Наступним етапом необхідно провести порівняння фактичного значення інтегрального показника інвестиційної привабливості з нормативним ($ИПП_{НОРМ}$):

$$ИПП_{НОРМ} = \sum_{i=1}^{n} w_i \frac{I_i^{НОРМ}}{I_i^{НОРМ}} = \sum_{i=1}^{n} w_i = 1. \qquad (11)$$

Проведені вище розрахунки свідчать, що у 2010-2012 рр. фактичне значення інтегрального показника інвестиційної привабливості ПАТ "Трест Житлобуд-1" нижче від нормативного.

Доцільним є визначення типу інвестиційної привабливості підприємства:

$ИПП_{ФАКТ} \geq 1$ – підприємство є інвестиційно-привабливим,

$ИПП_{ФАКТ} < 1$ – підприємство не є інвестиційно-привабливим.

Отже, ПАТ "Трест Житлобуд-1" за період, що оцінювався, не є інвестиційно-привабливим підприємством на будівельному ринку.

Висновки. Подальші дослідження будуть спрямовані на вдосконалення методики оцінки інвестиційної привабливості будівельного підприємства з врахуванням його внутрішнього потенціалу та сукупного впливу зовнішнього середовища.

ЛІТЕРАТУРА:

1. Алексєєнко Л.М. Фінансові аспекти оцінки інвестиційної привабливості підприємства / Л.М. Алексєєнко // Економічний форум. – 2009. – №3. – С.94–102.
2. Бланк И.А. Управление инвестициями предприятия / И.А. Бланк. – К. : Ника- Центр. – 2003. – 480 с.
3. Верзакова Е.А. Оценка инвестиционной привлекательности отраслей производственной сферы / Верзакова Е.А. // Современные проблемы науки и образования. – 2006. – №8. – С. 23–28.
4. Донцов С.С. Оценка инвестиционной привлекательности предприятия посредством анализа надежности его ценных бумаг / С.С. Донцов // Финансовый менеджмент. – 2010. – № 3. – С. 46–51.
5. Иванов А.П. Принципы и факторы определения инвестиционного рейтинга предприятий / А.П. Иванов, И.В. Сахарова, Е.Ю. Хрусталев // Консультант директора. – 2009. – № 12. – С. 31–37.
6. Козаченко Г.В. Управління інвестиціями на підприємстві : [монографія] / Г.В. Козаченко, О.М. Антіпов, О.М. Ляшенко, Г.І. Дібніс. – К.: Лібра. – 2007. – 368 с.
7. Майорова Т.В. Інвестиційна діяльність [навчальний посібник] / Майорова Т.В. – К. : «Центр навчальної літератури». – 2006. – 376 с.
8. Макарій Н.П. Оцінка інвестиційної привабливості українських підприємств / Н.П. Макарій // Економіст. – 2010. – № 10. – С. 52–60.
9. Трясцина Н.Ю. Комплексная оценка инвестиционной привлекательности предприятий / Н.Ю. Трясцина. – [Электронный ресурс]. – Режим доступа: http://www.fin-izdat/journal/analiz/detali.php?ID=2888.

УДК 519.81

Солодовник Г.В., Тоцька Д.Д.
Харківський національний університет будівництва та архітектури

МОДЕЛЮВАННЯ РИЗИКІВ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Вступ. Розвиток нових інформаційних технологій і загальна комп'ютеризація призвели до того, що інформаційна безпека не тільки стає обов'язковою, а набуває значення однієї з характеристик інформаційних систем. Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє провідну роль наприклад, банківські інформаційні системи. Численні публікації останніх років показують, що зловживання інформацією, що циркулює в інформаційних системах або передається по каналах зв'язку, удосконалюється не менш інтенсивно, ніж заходи захисту від них. В даний час для забезпечення захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії, тощо). Комплексний характер захисту виникає з комплексних дій зловмисників, які прагнуть будь-

якими засобами здобути важливу для них інформацію.

Мета і завдання: виявити та класифікувати загрози порушення цілісності інформації, та заходи їх нейтралізації; визначити найкращій проект із захисту інформації на підставі мір ризику; ознайомитися з теоретичними засадами якісного аналізу ризиків в сфері захисту інформаціі, а також моделями визначення кількісних мір ризику; автоматизувати процес обчислення мір ризику та визначення найкращого з варіантів захисту інформації.

Робота присвячена виявленню та класифікації найбільш суттєвих ризиків в сфері інформаційних технологій. Розв'язано задачу визначення найкращого, з точки зору прибутковості та ризикованості проекту, рішення автоматизовано за допомогою Microsoft Excel.

Результати досліджень. Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних коштів [1].

До основних загроз безпеці інформації і нормального функціонування ІС відносяться:

– витік конфіденційної інформації;
– компрометація інформації;
– несанкціоноване використання інформаційних ресурсів;
– помилкове використання інформаційних ресурсів;
– несанкціонований обмін інформацією між абонентами;
– відмова від інформації;
– порушення інформаційного обслуговування;
– незаконне використання привілеїв.

Класифікувати можливі порушення, які можуть викликати втрату або зміну інформації можна наступним чином:

1. Збої в роботі устаткування: збої кабельної системи, системі електроживлення; помилки в роботі серверів, робочих станцій, тощо.

2. Втрата інформації через помилки в роботі програмного забезпечення: через помилки в роботі операційних систем; зараженні комп'ютера вірусами.

3. Втрати, пов'язані з несанкціонованим доступом: незаконне копіювання, знищення інформації; ознайомлення з інформацією, що є таємницею.

4. Втрата інформації, пов'язана з невірним зберіганням інформації.

5. Помилки обслуговуючого персоналу: випадкове знищення даних; невірне використання програмного забезпечення, що призвело до втраиу даних.

Відповідно до виду можливих правопорушень, численні види захисту інформації поділяють на три основних види:

– програмні засоби захисту, наприклад, антивірусні пакети, системи багатокористувальницького доступу, тощо;

– засоби фізичного захисту, включаючи захист кабельних систем, використання різноманітних джерел безперебійного живлення, захист приміщень від стороннього доступу, резервне копіювання інформації;

– адміністративні засоби захисту, що об'єднують перші два пункти, формуючи політику інформаційної безпеки компанії.

Найчастіше застосовуються комплексні методи боротьби, які можна назвати програмно-апаратними [2].

За допомогою методу експертних оцінок проаналізуємо ризиковані ситуації захисту інформації. Суть методу експертних оцінок полягає в проведенні експертами інтуїтивно-логічного аналізу проблеми з кількісною оцінкою думок і формальною обробкою результатів. Результати експертних оцінок в табл. 1.

Під номерами ризиків мається на увазі: 1 – ризик несанкціонованого доступу; 2 – ризик зараження «троянським конем»; 3 – ризик зараження «хробаком»; 4 – ризик логічної бомби; 5 – ризик загарбника паролів.

Важливим моментом експертних процедур є оцінка погодженості дій експертів та вірогідності експертних оцінок. Найчастіше для цих цілей використовують коефіцієнт конкордації, величина якого дозволяє

судити про ступінь погодженості думок експертів і, як наслідок, про вірогідність їхніх оцінок. Його значення знаходиться в межах $0 < W < 1$, де $W = 0$ означає, що зв'язку між оцінками різних експертів немає, а $W = 1$ – повна погодженість думок.

Таблиця 1 – Результати оцінок експертів

експерти	Ризики				
	1	2	3	4	5
1	5	4	2	1	3
2	3	5	4	1	5
3	5	3	2	1	4
4	3	4	5	2	1
сумарне	16	16	13	5	13
погодженість	4	5	3	1	2
сум.погодженість	16	20	12	4	8

В нашому випадку коефіцієнт конкордації отриманий в результаті ділення фактичної дисперсії сумарних оцінок експертів на дисперсію сумарних оцінок, коли думка експертів цілком збігається становить 0,51895. Нормативна величина = 0,5 тобто вона менше коефіцієнта конкордації. Зробимо висновок, що можна ухвалити рішення про використання отриманих від експертів оцінок.

Забезпечення інформаційної безпеки – досить дорогий процесс, тому перш за все, треба визначити необхідний рівень захищеності. Під час вибору (розробки) системи захисту інформації слід вирішувати двукритеріальну задачу: мінізувати вартість комплексу захисних заходів та максимізувати ступінь захисту.

Витік та пошкодження бізнес-інформації також може бути виражений у грошовому еквіваленті. Об означимо різні комплекси захосних дії як проекти A,B,C, а різницю між вартістью інформації, що зберігається та передається, та витратою на придбання або розробки системи захисту, як прибуток за проектом. Прибуток за проектом є стохастичною величиною, значення якої залежить від настання тих або інших загроз інформації, які формулюємо як песимістични, стриманий та песимістичний стани зовнішнього середовища (табл. 2).

Таблиця 2 – Початкові данні

проект	**песимістичний**		**стриманий**		**оптимістичний**	
	прибуток	імовірн.	прибуток	імовірн.	прибуток	імовірн.
A	-200	0,2	150	0,6	300	0,2
B	-120	0,3	75	0,4	250	0,3
C	-170	0,4	130	0,2	270	0,4

Вибір проекта здійснюється на підставі мір ризику: обирається проект з максимальною прибутковістью та мінімальною ризикованістью. Прибутковість обчислюється, як математичне сподівання випадкової величини – прибуток за проектом [3].

$$M(x) = \sum_{i=1}^{n} x_i p_i \qquad (1)$$

Ризиковість – як середньоквадратичне відхилення.

$$\sigma_x = \sqrt{p_i(x_i - p_i)\text{^}2} \qquad (2)$$

У результаті розрахунків отримаємо такі дані: M_A=80; M_B=69; M_C=66; σ_A=165,29; σ_A=143,38; σ_A=199,36. На підставі отриманих оезультатів робимо висновок про відкидання проекту C, оскільки він має найнижчу прибутковість та найбільшу ризикованість. Вибір між проектами A та B слід залежить від ставлення до ризику особоби, що приймає рішення: проект A прибутковіший але має найбільше значення ризикованості.

Висновки. В ході аналізу були виявлені джерела ризику, класифіковані ризики пов'язані із захистом інформації, визначені міри ризику за трьома проектами, на підставі яких надані рекомендації щодо вибору одного з них.

ЛІТЕРАТУРА:

1. Россоха В.В. Системная процедура экономического анализа и оценки рисковых ситуаций / Економіка: проблеми теорії та практики: Зб. наук. пр./ ДНУ. - 20010. - Вип. 113. - С. 108-114.
2. Устенко О.Л. Теория экономического риска: Монография. – К.: МАУП, 2010. – 164 с.
3. Новожилова М.В., Солодовник Г.В. Моделювання управління комерційним ризиком: Навчально-методичний посібник. - Харків:ХНУБА, 2011 р.-81 с.