Висновки. В загальному випадку вирішення задачі оптимізації мережі МСАП повинно відповісти на запитання: де і скільки вузлів сенсорів необхідно встановити, щоб отримана мережа МСАП відповідала висунутим до неї вимогам. Класифікація задач оптимізації мереж МСАП може проводитись за відповідною областю оптимізації, заданістю кількості вузлів сенсорів, типом мережі тощо. Класифікація задач оптимізації мереж МСАП покликана спростити вибір необхідної математичної постановки відповідної задачі оптимізації та знайти методи для її вирішення.

1. *Артемчук В.О.* Математичні та комп'ютерні засоби для вирішення задачі розміщення пунктів спостережень мережі моніторингу стану атмосферного повітря [Текст] : дис. ... канд. техн. наук : спец. 01.05.02 "Математичне моделювання та обчислювальні методи" / В.О. Артемчук. – К., 2011. – 178 с.
2. Методичні рекомендації з підготовки регіональних та загальнодержавної програм моніторингу довкілля (затверджено Наказом Міністерства екології та природних ресурсів України 24.12.2001 р. N487)
3. *Рибалов О.О.* Основи моніторингу екологічного простору: Навчальний посібник. - Суми: Вид-во СумДУ, 2007. - 240 с.
4. *Гандин Л.С.* Об экономическом подходе к планированию сети метеорологических станций / Гандин Л.С., Каган Р.Л. // Труды ГГО. – 1967. – Вып. 208. – С.120–131.
5. *Дроздов О.А.* Теория интерполяции в стохастическом поле метеорологических элементов и её применение к вопросам метеорологических карт и рационализации сети / Дроздов О.А., Шепелевский А.П. // Труды НИУ. – 1964. – сер. 1. – Вып.13. – С.65–115.
6. *Верлан, В. А.* Оптимизация размещения сети постов мониторинга за загрязнением атмосферы в промышленном городе [Текст] : дис. ... канд. геогр. наук / В.А. Верлан. — О. – 1999. — 167 с.

Поступила 11.02.2013р.

УДК 004.056.5

В.М.Безштанько, Киев

ОПРЕДЕЛЕНИЕ ПРИЕМЛЕМОГО ЗНАЧЕНИЯ РИСКА ДЛЯ ИНФОРМАЦИОННЫХ АКТИВОВ ОРГАНИЗАЦИИ

Abstract. We propose approach for determining an acceptable risk value for the information assets of the organization

Актуальность

В процессе построения системы управления безопасностью информации (СУБИ), требованиями стандартов [1-2] на руководство организации возлагается задача установления приемлемого значения риска.

В соответствии с определением, изложенным в работе [3] под приемлемым значением риска, следует понимать обоснованную величину ущерба, с которой руководство организации готово согласиться и действовать в условиях ее существования. Информационными можно назвать риски, связанные с возможностью возникновения ущерба в результате использования организацией информационных активов [3,4]. Вопросы о том, какой риск следует считать приемлемым для информационных активов, являются одними из самих сложных и важных в практике построения системы СУБИ. Решение о приемлемости риска, как правило, руководитель или офицер безопасности организации принимают, опираясь на свои знания, опыт, а порой и интуицию, что не всегда позволяет получить правильный результат.

Постановка задачи

Стратегические планы организации разрабатываются в расчете на некоторые фиксированные условия или на их более или менее предсказуемое планомерное развитие. На практике, вследствие воздействия на организацию угроз, такие планы часто нарушаются, особенно в долгосрочной перспективе. В организации всегда существует вероятность не достижения намеченной цели и запланированного стратегического результата. Несовпадение полученного экономического результата с планируемым, то есть ущерб, можно охарактеризовать как риск. Снижение риска в организации происходит за счет внедрения организационных или технических мер безопасности активов. Можно предположить, что приемлемый риск организации состоит из суммы допустимых рисков активов. Следовательно, для определения допустимых значений риска каждого актива, возникает необходимость в разработке механизма, позволяющего устанавливать приемлемое значение риска в организации в целом.

Решение задачи

Пусть ущерб, при котором организация справляется с ним не прерывая своей повседневной деятельности, будет приемлемым риском r. Тогда величину допустимого риска r_j для j - того актива можно представить как произведение величины ущерба a_j на частость его возникновения x_j. Соответственно, для одного актива можно предложить следующее выражение:

$$a_j x_j = r_j .$$

Для организации важным является выполнение условия, когда произведение ущерба a_j на частость его возникновения x_j меньше или равно допустимого значения риска r_j. То есть $a_j x_j \le r_j$. Соответственно, можно предположить, что приемлемое значение риска организации r можно

представить в виде:

$$r_1+r_2+...+r_n \le r$$

или,

$$\sum_{j=1}^{n} r_j \le r ,$$

где, n - число оцениваемых рисков.

Допустим, что недополученный организацией доход $P_{план.}$, то есть ущерб A, можно взять за основу для расчета величины приемлемого значения риска r в организации. [5-8]. Пусть организация за определенный временной интервал (месяц, год) планировала получить значение прибыли $P_{план.}$. Реально за принятый для расчета период была получена прибыль $P_{пол.}$. Можно предположить, что разница между значением реальной и предполагаемой прибыли является нанесенным организации ущербом A.

Если организация получила прибыль больше планируемой, то можно предположить, что инцидентов, отрицательно воздействующих на активы организации за рассматриваемый период, не было. Если же инциденты, вследствие реализации которых, организация понесла убытки, имели место, то для ущерба A можно предложить выражение:

$$A=P_{план}-P_{пол.} .$$

Допустим, что для определения среднего значения ущерба $A_{ср}$ можно использовать выражение:

$$A_{ср.}=\frac{\sum_{i=1}^{m} A_i}{m},$$

или

$$A_{ср.}=\frac{\sum_{i=1}^{m}\left(P_{план.,i}-P_{пол.,i}\right)}{m},$$

где $i=1,2,...,m$ - количество проведенных измерений за рассматриваемый период времени.

Если, при проведении m- того измерения значения полученной прибыли $P_{пол.,i}$ будет больше $P_{план.,i}$, то значение ущерба A_i может принимать отрицательные значения. Следовательно, для измерения среднего значения ущерба $A_{ср}$ можно использовать среднеквадратичное отклонение дисперсий прибыли за рассматриваемый период. То есть:

$$A_{ср}=\sqrt{\frac{\sum_{i=1}^{m}\left(P_{план.i}-P_{пол.i}\right)^2}{m}}=\sqrt{\frac{\sum_{i=1}^{m}\left(A_i\right)^2}{m}} . \qquad (1)$$

Таким образом, можно предположить, что величина приемлемого риска r не должна превышать среднеквадратичного отклонения дисперсий ущерба проведенных измерений за рассматриваемый период успешной деятельности организации. То есть, для приемлемого значения риска r и среднего значения ущерба $A_{cp.}$ будет справедливо следующее соотношение:

$$r \le A_{cp.}$$

На практике, часто полученную прибыль измеряют в процентах. Для этого, значение ущерба A_i и среднеквадратичное отклонение дисперсий ущерба A_{cp} представляют в процентах.

Изложенные выше рассуждения рассмотрим на примере.

Допустим, что некую организацию за четыре года успешной деятельности можно оценить следующими характеристиками из таблицы 1.

Таблица 1

Рассматриваемый период, год	2009	2010	2011	2012
Планируемая прибыль, тис.грн.	200	210	215	220
Полученная прибыль, тис.грн.	180	195	210	210
Полученная прибыль, %.	90	92,75	97,67	95,45
Ущерб, тис.грн.	20	15	5	10
Ущерб %.	10	7,15	2,33	4,55

Используя выражение (1) можно определить среднее значение ущерба A_{cp} :

$$A_{cp} = \sqrt{\frac{(200-180)^2 + (210-195)^2 + (215-210)^2 + (220-210)^2}{4}} \approx 13{,}4 \text{ тис. грн.}$$

Или в процентах:

$$A_{cp} = \sqrt{\frac{(10)^2 + (7{,}15)^2 + (2{,}33)^2 + (4{,}55)^2}{4}} \approx 6{,}7\%.$$

Следовательно, для данного примера рекомендуется выбрать значение приемлемого риска r , удовлетворяющее следующие условия:

$$r \le A_{cp} \le 13{,}4 \text{ тис. грн.},$$

или

$$r \le A_{cp} \le 6{,}7\%$$

Выводы

В работе был предложен подход, который позволяет обосновать величину приемлемого значения риска в организации. Знание такой величины в дальнейшем позволит сформировать модель расчета допустимых значений риска r_j активов или группы активов организации. В свою очередь, знание допустимых значений риска r_j позволит принимать обоснованное управленческое решение о необходимости внедрения защитных мер для информационных активов организации.

1. ISO/IEC 27001:2005. Information technology -- Security techniques -- Information security management systems – Requirements.
2. ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management.
3. *В.В.Мохор, А.М.Богданов*, Изложение руководства «ISO GUIDE 73:2009. RISK MANAGEMENT – VOCABULARY» на руском языке», №2/04-06/2011 Das Management.
4. *В.И.Завгородний* /Парадигма информационных рисков // http://fa-kit.ru.
5. *Иванов А.А., Олейников С.Я., Бочаров С.А.* /Риск-менеджмент. Учебно-методический комплекс. Международный консорциум «Электронный университет».// Московский государственный университет экономики, статистики и информатики. Евразийский открытый институт. Москва - 2008.
6. *Лобанов А.Е. Чугунов А.В.* /Энциклопедия финансового риск–менеджмента,// Москва, Альпина Паблишер , 2003 .
7. *Е. Д. Соложенцев,* / Сценарное логико-вероятносное управление риском в бизнесе и технике,// Издательский дом «Бизнес-пресса», Санкт-Петербург -2006.
8. *И.А. Рябин* / Надежность и безопасность структурно-сложных систем.//Политехника 2000- 248с.

Поступила 18.02.2013р.

УДК 519.711

А.Е. Макаревич, И.В. Коцюба, г.Киев

ВОПРОСЫ ПРИМЕНЕНИЕ АППАРАТА ЛОГИКО-ВЕРОЯТНОСТНОГО МОДЕЛИРОВАНИЯ К РЕШЕНИЮ ЗАДАЧ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Abstract. We propose an approach for information security risk assessment with application of logical-and-probabilistic method.

Актуальность

Не секрет, что в наше время в повседневной деятельности организаций всех видов и форм собственности, все большую важность приобретает