезпечує мінімальні сумарні витрати на запобігання ІР та компенсацію збитків від них [2, 3]. Правові норми, економічні та організаційні заходи, технічні, програмні та криптографічні засоби об'єднані одним поняттям – система захисту від ІР [4].

У загальному випадку можна виділити наступні складові управління ризиками [4]:

1) моніторинг та оцінювання організаційних ризиків функціонування системи;

2) моніторинг та оцінювання ризиків технічних засобів;

3) прийняття рішення з управління ризиками на основі наявних оцінок;

4) проведення безпосередньої роботи з управління ризиками .

Поступово відходить у минуле підхід, коли окремі вимоги нормативних актів та окремі проблеми інформаційної безпеки вирішуються в порядку виникнення. Багато компаній сьогодні приходять до того, що система захисту інформаційних ресурсів повинна будуватися, виходячи із загальноприйнятих норм та з урахуванням напрацьованих практик. Це допомагає уникнути розбудови інфраструктури інформаційної системи (ІС) в «авральному режимі» під будь-які вимоги і знижує рівень незапланованих витрат на обслуговування системи (у тому числі і ризик витрат, пов'язаних з втратою або крадіжкою інформації).

Система управління інформаційними ризиками

Управління ризиками передбачає вживання заходів, спрямованих на зниження частоти реалізації загроз і зниження збитків від них. Залежно від отриманих показників ризиків власник інформаційних ресурсів повинен вибрати систему управління ризиками (СУІР). Існують наступні СУІР:

1) прийняття ризику: власник інформаційних ресурсів вважає, що ризик малий і не вживає ніяких заходів;

2) зниження (зменшення) ризику: власник інформації здійснює заходи щодо зниження показника ризику для інформаційних ресурсів;

3) виключення ризику: власник інформаційного ресурсу вживає заходи, які дозволяють повністю виключити ризик;

4) передача ризику третім особам: заходи, що вживаються власником з метою відшкодування можливих наслідків настання ризику (застосування страхування).

Постановка задачі дослідження

Розглянемо рішення задачі управління ІР без застосування страхування ІР. Формальна постановка задачі може бути представлена в наступному вигляді. Розглядається множина значущих ризиків $r_i \in R, i = \overline{1,N}$. Для кожного ризику r_i визначені збитки в грошовій формі U_i, очікуваний від настання і-ої ризикової події в році, на який здійснюється планування. Збитки розміщені в кортежі $U = (u_1, u_2, ..., u_N)$ в порядку убування значення збитку.

СУІР становить множину механізмів

$$M = (m_1, m_2, ..., m_K),$$

де $K = |M|$ – потужність множини механізмів захисту.

Механізми захисту — конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки [5].

Кожний j-й механізм захисту визначається наступними множинами характеристик: F_J, R_j, ρ_j, C_j. До них відноситься множина виконуваних функцій

$$F_j = (f_j^1, f_j^2, ..., f_j^{zi}),\ z_j = |F_j|,\ F_j \subseteq F,$$

де F – множина всіх функцій, виконуваних СУІР.

Механізм захисту m_j характеризується також підмножиною ІР $R_j \subseteq R$, від яких захищає даний механізм захисту. Ефективність механізму захисту ρ_j оцінюється множиною показників

$$\rho_j = (\rho_j^1, \rho_j^2, ..., \rho_j^L),$$

де $L = |R_j|$, а ρ_j^L – величина, що показує, наскільки відсотків зменшиться збиток від L-го інформаційного ризику при використанні j-го механізму захисту.

Сумісність механізмів захисту характеризується підмножиною механізмів захисту $M_j \subseteq M$, які сумісні з j-м механізмом.

Витрати C_j на придбання або на зміну, розробку, створення, а також на впровадження і експлуатацію j-го механізму дорівнюють одного року експлуатації. Це означає, що витрати на придбання, створення та впровадження нового або модифікованого механізму рівномірно розподіляються на всі роки передбачуваної експлуатації цього механізму. Перехідні витрати можуть коригуватися відповідно до прийнятої політики інвестиційних витрат. Розрахункові терміни служби механізмів захисту визначаються часом експлуатації відповідних елементів ІСП. Наприклад, за результатами досліджень Gartner Group [6] середній термін використання сучасних ПЕОМ складає чотири року. Для вже функціонуючих механізмів в складі СУІР враховуються тільки витрати на їх експлуатацію.

Необхідно визначити підмножину механізмів захисту $M^* = (m_1, m_2, ..., m_k)$, щоб отримати загальні мінімальні витрати S^* на управління ІР на планований рік.

Методика вибору оптимальної множини механізмів захисту від інформаційних ризиків

Для програмної реалізації методики вибору оптимальної множини механізмів захисту найбільш прийнятною є таблична форма подання вихідних даних.

У якості механізмів, які можуть бути використані при модернізації СУІР, необхідно розглядати механізми, що сумісні з апаратної і програмної платформами ІСП, мають офіційний сертифікат і відповідають національним стандартам. Бажано також мати відповідність світовим стандартам.

При формуванні вихідних даних і подальшого їх аналізу необхідно враховувати сумісність механізмів захисту. Сумісними будемо вважати механізми захисту від певного ІР, які допускають їх безконфліктне спільне використання і не є альтернативними. Під альтернативними будемо розуміти механізми захисту, які призначені для вирішення одних і тих же завдань і спільне використання яких технологічно неможливо або не призводить до підвищення ефективності системи в порівнянні з роздільним застосуванням механізмів. Як правило, альтернативними є механізми, що виконують однакові функції, і принципи дії яких ідентичні [7].

Альтернативні механізми захисту та ризики, від яких вони захищають, можуть бути зведені у таблицю вибору альтернативних механізмів захисту (табл. 1). Кожній підмножині альтернативних механізмів захисту $M_t \subset M, t = \overline{1,T}$ в табл. 1 відповідає один рядок – рівень t. Механізми з цієї підмножини можуть забезпечувати захист як від одного, так і від декількох ІР. У таблиці на кожному рівні представлено підмножина ризиків, від яких захищає відповідна підмножина альтернативних механізмів захисту. Підмножину ризиків зручно задавати в бінарному вигляді [7].

Якщо від ризику r_i захищають механізми, підмножина яких розміщено в рядку t табл. 1, то на перетині стовпця r_i та рядка t записується 1. В іншому випадку в цій клітці міститься 0. Потужність множини механізмів рівня t $\mu_t = |M_t|$ змінюється в межах $\mu_t = \overline{1, K+1}$, а потужність множини ризиків на тому ж рівні - $\rho_t = |R_t|$, знаходиться в межах $\rho_t = \overline{1, N}$.

Гранична кількість механізмів захисту на одиницю перевищує загальну кількість механізмів K, оскільки на кожному рівні вводиться один нульовий механізм m_l^a. Він використовується в методиках аналізу для забезпечення можливості виключення підмножини альтернативних механізмів.

Таблиця 1

Альтернативні механізми захисту

Рівень	Підмножина альтернативних механізмів						Підмножина ризиків					Потужності підмножин	
							r_1	r_2	…	r_{N-1}	r_N	$\mu_t = \|M_t\|$	$\rho_t = \|R_t\|$
1	m_l^1	m_l^2	…	$m_l^{\mu_2-1}$	m_l^1		1	0	…	1	0	μ_1	ρ_1
2	m_2^1	m_2^2	…	$m_l^{\mu_2-1}$	m_2^a		0	0	…	1	0	μ_2	ρ_2
…	…	…	…	…	…	…	…	…	…	…	…	…	…
t	m_t^1	m_t^2	…	$m_{l_1}^{\mu_{iT}-}$	m_l^a		0	1	…	0		μ_t	ρ_t
…	…	…	…	…	…	…	…	…	…	…	…		
T	m_T^1	m_T^2	…	$m_l^{\mu_2-1}$	m_T^a		0	1	…	0	1	μ_T	ρ_T

В СУІР необхідно передбачити також можливість прийняття ризиків. У цьому випадку на підприємстві не робиться ніяких дій для протидії незначному ризику. Якщо ризик r_a приймається, то він видаляється на всіх рівнях таблиці шляхом заповнення стовпця r_a нулями. У результаті збиток від прийнятого ризику не буде зменшуватися за рахунок використання механізмів захисту.

Заповнення рядків таблиці вибору альтернативних методик захисту може здійснюватися відповідно до різних підходів. Одним з можливих варіантів заповнення є вибір підмножин альтернативних механізмів в порядку убування середніх витрат на їх впровадження і експлуатацію. Другий підхід пов'язаний з аналізом суми збитку від ризиків, захист від яких забезпечують альтернативні механізми захисту та суми збитків від ризиків, яким протистоїть цей механізм. Порядок заповнення зберігається – за зменшенням загальної суми.

Однією з основних таблиць вихідних даних є таблиця ефективності механізмів захисту (табл. 2).

Таблиця 2

Показники ефективності механізмів захисту

Ризики	Механізми							
	m_l^1	m_l^2	m_l^3	…	m_t^j	m_t^{j+1}	…	$m_T^{\mu T}$
R_1	80%	75%	30%	….	0%		…	60%
R_2	0%		85%	…	0%		…	0%
…				…			…	
R_i	90%	70%	0%	…	ρ_{ij}	0%	…	60%
…	…	…	…	…	…	…	…	…
R_N	0%	90%	0%	…	85%	90%	…	40%

Вміст клітинки p_{ij} таблиці показує, на скільки відсотків зменшиться величина збитку від і-го ризику при наявності в СУІР j-го механізму захисту.

Значення клітинки p_{ij} = 0% вказує на те, що j-й механізм не впливає на і-й ризик. Якщо в системі для протидії будь-якого ІР використовуються одночасно два механізми з ефективністю, припустимо, 40% та 60%, то це не означає, що сумарна ефективність буде дорівнювати 100%. Ніякий механізм або навіть певна їх підмножина не можуть забезпечити стовідсотковий захист від ІР.

Розглянемо методику вибору оптимального складу механізмів захисту від ІР із застосуванням методики гілок та меж. Сутність цієї методики полягає в генерації підмножин механізмів, складових поточної гілки, та перевірці їх оптимальності з метою вибору підмножини механізмів, що забезпечує мінімальні повні витрати на управління ІР. Перевірка оптимальності поточної гілки проводиться при кожному включенні в неї чергового механізму, після чого приймається рішення про доцільність подальшого аналізу можливих варіантів включення нових механізмів. Відмова від аналізу завідомо безперспективних гілок дозволяє зменшити обчислювальну складність методики.

Повною гілкою будемо вважати підмножину сумісних механізмів захисту, що отримане в результаті перегляду всіх Т рівнів таблиці вибору альтернативних механізмів захисту (табл. 1). Перегляд ведеться в напрямку від першого рівня таблиці до рівня Т.

При включенні механізму m^j_t в гілку його поточна вага обчислюється за допомогою використання таблиці ефективності механізмів захисту (табл. 2) та таблиці збитків від ІР (табл. 3).

Таблиця 3

Величина збитків від інформаційних ризиків

	Інформаційні ризики					
	r_1	r_2	⋯	r_i	⋯	r_N
Величина збитку в грошовому еквіваленті	u_1	u_2		u_i		u_N

Для підрахунку повних витрат на управління ризиками необхідні також дані про витрати на впровадження та експлуатацію механізмів захисту. Їх доцільно звести в таблицю витрат на механізми захисту (табл. 4).

Таблиця 4

Витрати на механізми захисту

	Механізми захисту					
	m^1_1	m^2_1	⋯	m^2_1	⋯	$m^{\mu_T}_T$
Витрати на створення, впровадження та експлуатацію механізмів захисту	c^1_1	c^2_1	⋯	c^j_t	⋯	$c^{\mu_T}_T$

В якості ваги повної гілки будемо розглядати суму повних витрат на включення і експлуатацію механізмів у складі СУІР і збитку від ІР, які проаналізовані на всіх рівнях від першого до рівня Т включно.

Методика вибору оптимального набору механізмів захисту реалізується для певної підмножини прийнятих ризиків D, для яких не використовуються жодних механізмів захисту.

У загальному випадку можливий повний перебір всіх комбінацій прийнятих ризиків. Відбір ІР може здійснюватися експертами або відповідно до прийнятих правил прийняття рішення. Наприклад, до числа прийнятих ризиків відносять ті з них, збиток від яких очікується менше встановленого порогового значення.

Після формування підмножини D здійснюється коригування даних табл. 1, в якій замуляються стовпці r_i, відповідно включеним в підмножину D збиткам. Збиток від прийнятих ризиків враховується до реалізації методики визначення підмножини механізмів захисту.

Вага S^t_k поточної k-ої гілки підраховується як сума ваг витрат, визначених на кожному рівні t. Аналіз рівнів здійснюється в напрямку від 1-го до рівня Т.

При формуванні ваги гілки на рівні t враховується вага збитку кожного і-го ризику на цьому рівні:

$$u_i\varphi^i_t - f_t(p_{ij})u_i,$$

де $\varphi^i_t = \begin{cases} 1, \text{якщо}\,(r_{ti} = 1 \wedge \forall r_i = 0) \vee r_{li} = 1, \tau = \overline{1, t-1}; \\ 0, \text{в іншому випадку}; \end{cases}$

$$f_t(p_j) = \begin{cases} p_{ij}, \text{якщо}\,(r_{ti} = 1 \wedge \forall r_i = 0) \vee r_{li} = 1, \tau = \overline{1, t-1}; \\ \psi_i\left(\sum_T p_{ij}\right), \text{якщо}\ (r_{ti} = 1 \wedge \exists r_i = 1), \tau = \overline{1, t-1}; \end{cases}$$

$\psi_i\left(\sum_T p_{ij}\right)$ – функція, що визначає сумарну ефективність декількох механізмів захисту, включених в гілку, щодо зниження шкоди від і-го ІР, причому область допустимих значень цієї функції знаходиться в межах від 0 до 100 %.

На кожному рівні за допомогою функції $\psi_i\left(\sum_T p_{ij}\right)$ здійснюється корекція (зменшення) величини збитку за рахунок включення в гілку нового механізму, що доповнює можливості вже включених раніше механізмів захисту від і-го ризику.

Повна вага витрат на рівні tS_k^t поточної k-ої гілки визначається у відповідності з виразом:

$$S^t_k = \sum_D u_d + (c^j_t + \sum_T (u_i\varphi^i_t - u_i f_t(p_{uj})))\gamma_t,$$

де: γ_t – коефіцієнт необхідності включення механізму; m_t^j, c_t^j – витрати н створення та експлуатацію механізму захисту m_t^j.

Бінарний коефіцієнт приймає такі значення:

$$\gamma_t = \begin{cases} 1, \text{ якщо } \sum_{i=1}^{N} r_{ti} \neq 0; \\ 0, \text{ у іншому випадку.} \end{cases}$$

Отримання нульового коефіцієнту γ_t можливо в результаті корегування даних табл. 1 при прийнятті ризиків.

Повна вага k-ої гілки S_k може бути визначена у відповідності з наступним виразом:

$$S_k = \sum_D u_d + \sum_{t=1}^{T} (c_t^j + \sum_T (u_i \varphi_t^j - u_i f_t(p_{uj})))\gamma_t .$$

Дані для обчислення ваги гілки вибираються з табл. 1 – 4. Сума $\sum_D u_d$ є величиною постійною для усіх гілок вибраної підмножини ризиків. Тому для аналізу гілок, що генеруються, немає необхідності його використання при визначенні їх ваги. Достатньо аналізувати вираз:

$$S_k = \sum_D u_d + \sum_{t=1}^{T} (c_t^j + \sum_T (u_i \varphi_t^j - u_i f_t(p_{uj})))\gamma_t .$$

Сума $\sum_D u_d$ використовується при обчисленні повних витрат на управління ІР після вибору оптимальної підмножини механізмів захисту (оптимальної гілки).

У процесі аналізу гілок запам'ятовується найменша поточна сума витрат $S_{Tm,}$, що отримана в результаті аналізу повної гілки. Ця сума використовується в якості границі. Запам'ятовується також підмножина механізмів захисту, які утворили гілку з сумою витрат S_{Tm}. Сума S_{Tm} порівнюється із сумою витрат, отриманої після включення чергового механізму поточного рівня в аналізовану гілку. Якщо на кожному рівні сума, що отримується, була позитивною, то тоді була б можливість використовувати методику гілок і меж.

В даній методиці негативна сума може мати місце, якщо розглянутий на рівні t механізм захищає від ризиків, які вже аналізувалися на більш високих рівнях. На рівні t величина таких збитків вже не враховується для виключення її повторного використання у виразі підрахунку ваги гілки. Сума буде позитивною тільки при виконанні умови:

$$c_t^j > \sum_T \text{ та } u_i f_t(p_{ji}).$$

Тобто витрати на механізм m_t^j перевершують величину, на яку знизиться величина збитку від ризику за умови, що цей механізм застосовується на додаток до вже використовуваних механізмів захисту від розглянутих ризиків.

Щоб врахувати особливості методики, необхідно виконувати на цьому етапі додаткову перевірку перспективності гілки в разі отримання ваги поточної гілки, що перевищує границю. Формально ця умова може бути представлена таким чином:

якщо

$$i = \overline{1,N}\ \exists r_{\tau i} = 1 \wedge \exists r_{lk} \text{ при } \tau = \overline{1,t-1} \text{ та } \overline{k = t+1,T},$$

то необхідно продовжити аналіз гілки.

Якщо приведена умова не виконується, то подальший аналіз поточних гілок не виконується.

Після закінчення аналізу повної гілки, що сгенерована, сума S_T порівнюється з S_{Tm}. Якщо $S_T < S_{Tm}$, то в якості S_{Tm} надалі використовується сума S_T. Запам'ятовується також підмножина механізмів захисту, що входить в отриману гілку, яка в подальшому буде використана в якості граничної гілки.

Рішенням задачі є підмножина механізмів захисту, що відповідає найменшій вазі $S_{Tm} = S^*$, яка отримана на момент перегляду всіх можливих гілок для даної комбінації прийнятих ризиків. Шляхом перебору комбінацій прийнятих ризиків вибирається чергова їх комбінація, проводиться корекція таблиці вибору альтернативних механізмів захисту та виконується методика пошуку оптимальної гілки механізмів.

За результатами аналізу всіх обраних комбінацій прийнятих ризиків отримується множина оптимальних механізмів, що забезпечує мінімальні витрати на управління ІР.

Висновки

Запропонована методика дозволяє знайти оптимальну множину механізмів захисту від ІР. Ця методика може бути покладена в основу методики оптимізації СУІР компаній. Розвитком методики може служити створення ітеративного алгоритму оптимізації за участю особи, яка приймає рішення на етапах реалізації методики.

Обов'язковою умовою успішного ризик-менеджменту в галузі інформаційних технологій є його безперервність. Тому оцінка ІР, а також розробка та оновлення планів по їх мінімізації повинні проводитися з певною періодичністю, наприклад раз на квартал.

На підставі отриманих результатів може прийматися рішення на модернізацію СУІР.

Напрям подальших досліджень пов'язаний з розробкою програмної реалізації запропонованої методики системи управління інформаційних ризиків.

Література

1. Черныш, В.И. Методы оценивания информационных рисков компании [Текст] / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: сб. тез., 18–20 апреля 2011 р., т. 5. – Х.: ХНУРЭ. 2011. – С. 195.

2. Замула, О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки [Текст] / О.А. Замула, В.І. Черниш // Системи обробки інформації. – Х.: ХУ ПС, 2011. – Вип. 2 (92). – С. 53-56.

3. Замула, А.А. Оценивание рисков информационной безопасности в современных информационных системах [Текст] / А.А. Замула, В.И. Черныш, К.И. Иванов // XIV Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах»: тез. докл. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2011. – С. 31.

4. Ильенкова Н.Д. Методология исследования риска хозяйственной деятельности [Текст]: Дис. докт. эком. наук: 08.00.01; защищена 2.05.99; утв. 15.09.99 / Ильенков Николай Дмитриевич. – М., 1999. – 208 с.

5. НД ТЗІ 1.1_003_99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Текст]. – К., 1999. – 24 с.

6. Скрипкин, М.С. Финансовая информатика: учеб. для вузов [Текст] / М.С. Скрипкин. – М.: ТЕИС, 1997. – 296 с.

7. Конев И.Р. Информационная безопасность предприятия [Текст] / И.Р. Конев, А.В. Беляев. – СПб.: БХВ-Петербург, 2003. – 220 с.

Поступила в редакцию 25.10.2011

Рецензент: д-р техн. наук, проф. Є.І. Літвінова, Харківський національний університет радіоелектроніки, Харків.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ КОМПАНИЙ

А.А. Замула, В.И. Черныш, К.И. Иванов, Б.В. Волобуев

Разработана модель системы управления информационными рисками. В статье рассмотрен пример решения задачи управления информационными рисками без применения страхования рисков. Предложенная методика позволяет найти оптимальное множество механизмов защиты от информационных рисков. Эта методика может быть положена в основу методики оптимизации системы управления информационными рисками и внедрена в информационные системы компаний. Развитием методики может служить создание итеративного алгоритма оптимизации с участием лица, принимающего решения на этапах реализации методики.

Ключевые слова: информационная безопасность, информационный риск, механизмы защиты.

CONTROL SYSTEM FOR INFORMATION RISK COMPANIES

A.A. Zamula, V.I. Chernish, K.I. Ivanov, B.V. Volobuiev

A model of information risk management. The article presents an example of problem-solution information risk management without the use of non-life insurance. The proposed method allows to find an optimal set of mechanisms for the protection of information risks. This technique can be used as the basis of the methods of optimization of information risk management and information systems are implemented in companies. Development methodology is the establishment of an iterative optimization algorithm with a decision-maker on the stages of the procedure.

Key words: information security, information risk protection mechanisms.

Замула Олександр Андрійович – канд. техн. наук, доцент, професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: bit@iit.com.

Черниш Владислав Ігорович – магістрант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: vlad.chernish@gmail.com.

Іванов Костянтин Ігорович – магістрант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: kiivnv@gmail.com.

Волобуєв Богдан Володимирович – магістрант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: bodog2008@narod.ru.