УДК 681.3

МНОГОКРИТЕРИАЛЬНАЯ МОДЕЛЬ ВЫБОРА ВАРИАНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ РАСПРЕДЕЛЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

А. Г. Кащенко

Воронежский государственный технический университет

Поступила в редакцию 04.11.2010 г.

Аннотация. В работе рассмотрена задача выбора варианта системы защиты информации (СЗИ) для вычислительной сети предприятия. Задача выбора варианта СЗИ математически формализована в виде многокритериальной задачи оптимизации, для решения которой разработан алгоритм и программа на основе метода вектора спада.
Ключевые слова: множество Парето, система защиты информации, выбор варианта.
Annotation. In work the problem of a choice of a variant of information security system (ISS) for the enterprise computer network is considered. The problem of an optimum choice of security facilities for information security system is mathematically formalized in a kind multicriterion problem optimization for which decision the algorithm and the program on the basis of a method of a vector of recession is developed.
Keywords: ensemble Pareto, information security system, choice of variant

Информационная безопасность (ИБ) – один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере очень часто приводят к гибельным последствиям для бизнеса любой компании. Применение высоких информационных технологий, с одной стороны, дает значительные преимущества в деятельности предприятий и организаций, а с другой – потенциально создает предпосылки для утечки, хищения, утраты, искажения, подделки, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, социального или других видов ущерба. В этой связи задача нахождения путей снижения ущерба от нарушений ИБ становятся с каждым годом все острее. Особенно остро проблема обеспечения ИБ стоит перед территориально распределенными вычислительными системами (РВС), в частности, корпоративными вычислительными сетями.

Проблема снижения ущерба от нарушений ИБ РВС часто решается на основе оценки и управления рисками ИБ [1]. Целью процесса оценки и управления рисками ИБ РВС является принятие и реализация таких управленческих решений, чтобы в течение заданного времени функционирования РВС уровень остаточного риска соответствовал бы требуемому при минимальных затратах на механизмы защиты. Для оценки и управления рисками ИБ разрабатываются системы защиты информации (СЗИ).

В наиболее общем случае математически задача выбора рационального варианта СЗИ формулируется в виде следующей многокритериальной задачи выбора [2]: найти такой вариант СЗИ $\vec{X}^* \in \Pi \subset D$, для которого

$$Q(\vec{X}^*) = (q_1(\vec{X}^*), q_2(\vec{X}^*), \ldots, q_m(\vec{X}^*)) \to \to \underset{\vec{X}^* \in \Pi \subset D}{extr}, \tag{1}$$

$$G(\vec{X}^*) \le 0 \tag{2}$$

где Π – множество Парето – оптимальных решений; D – множество допустимых решений, в пределах которого выполняются функциональные и критериальные ограничения $G(\vec{X}^*) \le 0$, в частности, ограничение на уровень остаточного риска; $q_i(\vec{X}^*), i = 1, 2, \ldots, m$ – частные критерии оптимальности.

В частном случае при $m = 1$ задача (1–2) представляет собой известную в литературе задачу выбора СЗИ со скалярным критерием [2–5].

Таким образом, задача многокритериального выбора (1–2) обобщает обычную задачу выбора на случай $m > 1$, обеспечивая более адекватное представление реальной задачи выбора варианта СЗИ. В качестве частных критериев могут рассматриваться, например, интегральный риск $q_1(\vec{X}) = R_S(\vec{X})$, затраты на реализацию механизмов защиты $q_2(\vec{X}) = C_S(\vec{X})$, производительность РВС $q_3(\vec{X}) = G_S(\vec{X})$ и др.

Методика решения многокритериальных задач включает в себя два основных этапа [6]: построение множества Парето – оптимальных решений; выбор одного оптимального решения из множества Парето – оптимальных решений. Построение множества Парето является достаточно трудной и в то же время чрезвычайно важной задачей.

Для наглядности рассмотрим алгоритмы построения множества Парето при $m = 2$.

Множество Парето представляет собой юго-западную (для задач минимизации) границу множества альтернатив. Найти множество Парето в этом случае можно методом последовательного приближения (см. рис. 1), используя линейную (кусочно-линейную, полиэдральную) аппроксимацию, когда приближение осуществляется отрезками прямых и в результате получают ломаную линию, точки изломов которой принадлежат аппроксимируемой кривой.

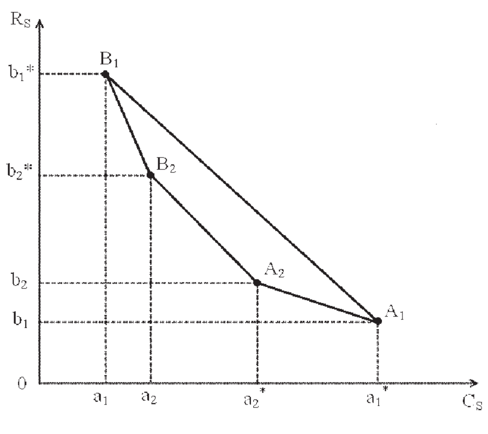

Рис. 1. Юго-западная граница множества альтернатив

Алгоритм решения сводится к следующему:

1 шаг. Полагают $C(\vec{X}) = a_1$; $R_S(\vec{X}) = b_1$, где a_1, b_1 принадлежат множеству оценок и $\vec{X} \in D$ – множество альтернатив.

2 шаг. Решают оптимизационные задачи

$$C(\vec{X}) \to \min; \vec{X} \in D, R_S(\vec{X}) = b_1$$

и

$$R_S(\vec{X}) \to \min; \vec{X} \in D, C(\vec{X}) = a_1 .$$

Решения этих задач позволяют получить соответственно точки $A_1(a_1^*, b_1)$ и $B_1(a_1, b_1^*)$, лежащие на множестве Парето.

3 шаг. Через точки A_1 и B_1 проводят прямую, которая и будет первым приближением множества Парето.

4 шаг. Второе приближение получают после решения очередных двух оптимизационных задач при выборе других точек из множества оценок b_2 и a_2:

$$C(\vec{X}) \to \min; \vec{X} \in D, R_S(\vec{X}) = b_2;$$

$$R_S(\vec{X}) \to \max; \vec{X} \in D, C(\vec{X}) = a_2$$

что дает точки $A_2(a_2^*, b_2)$ и $B_2(a_2, b_2^*)$.

5 шаг. Ломаная $A_1A_2B_2B_1$ является вторым приближением множества Парето.

6 шаг. При необходимости получения более точного результата, например, между точками B_1 и B_2, задача решается аналогично, то есть на отрезке (a_1, a_2) выбирают новое значение для $C(\vec{X})$, а на отрезке (b_2^*, b_1^*) – новое значение $R_S(\vec{X})$ и решаются две оптимизационные задачи как в на шаге 2 и шаге 4 и т. д.

Рассмотрим алгоритм построения множества Парето на основе метода взвешенной суммы [7]. Этот метод основан на том, что если частные критерии $R_S(\vec{X})$ и $C_S(\vec{X})$ являются линейными функциями, то координату j-ой точки множества Парето определяет совокупность чисел R_S, C_S, получаемых из решения задачи оптимизации вида

$$\alpha_1 R_S(\vec{X}) + \alpha_2 C_S(\vec{X}) \to \min_{\vec{X}};$$

$$\alpha_1 + \alpha_2 = 1; \alpha_1, \alpha_2 > 0.$$

Отсюда следует, что, во-первых, существуют такие $\vec{\alpha} = (\alpha_1, \alpha_2)$, для которых все точки $\vec{X}$ эффективны и дают один и тот же данный не улучшаемый вектор результатов; во-вторых, изменяя $\vec{\alpha} = (\alpha_1, \alpha_2)$, получаем все множество.

Тогда алгоритм аппроксимации множества Парето можно реализовать следующим способом (см. рис. 2):

1 шаг. Решаем задачу

$$\alpha_1 R_S(\vec{X}) + \alpha_2 C_S(\vec{X}) \to \min_{\vec{X}};$$

$$\alpha_1 + \alpha_2 = 1; \alpha_1, \alpha_2 > 0,$$

из которой находят первую точку $A(C_S(\vec{X}), R_S(\vec{X}))$.

2 шаг. Вторую точку $B(C_S(\vec{X}), R_S(\vec{X}))$ получают решением задачи

$$\alpha_1' R_S(\vec{X}) + \alpha_2' C_S(\vec{X}) \to \min_{\vec{X}};$$

$$\alpha_1' + \alpha_2' = 1; \alpha_1', \alpha_2' > 0.$$

Прямая AB есть первое приближение множества Парето. Аналогично можно построить точку C, тогда ломаная ACB представляет собой второе приближение и т. д. Рассмотренный способ аппроксимации множества Парето основан на исследовании агрегированного (интегрального) критерия. Следует отметить, что, увеличивая количество точек, можно построить многогранник, аппроксимирующий выпуклое множество Парето с любой степенью сложности.

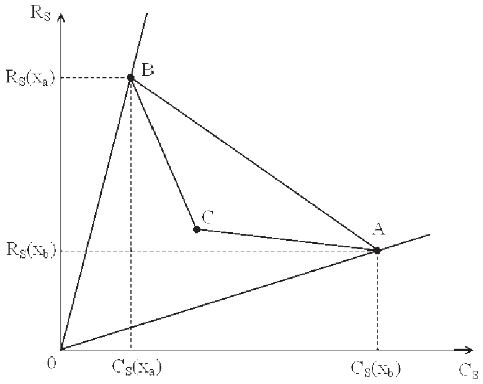

Рис. 2. Аппроксимация множества Парето

После получения множества Парето необходимо выбрать оптимальное решение. Для этого требуется принять соглашение о возможных (целесообразных) компромиссах между критериями. Это – акция ЛПР и она во многом определяется особенностями задачи, опытом и интуицией ЛПР.

Один из путей реализации такого соглашения – скаляризация задачи. В этом случае приходим к однокритериальной задаче оптимизации на множестве Парето. Казалось бы, в финале получено то, от чего отказались в начале. Однако это не так, поскольку при формировании множества Парето отброшены все заведомо худшие в смысле многокритериальной оптимизации варианты и предельно сужена область поиска.

На рис. 3 изображено множество Парето оптимальных решений найденное с использованием рассмотренного выше подхода. Для решения задач оптимизации использовался метод вектора спада [6].

Точки множества Парето представлены на рисунке 3 треугольниками. На оси абсцисс показаны затраты на реализацию механизмов защиты, а по оси ординат отложены значения возможного ущерба.

Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры инновационной России на 2009-2013 годы».

СПИСОК ЛИТЕРАТУРЫ

1. *Петренко С.А.* Управление информационными рисками / С.А. Петренко, С.В. Симонов. М.: ДМК Пресс. 2004. – С. 384.

2. *Кащенко А.Г.* Математические модели для выбора комплекса средств защиты информации в автоматизированных системах /А.Г. Кащенко // Кибернетика и высокие технологии XXI века: матер.

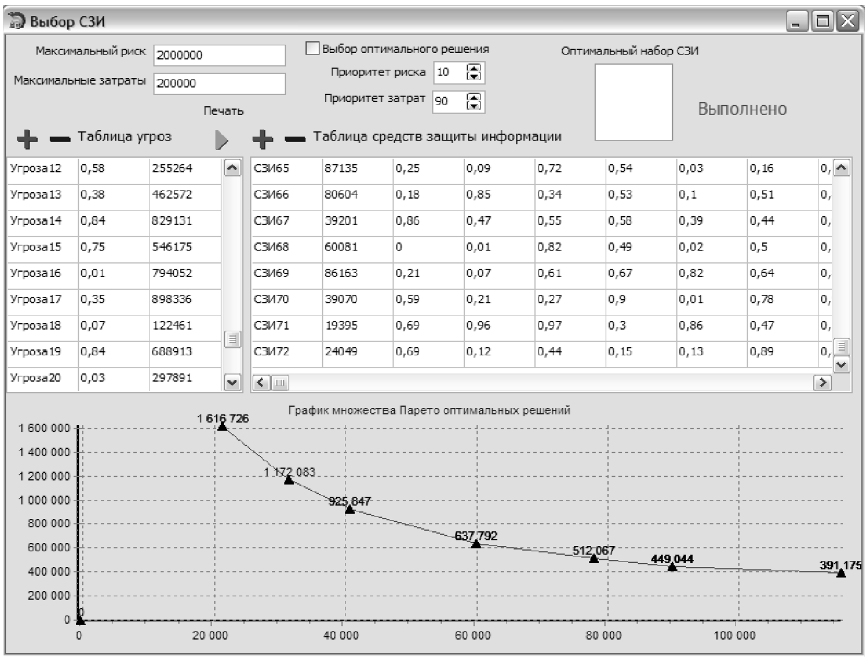

Рис. 3. Пример работы программы

науч. конф. 13 – 15 мая 2008 г. – Воронеж. 2008. – С. 876 – 888.

3. *Гагарина Л.Г.* Методические основы выбора средств защиты информации на базе алгоритмов дискретного программирования для создания информационного хранилища данных / Л.Г. Гагарина, Е.Г. Дорогова, Т.Н. Маклакова // Вопросы защиты информации. – Москва, 2006. Вып. 2. – С. 40–41.

4. *Дидюк Ю.Е.* Методика выбора комплекса средств защиты информации в автоматизированных системах / Ю.Е. Дидюк // Информация и безопасность: регион. научно – техн. журнал. – Воронеж, 2006. Вып. 2. – С. 45–47.

5. *Овчинников А.И.* Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия / А.И. Овчинников, А.М. Журавлев, Н.В. Медведев, А.Ю. Быков // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение», 2007. № 3. – С. 115 – 121.

6. *Черноруцкий И.Г.* Методы принятия решений / И.Г. Черноруцкий. – СПб.: БХВ – Петербург, 2005. – 416 с.

7. *Моисеев Н.Н.* Математические методы системного анализа / Н.Н. Моисеев. – М.: Наука, 1981. – 488 с.

8. *Сергиенко И.В.* Приближенные методы решения дискретных задач оптимизации / И.В. Сергиенко, Т.Т. Лебедева, В.А. Рощин. – Киев : Наук. думка, 1980. – 276 с.

Кащенко Алексей Геннадиевич – начальник бюро ЗАО «Воронежстальмост». E-mail: alexeykg@yandex.ru

Kashchenko Alex G. – Head Office of JSC «Voronezhstalmost». E-mail: alexeykg@yandex.ru