УДК 004.5:519.854.33

А. И. Овчинников, А. М. Журавлев,
Н. В. Медведев, А. Ю. Быков

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПТИМАЛЬНОГО ВЫБОРА СРЕДСТВ ЗАЩИТЫ ОТ УГРОЗ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Рассмотрена задача оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия: выполнена математическая постановка задачи, обозначены основные этапы ее решения. Математическая постановка задачи выполнена для оптимизации двух показателей качества: максимизации возможного среднего предотвращенного ущерба при ограничении на затраты; минимизации затрат при ограничении на возможный средний предотвращенный ущерб. Задача оптимального выбора средств защиты представляет собой задачу булева нелинейного программирования, для решения которой можно применить оптимизационно-имитационный подход.

Информационная безопасность — один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере приводят к гибельным последствиям для бизнеса любой компании. Применение высоких информационных технологий XXI в., 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, т. е. проблема информационных рисков и нахождения путей снижения ущерба становится с каждым годом все острее.

Уязвимость распределенных вычислительных систем существенно превышает уязвимость автономных компьютеров. Это связано, прежде всего, с открытостью, масштабностью и неоднородностью самих компьютерных сетей. Существует немало способов атак на современные компьютерные сети [1, 2]. При этом число угроз информационно-компьютерной безопасности и способов их реализации постоянно увеличивается. Основными причинами здесь являются недостатки современных информационных технологий, а также неуклонный рост сложности программно-аппаратных средств.

Для эффективного решения задачи защиты информации в вычислительной сети необходим тщательный анализ всех возможных угроз информационной безопасности, что позволит своевременно принять

меры для противодействия угрозам. При анализе угрозы необходимо оценить возможность ее проявления, а также ущерб, который будет нанесен предприятию в случае непредотвращения угрозы.

Для противодействия одной и той же угрозе обычно существует несколько средств защиты, которые выпускаются разными производителями, различаются по стоимости реализации и обеспечивают различную возможность предотвращения угроз.

В простейшем случае можно предположить, что каждое средство защищает ровно от одной угрозы. Тогда задача оптимального выбора вариантов защиты представляет собой задачу булева программирования, для решения которой разработано множество алгоритмов [3–5]. К сожалению, указанное предположение не соответствует реальным условиям, по которым развивается рынок средств информационной безопасности, поэтому построим математическую модель, соответствующую реальному положению дел, т.е. когда каждое средство защиты противодействует произвольному числу угроз, причем возможность предотвращения каждой угрозы разная.

Исходные данные. 1. $A = \{a_1, a_2, \ldots, a_n\}$ — множество возможных угроз безопасности, $N = \{1, 2, \ldots, n\}$ — множество индексов угроз.

2. $B = \{b_1, b_2, \ldots, b_m\}$ — множество средств защиты от угроз безопасности, $M = \{1, 2, \ldots, m\}$ — множество индексов вариантов защиты.

3. $T = [t_0, t_{\max}]$ — рассматриваемый период функционирования.

4. $p_i, \forall i \in N, p_i \in [0, 1]$ — возможность (вероятность) проявления i-й угрозы на интервале T, определяется по данным средств или с помощью экспертов.

5. $u_i, \forall i \in N$ — средний ущерб от возможного непредотвращения i-й угрозы.

6. $c_j, j \in M$ — стоимость j-го средства защиты.

7. $v_{ij}, \forall i \in N, j \in M, v_{ij} \in [0, 1]$ — возможность (вероятность) предотвращения последствий i-й угрозы с помощью j-го средства защиты, определяется по данным статистики или с помощью экспертов.

Постановка задачи возможна в двух вариантах:

— максимизация возможного среднего предотвращенного ущерба при ограничении на затраты;

— минимизация затрат при ограничении на возможный средний предотвращенный ущерб.

Максимизация возможного предотвращенного ущерба при ограничении на затраты. Введем булеву переменную $x_j \in \{0, 1\}$, $\forall j \in M$:

$x_j = 1$, если j-е средство защиты будет применяться в вычислительной сети для защиты от тех или иных угроз;

$x_j = 0$ в противном случае, т.е. если j-е средство не применяется.

Тогда $\overrightarrow{X}$ — вектор булевых переменных $x_j, \forall j \in M$.

Введем следующий показатель качества выбора средств защиты от угроз безопасности:

$$U\left(\overrightarrow{X}\right) = \sum_{i \in N} u_i p_i \max_{j \in M}(v_{ij} x_j). \tag{1}$$

Данный показатель имеет смысл возможного среднего предотвращенного ущерба при использовании средств защиты, определяемых вектором $\overrightarrow{X}$, его значение необходимо максимизировать при следующем ограничении:

$$\sum_{j \in M} c_j x_j \leqslant C. \tag{2}$$

Этим условием ограничивается стоимость выбранных средств защиты от угроз безопасности, где C — максимально возможные затраты, выделенные на защиту от угроз безопасности.

Итоговое выражение математической постановки задачи при условии максимизации возможного среднего предотвращенного ущерба при ограничении на затраты имеет вид

$$\begin{aligned} &U(\overrightarrow{X}) = \sum_{i \in N} u_i p_i \max_{j \in M}(v_{ij} x_j) \to \max_{\overrightarrow{X} \in \Delta^{\text{доп}}}; \\ &\Delta^{\text{доп}} : \sum_{j \in M} c_j x_j \leqslant C, \end{aligned} \tag{3}$$

где $\Delta^{\text{доп}}$ — множество допустимых альтернатив (значений компонент) неизвестного вектора $\overrightarrow{X}$.

Решение задачи сводится к нахождению всех неизвестных компонентов вектора $\overrightarrow{X}$ и выбору тех средств защиты b_j, для которых компонент вектора $x_j (\forall j \in M)$ равен 1.

Минимизация затрат при ограничении на возможный средний предотвращенный ущерб. По аналогии с предыдущей постановкой задачи введем булеву переменную $x_j \in \{0, 1\}, \forall j \in M$:

$x_j = 1$, если j-е средство защиты будет использоваться;

$x_j = 0$ в противном случае, т.е. если j-е средство защиты не используется.

Тогда $\overrightarrow{X}$ — вектор булевых переменных $x_j, \forall j \in M$.

Введем следующий показатель стоимости вариантов защиты от угроз безопасности:

$$C(\overrightarrow{X}) = \sum_{j \in M} c_j x_j. \tag{4}$$

Значение данного показателя необходимо минимизировать при ограничении

$$\sum_{i\in N} u_i p_i \max_{j\in M}(v_{ij}x_j) \geqslant U_{zad}, \tag{5}$$

чтобы возможный средний предотвращенный ущерб был не меньше заданного, где U_{zad} — заданное значение возможного среднего предотвращенного ущерба.

Итоговое выражение математической постановки задачи при условии минимизации затрат при ограничении на возможный средний предотвращенный ущерб имеет вид

$$\begin{gathered} C(\overrightarrow{X}) = \sum_{j\in M} c_j x_j \to \min_{\overrightarrow{X}\in\Delta^{\text{доп}}}; \\ \Delta^{\text{доп}} : \sum_{i\in N} u_i p_i \max_{j\in M}(v_{ij}x_i) \geqslant U_{zad}. \end{gathered} \tag{6}$$

Решение задачи — нахождение всех неизвестных компонент вектора $\overrightarrow{X}$ и выбор тех средств защиты b_j, для которых соответствующая компонента вектора x_j равна 1.

Практическая постановка задачи. Для демонстрации использования приведенной математической постановки задачи рассмотрим небольшой пример, показывающий практическое применение изложенных идей в предлагаемой модели на основе рассмотрения трех угроз безопасности и пяти средств защиты. В реальных системах число угроз и возможных средств защиты может достигать нескольких десятков, а если рассматривать дополнительно организационно-технические методы защиты, то число средств защиты может превышать 100.

Рассматриваемый период функционирования $T = 1$ год.

В табл. 1 приведены три типовые угрозы вычислительной сети предприятия (реально их намного больше). Возможности проявления угроз выбраны на основе статистических исследований. Данные о среднем ущербе от возможного непредотвращения угроз безопасности сильно зависят от специфики деятельности компании и выбраны на основе некоторых средних показателей для типового предприятия.

В табл. 2 приведены, для примера, пять средств защиты от угроз безопасности. Стоимость реализации средств защиты выбрана на основе предположения о наличии в компании 250 рабочих станций и 5 файловых серверов. Данные о стоимости лицензий взяты с сайта компании SoftLine. Возможность предотвращения угроз выбрана на основе экспертных оценок.

Рассмотрим пример постановки задачи на основе минимизации затрат при ограничениях на возможный средний предотвращенный

Таблица 1

Возможности проявления угроз безопасности и ущерб от их непредотвращения на интервале времени один год

Угроза	Возможность проявления	Возможный ущерб от не предотвращения, руб.
Несанкционированное вторжение в сеть	0,6	1 000 000
Вирусная атака	0,9	200 000
Утечка конфиденциальной информации	0,8	1 500 000

Таблица 2

Средства защиты от угроз безопасности, стоимости из реализации и возможности предотвращения угроз на интервале времени один год

Средство защиты	Стоимость реализации, руб.	Возможность предотвращения угрозы		
		несанкционированного вторжения в сеть	вирусной атаки	утечки конфиденциальной информации
Kaspersky Anti-Virus	110841	0	0,8	0
Инфосистемы Джет Z-2	258375	0,7	0,4	0
Symantec Antivirus Enterprise	290000	0	0,9	0,7
Outpost Network Security	182061	0,8	0,5	0,6
Kerio WinRoute Firewall	79000	0,7	0,3	0,7

ущерб (нумерация угроз и средств защиты используется, как в табл. 1 и 2).

Показатель качества, который необходимо минимизировать, имеет вид

$$C(\overrightarrow{X}) = 110841x_1 + 258375x_2 + 290000x_3 + \\ + 182061x_4 + 79000x_5 \to \min_{\overrightarrow{X} \in \Delta^{\text{доп}}}.$$

Множество допустимых альтернатив определяется условием

$$\Delta^{доп}: 0{,}6 \times 1\,000\,000 \times \max(0x_1,\ 0{,}7x_2,\ 0x_3,\ 0{,}8x_4,\ 0{,}7x_5) + \\ + 0{,}9 \times 200\,000 \times \max(0{,}8x_1,\ 0{,}4x_2,\ 0{,}9x_3,\ 0{,}5x_4,\ 0{,}3x_5) + \\ +0{,}8\times 1\,500\,000 \times \max(0x_1,\ 0x_2,\ 0{,}7x_3,\ 0{,}6x_4,\ 0{,}7x_5) \geqslant 1500000(\text{руб.}),$$

где 1 500 000 (руб.) — ограничения на максимальный средний предотвращенный ущерб.

Цель данного примера — демонстрация того, какие данные необходимы для решения задачи оптимального выбора вариантов защиты

от угроз безопасности. Анализ всех существующих угроз безопасности и средств защиты не рассматривается в настоящей статье, поэтому приведенные данные не могут претендовать на полноту.

Заключение. Рассмотрена математическая постановка задачи оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия. Ввиду необходимости вычисления максимума в показателе качества (1) и ограничениях (5) для решения подобных задач не могут использоваться классические методы булева линейного программирования [3–5]. Разработка методов решения подобных задач является весьма непростой задачей. Для этого, в частности, может использоваться подход, предложенный в работе [6] и названный оптимизационно-имитационным. Суть данного подхода заключается в том, что если ограничения или показатель не могут быть явно вычислены (заданы в виде некоторой формулы), то для их расчета существует некоторая процедура, возможно приводящая к имитационному моделированию. В рамках данного подхода могут быть использованы модификации некоторых классических методов дискретной оптимизации. Например, некоторые модификации метода вектора спада позволяют решать задачи, для которых ограничения не могут быть явно заданы. В этом случае происходит переход от одного решения к другому для улучшения значения целевой функции, при этом допустимость решения проверяется с помощью отдельной процедуры.

В соответствии с постановкой задачи основными этапами ее решения являются:

— анализ угроз информационной безопасности;

— анализ рынка средств защиты от угроз;

— сбор и обработка информации о характеристиках угроз (возможности проявления и ущербе от непредотвращения);

— сбор и обработка информации о возможности предотвращения угроз различными средствами защиты;

— разработка алгоритмов оптимального выбора вариантов защиты.

В результате решения задачи будут найдены средства обеспечения информационной безопасности, которые позволят оптимально защитить вычислительную сеть предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Домарев В. В. Безопасность информационных технологий: Методология создания систем защиты. – Киев: Диасофт, 2002. – 688 с.
2. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 с.

3. Саати Т. Целочисленные методы оптимизации и связанные с ними экстремальные проблемы. – М.: Мир, 1973. – 302 с.
4. Alexander Schrijver. Theory of linear and integer programming // John Wiley and Sons, 1998. – 483 с.
5. David G. Luenberger. Introduction to Linear and Nonlinear Programming // Addison Wesley, 1984. – 491 с.
6. Цвиркун А. Д., Акинфиев В. И., Филимонов В. А. Имитационное моделирование в задачах синтеза структуры сложных систем: Оптимизационно-имитационный подход. – М.: Наука, 1985. – 173 с.

Статья поступила в редакцию 24.01.2007

Андрей Игоревич Овчинников родился в 1982 г., окончил МГТУ им. Н.Э. Баумана в 2005 г. Аспирант кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана.

A.I. Ovchinnikov (b. 1982) graduated from the Bauman Moscow State Technical University in 2005. Post-graduate of "Information Security" department of the Bauman Moscow State Technical University.

Алексей Михайлович Журавлев родился в 1981 г., окончил в 2003 г. Государственный университет управления и в 2006 г. аспирантуру на кафедре "Информационная безопасность" МГТУ им. Н.Э. Баумана. Специализируется в области безопасности компьютерных сетей.

A.M. Zhuravlyov (b.1981) graduated from the State University for Management in 2003. Specializes in the field of safety of computer networks.

Николай Викторович Медведев родился в 1954 г., окончил МВТУ им. Н.Э. Баумана в 1977 г. Канд. техн. наук, заведующий кафедрой "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор около 50 научных работ в области исследования и разработки защищенных систем автоматической обработки информации.

N.V. Medvedev (b. 1954) graduated from the Bauman Moscow Higher Technical School in 1977. Ph. D. (Eng.), head of "Information Security" department of the Bauman Moscow State Technical University. Author of about 50 publications in the field of study and development of protected systems for automatic data processing.

Александр Юрьевич Быков родился в 1969 г., окончил в 1991 г. ВИКИ им. А.Ф. Можайского. Канд. техн. наук, доцент кафедры "Информационная безопасность" МГТУ им. Н.Э. Баумана. Автор около 20 научных работ в области информационной безопасности и исследования систем обработки информации и управления.

A.Yu. Bykov (b. 1969) graduated from the Military Engineering Space Institute n.a. A.F. Mozhaiskii in 1991. Ph. D. (Eng.), assoc. professor of "Information Security" department of the Bauman Moscow State Technical University. Author of about 20 publications in the field of information security and study of systems of data processing and control.