Список літератури: 1. *Абалкин Л.И.* Диалектика социалистической экономики. – М., 1981. – С. 24. **2.** *Лукинов И.И.* Интенсификация социалистической экономики / И.И. Лукинов / – Т.1. – К., 1989. **3.** *Попов Е.* Структура рыночного потенциала предприятия / Е. Попов, В. Ханжина // Проблемы теории и практики управления. – 2001. – № 6. **4.** *Катькало В.С.* Место и роль ресурсной концепции в развитии теории стратегического управления / В.С. Катькало // Вестник СпбГУ. Сер. 8. – 2002. – Вып. 3. – № 4. **5.** *Сычева Г.И.* Оценка стоимости предприятия (бизнеса) / Г.И. Сычева, Е.Б. Колбачев, В.А. Сычев. – Ростов-на-Дону: Феникс, 2003. – 384 с. **6.** Виробничий потенціал та його використання в Україні. [Електронний ресурс]. – Режим доступу: http://info-works.com.ua/referats/econimichna_teoria/1797.html. **7.** *Отенко І.П.* Механізм управління потенціалом підприємства / І.П. Отенко, Л.М. Малярець. – Х.: Вид -во ХДЕУ, 2003. – 220 с. **8.** *Бакунов О.А., Яременко М.О.* Концептуальний підхід до управління потенціалом торговельного підприємства / О.А. Бакунов, М.О. Яременко // Європейський вектор економічного розвитку. – 2011. – № 2 (11). – С. 20–27.

Надійшла до редколегії 20.10.2013

УДК 336:339.17

Концептуальні підходи до управління потенціалом розвитку підприємства / Іванець О. О. // Вісник НТУ «ХПІ». Серія: Актуальні проблеми управління та фінансово-господарської діяльності підприємства – Харків: НТУ «ХПІ». – 2013. – № 52 (1025). – С. 62–69. Библиогр.: 8 назв.

В статье раскрыты основные концептуальные подходы к управлению потенциалом развития предприятия. Определены факторы и принципы, которые обусловливают развитие его элементов.

Ключевые слова: концептуальные подходы, потенциал развития, потенциал предприятия.

In the article basic conceptual approaches to the management potential of development of the enterprise. Factors and principles that determine the development of its elements are defined.

Keywords: conceptual approaches, development potential, the potential of enterprise.

УДК 330.47

Э. А. КАРПОВ, профессор, канд. экон..наук, Старооскольский технологический институт, Старый Оскол, Россия;
И. Н. КОСАРЕВА, ассистент, Старооскольский технологический институт;
А. Г. КОБЗЕВА, ассистент, Старооскольский технологический институт.

ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ ПО МЕТОДИКЕ CRAMM

В современных условиях одной из актуальных задач является оценка эффективности мероприятий по защите информации в информационных компьютерных системах. Данная работа посвящена одной из наиболее популярных и универсальных методик – cramm.

Ключевые слова: информационные риски, методика cramm.

Введение. Растет информационная инфраструктура организаций, которая по мере приобретения средств вычислительной техники, часто, разрастается «вширь», приобретая неструктурированный гетерогенный характер. Это в свою очередь приводит к неконтролируемому росту количества уязвимостей и увеличению возможностей доступа к информации со стороны внешних и внутренних нарушителей.

Появление и осознание проблем информационной безопасности приводит к необходимости измерения величины информационного риска. Оценка риска

позволяет определить необходимую степень защиты, выбрать стратегию развития информационной структуры организации и поддерживать на должном уровне безопасность организации.

В настоящее время многие организации, специализирующиеся в решении проблем информационной безопасности предлагают (часто в качестве коммерческого продукта) различные методики оценки информационных рисков. Известные методики можно классифицировать по типу используемой в них процедуры принятия решения на одноэтапные и многоэтапные. В одноэтапных методиках (электронные таблицы типа "Risk Matrix") оценка риска выполняется с помощью одноразовой решающей процедуры. В многоэтапных методиках (NIST, CRAMM) оценка риска проводится с предварительным оцениванием ключевых параметров.

Механизм оценивания рисков на основе нечеткой логики, по существу, является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин и риска. В простейшем случае это «табличная» логика, в общем случае – более сложная логика, отражающая реальные взаимосвязи, которые могут быть формализованы с помощью продукционных правил вида «ЕСЛИ, …, ТО».

Методика. Рассмотрим механизм получения оценок риска на основе нечеткой логики по методике CRAMM с предварительным оцениванием двух входных параметров: оценки вероятности некоторого инцидента и ущерба от этого инцидента. Для измерения входных параметров используются пятиуровневые шкалы.

CRAMM – инструментальное средство, реализующее одноименную методику, которая была разработана компанией BIS Applied Systems Limited no заказу британского правительства. Метод CRAMM позволяет производить анализ рисков и решать ряд других аудиторских задач: обследование информационной системы, проведение аудита в соответствии с требованиями стандарта BS 7799, разработка политики безопасности.

Данная методика опирается на оценки качественного характера, получаемые от экспертов, но на их базе строит уже количественную оценку. Метод является универсальным и подходит и для больших, и для мелких организаций как правительственного, так и коммерческого сектора.

CRAMM предполагает разделение всей процедуры на три последовательных этапа. Задачей первого этапа является определение достаточности для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимость проведения более детального анализа. На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается

вопрос о выборе адекватных контрмер. Для каждого этапа определяются набор исходных данных, последовательность мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов.

Достоинства метода CRAMM: хорошо структурированный и широко опробованный метод анализа рисков; может использоваться на всех стадиях проведения аудита безопасности информационных систем; в основе программного продукта лежит объемная база знаний по контрмерам в области информационной безопасности, гибкость и универсальность данного метода позволяют его использовать для аудита информационной системы любого уровня сложности и назначения; данный метод позволяет разрабатывать план непрерывности бизнеса.

Шкала вероятности содержит следующие уровни:

A – событие практически никогда не происходит;

B – событие случается редко;

C – вероятность события за рассматриваемый промежуток времени около 0.5 (*событие вполне возможное при соответствующем стечении обстоятельств – авт.*);

D – скорее всего событие произойдет (*при организации атаки – авт.*);

E – событие, вероятнее всего, произойдет (*при организации атаки – авт.*).

Шкала ущерба содержит также пять уровней:

N (Negligible) – ущерб, которым можно пренебречь;

Mi (Minor) – незначительный ущерб, последствия которого легко устранить;

Mo (Moderate) – умеренный ущерб;

S (Serious) – серьезный ущерб, ликвидация которого возможна, но связана со значительными затратами;

C (Critical) – критический ущерб, который ставит под сомнение возможность устранения его последствий.

Следуя методике CRAMM, шкалу для оценки риска зададим в виде последовательности чисел от 0 до 8, включительно (таблица 1). Зависимость риска от вероятности и ущерба приведена в таблице 2.

Таблица 1 – Шкала оценки риска

Содержание описания оценки	Числовое значение
0 – незначимый	0 -0,111
1 – очень низкий	0,111 – 0,222
2 – низкий	0,222 – 0,333
3 – удовлетворительный	0,333 – 0,444
4 – средний	0,444 – 0,555
5 – приемлемый	0,555 – 0,666
6 – высокий	0,666 – 0,777
7 – критический	0,777 – 0,888
8 – недопустимый	0,888 – 1

Таблица 2 – Шкала оценки риска по пятиуровневым шкалам

Вероятность	Ущерб				
	N	Mi	Mo	S	C
A	0	1	2	3	4
B	1	2	3	4	5
C	2	3	4	5	6
D	3	4	5	6	7
E	4	5	6	7	8

Выводы. На кафедре Экономики и менеджмента СТИ НИТУ «МИСиС» был проведен анализ информационной безопасности ОАО «Оскольский электрометаллургический комбинат».

Таблица 3 – Результаты оценки риска по каждой угрозе методом нечеткой логики

Угроза	Величина риска
Уп	0,483
Ут	0,411
Ух	0,403
Ук	0,513
Уж	0,185

В общем, ни по одной из угроз риск утечки информации не превышает среднего значения, что в целом благоприятно для предприятия. Однако, наибольшую угрозу для ОАО ОЭМК представляют конкуренты (0,513) и персонал (0,483). Поэтому предприятию необходимо:

- более тщательно отбирать персонал
- ужесточить политику информационной безопасности
- тщательно следить за деятельностью своих конкурентов.

Список литературы: 1. *А. Балашов, Р.И. Кислов, В.П. Безгузиков* Оценка рисков информационной безопасности на основе нечеткой логики // Защита информации. Конфидент. – 2003 г. – №5. – С. 56-59 **2.** *С. Петренко, С. Симонов*, Методики и технологии управления информационными рисками «IT Manager», №3/2003 **3.** *Петренко С.А., Симонов С.В*. Управление информационными рисками. Экономически оправданная безопасность. − М.: АйТи-Пресс, 2004. − 384 с.

Надійшла до редколегії 20.10.2013

УДК 330.47

Оценка информационных рисков по методике CRAMM / Карпов Э.А., Косарева И.Н., Кобзева А.Г. // Вісник НТУ «ХПІ». Серія: Актуальні проблеми управління та фінансово-господарської діяльності підприємства – Харків: НТУ «ХПІ». – 2013. – № 52 (1025). – С. 69–72. Библиогр.: 3 назви.

В сучасних умовах однією з актуальних задач є оцінка ефективності заходів по захисту інформації у інформаційних комп’ютерних системах. Дана робота присвячена однієї з найбільш популярних та універсальних методик – cramm.

Ключові слова: інформаційні ризики, методика cram.

One of the most urgent tasks in the current circumstances, is to evaluate the effectiveness of measures for the protection of information in computer information systems. This work is devoted to one of the most popular and versatile methods – cramm.

Keywords: information risk, methodology cramm.