УДК 004.056 : 519.85

А.Ю. Быков, Ф.А. Панфилов, Д.В. Шмырев

ЗАДАЧА ВЫБОРА СРЕДСТВ ЗАЩИТЫ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ С УЧЕТОМ КЛАССОВ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Рассмотрена задача выбора средств защиты от несанкционированного доступа к информации в автоматизированной системе: выполнена математическая постановка задачи в виде задачи линейного программирования с булевыми переменными. В математической постановке введен показатель стоимости средств защиты. Ограничения задачи учитывают требования классов защищенности от несанкционированного доступа в автоматизированных системах. Рассмотрен пример постановки задачи и подходы к ее решению.

E-mail: abykov@bmstu.ru

Ключевые слова: *защита информации, средства защиты информации, несанкционированный доступ, класс защищенности.*

Для обеспечения защищенности автоматизированных систем (АС) от несанкционированного доступа (НСД) к информации можно использовать различные постановки задач выбора средств защиты и планирования решения заданий [1–3].

В работе [2] представлена модель планирования комплекса заданий в вычислительной сети с учетом требований защиты информации, основанная на линейных дифференциальных уравнениях. В статье [3] предложена математическая постановка задачи выбора средств защиты для вычислительной сети в виде задачи булевого программирования. Однако в приведенных математических моделях не учитываются классы защищенности АС от НСД к информации, определенные в работе [4].

Рассмотрим математическую постановку задачи, учитывающую требования классов защищенности АС от НСД при выборе средств защиты.

Исходные данные. 1. $K = \{k_1, k_2, ..., k_l\}$ – множество классов защищенности от НСД, $L = \{1, 2, ..., l\}$ – множество индексов классов защищенности. В руководящем документе [4] введено девять классов защищенности.

2. $Tr = \{Tr_1, Tr_2, ..., Tr_m\}$ – множество требований к классам защищенности от НСД, определенных в работе [4]; $M = \{1, 2, ..., m\}$ – множество индексов требований.

3. $S = \{S_1, S_2, ..., S_n\}$ – множество средств защиты информации (СЗИ), $N = \{1, 2, ..., n\}$ – множество индексов СЗИ.

4. $A = \|a_{ij}\|, i \in M, j \in L$ – булева матрица размерности $m \times l$, задающая требования к классам защищенности, $a_{ij} = 1$, если для *j*-го класса защищенности должно быть обязательно выполнено *i*-е требование, $a_{ij} = 0$ – в противном случае.

5. $B = \|b_{ij}\|, i \in N, j \in M$ – булева матрица размерности $n \times m$, задающая параметры средств защиты для обеспечения выполнения требований классов защищенности от НСД, $b_{ij} = 1$, если *i*-е средство защиты обеспечивает выполнение *j*-го требования, $b_{ij} = 0$ – в противном случае.

6. $C = \|c_1, c_2, ..., c_n\|^T$ – вектор, содержащий «стоимости» СЗИ. Здесь понятие «стоимость» может иметь более широкий смысл, чем цена в рублях или условных единицах. Можно оценивать «стоимость» СЗИ в ресурсах вычислительных средств, затрачиваемых на обеспечение функций защиты, для программных СЗИ, или в энергозатратах – для технических средств и т.п. Следует учесть, что некоторые программные средства, такие, как операционные системы (ОС), системы управления базами данных (СУБД) и другие обладают встроенными сертифицированными механизмами защиты. Если данные средства будут использованы, исходя из функционального назначения АС, и предполагается использование встроенных механизмов защиты, то в этом случает можно считать, что стоимость средства защиты равна нулю, так как программное средство в любом случае используется для решения задач в АС, не связанных с защитой от НСД.

7. $D = \|d_{ij}\|, i \in N, j \in L$ – булева матрица размерности $n \times l$, задающая разрешения на использование СЗИ для классов защищенности от НСД, исходя из наличия сертификатов у данных средств защиты, $d_{ij} = 1$, если *i*-е средство защиты разрешается использовать в АС, удовлетворяющих *j*-му классу защищенности (имеется сертификат), $d_{ij} = 0$ – в противном случае.

8. k – индекс класса защищенности от НСД, требованиям которого должна удовлетворять АС.

Показатель качества выбора средств защиты. Введем булеву переменную $x_i \in \{0,1\}$, $\forall i \in N$. Значения переменной определяются следующим образом:

- $x_i = 1$, если *i*-е средство защиты будет применяться в АС для защиты от НСД;
- $x_i = 0$, в противном случае.

Тогда $\boldsymbol{X}$ – вектор булевых переменных $x_i, \forall i \in N$.

Введем показатель стоимости выбранных СЗИ:

$$C(\boldsymbol{X}) = \sum_{i=1}^{n} c_i x_i. \qquad (1)$$

Значение данного показателя необходимо минимизировать.

Ограничения. Ограничения на то, что должны быть выполнены все требования, определенные для *k*-го класса защищенности от НСД к информации в руководящем документе [4], причем выполнение данных требований должны обеспечивать средства защиты, имеющие сертификат для этого класса защищенности, имеют вид

$$\sum_{i=1}^{n} b_{ij} d_{ik} x_i \geq 1, \; \exists j \in M, \; a_{jk} = 1. \qquad (2)$$

Постановка задачи. Постановка задачи может быть представлена следующим образом:

$$C(\boldsymbol{X}) = \sum_{i=1}^{n} c_i x_i \to \min_{\overline{X} \in \Delta_{\text{доп}}},$$

$$\Delta_{\text{доп}} : \left\{ \sum_{i=1}^{n} b_{ij} d_{ik} x_i \geq 1, \; \exists j \in M, \; a_{jk} = 1, \right.$$

где $\Delta_{\text{доп}}$ – множество допустимых альтернатив (значений компонент неизвестного вектора $\boldsymbol{X}$), заданное системой неравенств.

Решение задачи – нахождение всех неизвестных компонент вектора $\boldsymbol{X}$ и выбор тех средств защиты $s_i (\forall i \in N)$, для которых компонента вектора $x_i (\forall i \in N)$ равна 1.

Поставленная задача является задачей линейного булевого программирования.

Практическая постановка задачи и численные расчеты. Для демонстрации использования приведенной математической

постановки задачи рассмотрим небольшой фрагмент исходных данных.

Проанализируем требования, предъявляемые только к подсистеме управления доступом, определенные в [4]. Эти требования представлены в табл. 1, в которой, по сути, приведен фрагмент матрицы исходных данных – A (в табл. 1 представлено 11 требований, в работе [4] задано более 60 подобных требований к различным подсистемам).

Требуется обеспечить класс защищенности 1В (класс с индексом 7). В этом случае важны только значения элементов 7-го столбца матрицы D- d_{i7}, $\forall i \in N$. Параметры некоторых средств защиты для обеспечения выполнения требований из табл. 1 (фрагмент матрицы B), их класс защищенности от НСД в соответствии с сертификатом и значения элементов d_{i7}, $\forall i \in N$ столбца матрицы D, а также примерные стоимости средств защиты (вектор C) представлены в табл. 2. Представленные цены задают конфигурацию средств защиты для АС на основе локальной вычислительной сети с одним сервером и 20 рабочими местами.

При заданных исходных данных (индексы переменной x соответствуют номерам средств, представленных в табл. 2). Показатель качества (1) имеет вид:

$$C(\boldsymbol{X}) = \sum_{i=1}^{n} 0x_1 + 0x_2 + 155000x_3 + 300000x_4 + 160000x_5 + 180000x_6.$$

Для класса защищенности 1В должны быть выполнены требования из табл. 1 с номерами: 2, 5, 8, 10, 11 (в матрице A соответствующий элемент $a_{jk} = 1$). Каждому такому требования согласно (2) соответствует свое ограничение в виде неравенства. На основе значений элементов матрицы B и элементов d_{i7}, $\forall i \in N$, столбца матрицы D, представленных в табл. 2, ограничения имеют вид:

- для требования № 2: $x_3 + x_5 + x_6 \geq 1$;
- для требования № 5: $x_3 + x_5 \geq 1$, (предыдущее неравенство для требования № 2 можно исключить, так как оно следует из данного неравенства);
- для требования № 8: $x_3 + x_5 \geq 1$ (неравенство можно исключить, совпадает с требованием № 5);
- для требования № 10: $x_3 + x_5 \geq 1$ (неравенство можно исключить, совпадает с требованием № 5);
- для требования № 11: $x_3 + x_5 \geq 1$.

Таблица 1

Требования к подсистеме управления доступом (фрагмент матрицы исходных данных A)

Требование		Класс и его индекс								
		3Б 1	3А 2	2Б 3	2Б 4	1Д 5	1Г 6	1В 7	1Б 8	1А 9
Идентификация и аутентификация при входе в систему										
1	По паролю условно-постоянного действия (6 символов)	1	1	0	0	1	0	0	0	0
2	По идентификатору и паролю условно-постоянного действия (6 символов)	0	0	1	1	0	1	1	0	0
3	По идентификатору и паролю условно-постоянного действия (8 символов)	0	0	0	0	0	0	0	1	0
4	По биометрическим характеристикам или специальным устройствам и паролю временного действия не менее 8 символов	0	0	0	0	0	0	0	0	1
Идентификация терминалов ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ										
5	По их логическим адресам	0	0	0	1	0	1	1	0	0
6	По физическим адресам	0	0	0	0	0	0	0	1	0
7	Аппаратурная по уникальным встроенным устройствам	0	0	0	0	0	0	0	0	1
Идентификация программ, томов, каталогов, файлов, записей, полей записей										
8	По их именам	0	0	0	1	0	1	1	1	1
9	По контрольным суммам	0	0	0	0	0	0	0	0	1
10	Контроль доступа к защищаемым ресурсам в соответствии с матрицей доступа	0	0	0	0	0	1	1	1	1
11	Управление потоками информации с помощью меток конфиденциальности	0	0	0	0	0	0	1	1	1

Таблица 2

Параметры средств защиты от НСД

Средство защиты		Номер требований классов защищенности в соответствии с табл. 1											Класс защищенности и $d_{i7},\ \forall i \in N$	Стоимость, руб.
		1	2	3	4	5	6	7	8	9	10	11		
1	Типовая ОС	1	1	1	0	1	0	0	1	0	1	0	1Г $d_{17} = 0$	0 (используется в любом случае)
2	Встроенные средства защиты типовой СУБД	1	1	1	0	0	0	0	0	0	0	0	1Г $d_{27} = 0$	0 (используется в любом случае)
3	Система защиты от НСД № 1	1	1	1	1	1	1	0	1	0	1	1	1Б $d_{37} = 1$, так как СЗИ с сертификатом для класса 1Б разрешено использовать для класса 1В	155 000
4	Комплекс СЗИ НСД	1	1	1	0	1	0	0	1	0	1	0	1Г $d_{47} = 0$	300 000
5	Система защиты информации от НСД № 2	1	1	1	1	1	1	0	1	0	1	1	1Б $d_{57} = 1$	160 000
6	Программно-аппаратный комплекс средств защиты компьютера	1	1	1	1	0	0	0	0	0	0	0	1Б $d_{67} = 1$	180 000

Таким образом, для представленного фрагмента исходных данных постановка задачи имеет следующий вид:

$$C(\boldsymbol{X}) = \sum_{i=1}^{n} 0x_1 + 0x_2 + 155000x_3 + 300000x_4 + 160000x_5 +$$

$$+180000x_6 \to \min_{\bar{X} \in \Delta_{\text{доп}}};$$

$$\Delta_{\text{доп}} : \{ x_3 + x_5 \geq 1.$$

При таких исходных данных задача может быть решена «вручную», в соответствии с ограничением для того, чтобы выполнить заданные требования необходимо выбрать средство защиты № 3 или 5, но стоимость средства № 3 ниже, чем № 5. Таким образом, получаем решение, $x_3 = 1$, все остальные компоненты равны 0. Стоимость решения 155 000 рублей.

Если использовать реальные исходные данные, то может быть получена задача булевого программирования большой размерности. В этом случае следует применять методы булевого программирования, один из подобных методов – метод вектора спада рассмотрен в работе [5].

СПИСОК ЛИТЕРАТУРЫ

1. Домарев В. В. Безопасность информационных технологий: Методология создания систем защиты. – Киев: Диасофт, 2002. – 688 с.
2. Быков А. Ю. Планирование выполнения комплекса заданий в распределенной вычислительной системе с обеспечением защиты информации // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. – 2001. – № 2. – С. 93–105.
3. Овчинников А. И., Журавлев А. М., Медведев Н. В., Быков А.Ю. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение.– 2007. – № 3. – С. 115–121.
4. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации // Сб. руководящих документов по защите информации от НСД. – М.: Гостехкомиссия России, 1998. – С. 23–52.
5. Овчинников А. И., Медведев Н. В., Быков А. Ю. Применение метода вектора спада для решения задачи поиска вариантов защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение.– 2008. – № 2. – С. 73–82.

Статья поступила в редакцию 14.05.2012