DOI: http://dx.doi.org/10.21686/2413-2829-2021-1-173-178

МОДЕЛИРОВАНИЕ ЭКОНОМИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТА ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ НА ОСНОВЕ СИМПЛЕКС-МЕТОДА

В. А. Сизов
Российский экономический университет имени Г. В. Плеханова, Москва, Россия
А. А. Дрожкин
Группа компаний «МультиСофт», Москва, Россия

В сфере информационной безопасности всегда следует поддерживать необходимый уровень защищенности, что приводит к значительным финансовым затратам. Чем больше информации нужно защитить, тем больше средств необходимо потратить на ее защиту. Специалисту по информационной безопасности важно не только разрабатывать методику по улучшению состояния информационной системы, но и экономить денежные ресурсы. Для решения такого рода задач используются различные математические модели. Оптимизировать поставленную задачу позволяют методы линейного программирования. Линейное программирование – математическая дисциплина, посвященная теории и методам решения экстремальных задач на множествах *n*-мерного пространства, задаваемых системами линейных уравнений и неравенств. Такие математические модели нужно применять после оценки возможного ущерба при утечке информации. В качестве примера в данной статье авторами рассматривается задача оптимизации затрат компании. Чаще всего суммарные затраты можно записать в виде линейного уравнения. Вместе с тем существует несколько ограничений на определенный корень уравнения. Симплекс-метод позволяет быстро получить решение, не используя значительные технические мощности электронно-вычислительной техники.
Ключевые слова: линейная оптимизация, информационная безопасность, оптимизация затрат, линейное программирование.

MODELING ECONOMY OF INFORMATION SECURITY OF BUSINESS ENTITY BASED ON SIMPLEX-METHOD

Valery A. Sizov
Plekhanov Russian University of Economics, Moscow, Russia
Alexander A. Drozhkin
MultiSoft Group, Moscow, Russia

In the field of information security it is always necessary to support a required level of protection, which can cause serious financial costs. The more information you should protect, the more money you should spend on it. The expert on information security shall both develop methods aimed at improvement of information system condition and save funds. To resolve these tasks different mathematic models can be used, such as methods of linear programming. Linear programming is a mathematic subject dealing with theory and methods of resolving extreme tasks on sets of n-dimensional space given by systems of linear equations and inequalities. These mathematic models should be used after assessing a possible damage after information leakage. In the article the authors study the task of company cost optimization. In the majority of cases total costs can be written as a linear equation. At the same time there are some restrictions on a certain root of equation. Simplex-method provides an opportunity to find the solution without using considerable technical capacities of computing.
Keywords: linear optimization, information security, cost optimization, linear programming.

Поддержание необходимого уровня информационной безопасности всегда связано с затратами, поэтому специалисту по информационной безопасности при разработке методики улучшения состояния информационной системы необходимо также максимально экономить денежные средства.

Решение такого рода задач возможно с использованием методов линейного программирования. Симплекс-метод – один из методов линейного программирования, позволяющий найти решение линейного уравнения с определенными ограничениями. Метод динамического программирования позволяет среди множества возможных решений найти наиболее оптимальное.

В зависимости от объекта оптимизации специалисту необходимо создать математическую модель и подобрать один из алгоритмов метода решения.

Рассмотрим применение этих методов на примере оптимизации компании до 50 человек. В качестве возможных вариантов защиты рассмотрим DLP-системы, межсетевые экраны и антивирусное программное обеспечение (ПО).

Наиболее известные DLP-системы – InfoWatch Traffic Monitor, КИБ SearchInform, Falcongaze SecureTower. Необходимо оценить их по эффективности для внесения в модель. Решением задачи оценивая эффективности различных DLP-систем будет введение экспертной балльной системы, показанной в табл. 1. В скобках указана максимально возможная оценка в баллах.

Таблица 1

Оценка эффективности DLP-систем

DLP-система	Базовая защита (1)	Дополнительные функции защиты от внешних угроз (1)	Дополнительные функции защиты от внутренних угроз (1)	Легкость использования (5)	Надежность защиты (5)
InfoWatch Traffic Monitor	1	2	3	3	5
КИБ SearchInform	1	2	3	4	3
Falcongaze SecureTower	1	2	3	2	2

Следующее средство защиты – межсетевые экраны. Самыми популярными производителями межсетевых экранов (по версии Gatner) являются Check Point Software Technologies, Fortinet и Palo Alto Networks. Межсетевые экраны могут быть для защиты как от внешних (табл. 2), так и от внутренних (табл. 3) угроз.

Таблица 2

Оценка межсетевых экранов для защиты от внешних угроз

Межсетевые экраны	Базовая защита (1)	Дополнительные функции защиты от внешних угроз (1)	Дополнительные функции защиты от внутренних угроз (1)	Легкость использования (5)	Надежность защиты (5)
Check Point Software Technologies	1	0	2	3	5
Fortinet	1	0	2	4	3
Palo Alto Networks	1	0	2	2	2

Таблица 3

Оценка межсетевых экранов для защиты от внутренних угроз

Межсетевые экраны	Базовая защита (1)	Дополнительные функции защиты от внешних угроз (1)	Дополнительные функции защиты от внутренних угроз (1)	Легкость использования (5)	Надежность защиты (5)
Check Point Software Technologies	1	2	0	3	5
Fortinet	1	2	0	4	3
Palo Alto Networks	1	2	0	2	2

Лидерами на рынке антивирусного программного обеспечения в России являются Kaspersky Anti-Virus, ESET NOD32 и Dr.Web для Windows (табл. 4).

Таблица 4

Оценка антивирусного программного обеспечения

Антивирусное ПО	Базовая защита (1)	Дополнительные функции защиты от внешних угроз (1)	Дополнительные функции защиты от внутренних угроз (1)	Легкость использования (5)	Надежность защиты (5)
Kaspersky Anti-Virus	1	2	3	4	5
ESET NOD32	1	2	3	5	4
Dr.Web для Windows	1	2	3	4	4

Для полноценной модели следует определить стоимость каждого средства защиты (табл. 5).

Таблица 5

Стоимость средств защиты информационной системы

Название	Стоимость, тыс. руб.
InfoWatch Traffic Monitor	5 000
КИБ SearchInform	4 000
Falcongaze SecureTower	4 300
Check Point Software Technologies	1 500
Fortinet	1 600
Palo Alto Networks	1 800
Kaspersky Anti-Virus	114
ESET NOD32	97
Dr.Web для Windows	112

Все входные данные определены. Сформулируем задачу в соответствии с введенной математической моделью. Предположим, что мы ищем оптимальное решение и в деньгах не ограничены ($Z_0 = 0$):

$$Z = \sum_{i=1}^{9} c_i \cdot x_i \to \min,$$

где c – коэффициент целевой функции;

x – базисная переменная;

i – порядковый номер переменной.

Таким образом,

$$Z = \begin{pmatrix} 5000 \\ 4000 \\ 4300 \end{pmatrix} \cdot x_{1\ldots3} + \begin{pmatrix} 1500 \\ 1600 \\ 1800 \end{pmatrix} \cdot x_{4\ldots6} + \begin{pmatrix} 114 \\ 97 \\ 112 \end{pmatrix} \cdot x_{7\ldots9}.$$

Ограничениями являются:

– защита от внешних угроз (по группам):

$x_{1\ldots3} \geq 1$,

$x_{4\ldots6} \geq 1$,

$q_i \cdot x_{1\ldots3} \geq 5$,

$q_i \cdot x_{4\ldots6} \geq 6$,

$q_i \cdot x_{7\ldots9} \geq 6$;

– защита от внутренних угроз:

$x_{1...3} \geq 1$,

$x_{4...6} \geq 1$,

$g_1 \cdot x_{1...3} \geq 7$,

$g_2 \cdot x_{4...6} \geq 4$,

$g_i \cdot x_{7...9} \geq 6$,

где q – эффективность i-го средства защиты от внутренних угроз;

g – эффективность защиты от внешних угроз.

Необходимо преобразовать все уравнения в канонический вид. Для этого следует изменить уравнения ограничения:

– внешние угрозы:

$14 \cdot x_1 + 13 \cdot x_2 + 10 \cdot x_3 \geq 15$,

$11 \cdot x_4 + 10 \cdot x_5 + 7 \cdot x_6 \geq 18$,

$15 \cdot x_7 + 15 \cdot x_8 + 14 \cdot x_9 \geq 18$,

$x_1, x_2, x_3 \geq 1$; $x_4, x_5, x_6 \geq 1$;

– внутренние угрозы:

$14 \cdot x_1 + 13 \cdot x_2 + 10 \cdot x_3 \geq 21$,

$11 \cdot x_4 + 10 \cdot x_5 + 7 \cdot x_6 \geq 12$,

$15 \cdot x_7 + 15 \cdot x_8 + 14 \cdot x_9 \geq 18$,

$x_1, x_2, x_3 \geq 1$; $x_4, x_5, x_6 \geq 1$;

Целевая функция будет выглядеть следующим образом:

$$Z = 5\,000 \cdot x_1 + 4\,000 \cdot x_2 + 4\,300 \cdot x_3 + \\ + 1\,500 \cdot x_4 + 1\,600 \cdot x_5 + 1\,800 \cdot x_6 + 114 \cdot x_7 + \\ + 97 \cdot x_8 + 112 \cdot x_9.$$

Воспользуемся модулем MATLAB – Optimization Toolbox. Функция linprog позволяет решить задачу оптимизации двойственным симплекс-методом (универсальным симплекс-методом) (рис. 1 и 2).

```
F = [5000,4000,4300,1500,1600,1800,114,97,112];
%F=-F;
A = [[14,13,10,0,0,0,0,0,0]
     [0,0,0,11,10,7,0,0,0]
     [0,0,0,0,0,0,15,15,14]
     [14,13,10,0,0,0,0,0,0]
     [0,0,0,11,10,7,0,0,0]
     [0,0,0,0,0,0,15,15,14]];
%Ибо знак равенства в другую сторону
A=-A;
B=[15,18,18,21,12,18];
%Ибо знак равенства в другую сторону
B=-B;
Aeq =[];
Beq =[];
lb=[0,0,0,0,0,0,0,0,0]; %с нулями более корректный результат
%lb=zeros(9);
%lb=[];
[x,fval,exitflag,output] = linprog(F,A,B,Aeq,Beq,lb);
```

Рис. 1. Код программы в MATLAB с расчетом универсальным симплекс-методом

```
>> x'
ans =
         0       1.6154            0       1.6364            0            0            0       1.2000            0
>> fval
fval =
       9032.5
```

Рис. 2. Результаты программы

В итоге были получены следующие результаты: Z = 9 032,5 тыс. рублей – минимальные затраты при заданных параметрах эффективности; x_2 = 1,6154, x_4 = 1,6364, x_8 = 1,2 (дробные корни в данном случае округлим в меньшую сторону, так как цены были подобраны на 50 рабочих компьютеров). Оптимальным выбором будет DLP-система КИБ SearchInform, межсетевой экран Fortinet, антивирус ESET NOD32.

Решение задачи можно проверить с помощью другого метода линейного программирования (рис. 3 и 4).

```
F = [5000,4000,4300,1500,1600,1800,114,97,112];
%F=-F;
A = [[14,13,10,0,0,0,0,0,0]
     [0,0,0,11,10,7,0,0,0]
     [0,0,0,0,0,0,15,15,14]
     [14,13,10,0,0,0,0,0,0]
     [0,0,0,11,10,7,0,0,0]
     [0,0,0,0,0,0,15,15,14]];
%Ибо знак равенства в другую сторону
A=-A;
B=[15,18,18,21,12,18];
%Ибо знак равенства в другую сторону
B=-B;
Aeq =[];
Beq =[];
lb=[0,0,0,0,0,0,0,0,0]; %с нулями более корректный результат
%lb=zeros(9);
%lb=[];
option=optimoptions('linprog','Algorithm','interior-point')
[x,fval,exitflag,output] = linprog(F,A,B,Aeq,Beq,lb,[],option);
```

Рис. 3. Код программы в MATLAB с расчетом методом интерполяции

```
>> fval
fval =
       9032.5
>> x'
ans =
   4.3366e-12       1.6154   5.8385e-12       1.6364   9.0817e-12   2.3853e-11   5.2401e-11          1.2   1.8213e-11
```

Рис. 4. Результаты расчета

Результаты расчета методом интерполяции соответствуют результатам расчета симплекс-методом (Z = 9 032,5 тыс. рублей).

Таким образом, использование точных итерационных математических операций в области информационной безопасности, таких как симплекс-метод, позволяет быстрее решать различные оптимизационные задачи. В частности, на основе экспертных оценок можно подобрать наиболее выгодный и необходимый комплект продуктов для обеспечения безопасности информационной системы предприятия.

Список литературы

1. *Банди Б.* Основы линейного программирования : пер. с англ. – М. : Радио и связь, 1989.
2. *Бирюков А. А.* Информационная безопасность: защита и нападение. – 2-е изд. – М. : ДМК-Пресс, 2017.
3. *Гордиенко В. В., Лисицин А. Л.* Технические и организационные методы борьбы с внутренними угрозами утечки информации организаций и предприятий // AUDITORIUM. – 2019. – № 4 (24). – С. 69–76.
4. *Коккоз М. М., Альжанова А. У., Зияшева А. М., Аубакиров А. М.* Анализ методов управления информационными рисками // Молодой ученый. – 2017. – № 10 (144). – С. 26–29.
5. *Кульневич А. Д.* Линейное программирование // Молодой ученый. – 2017. – № 10 (144). – С. 29–32.

References

1. Bandi B. Osnovy lineynogo programmirovaniya [Principles of Linear Programming], translated from English. Moscow, Radio and Communication, 1989. (In Russ.).
2. Biryukov A. A. Informatsionnaya bezopasnost: zashchita i napadenie [Information Security: Protection and Attack], 2nd ed. Moscow, DMK-Press, 2017. (In Russ.).
3. Gordienko V. V., Lisitsin A. L. Tekhnicheskie i organizatsionnye metody borby s vnutrennimi ugrozami utechki informatsii organizatsiy i predpriyatiy [Technical and Organizational Methods of Struggling with Internal Threats of Information Leakage in Organizations and Enterprises]. *AUDITORIUM*, 2019, No. 4 (24), pp. 69–76. (In Russ.).
4. Kokkoz M. M., Alzhanova A. U., Ziyasheva A. M., Aubakirov A. M. Analiz metodov upravleniya informatsionnymi riskami [Analyzing Methods of Information Risk Management]. *Molodoy uchenyy* [Young Scientist], 2017, No. 10 (144), pp. 26–29. (In Russ.).
5. Kulnevich A. D. Lineynoe programmirovanie [Linear Programming]. *Molodoy uchenyy* [Young Scientist], 2017, No. 10 (144), pp. 29–32. (In Russ.).

Сведения об авторах

Валерий Александрович Сизов
доктор технических наук, профессор,
профессор кафедры прикладной информатики и информационной безопасности института математики, информационных систем и цифровой экономики
РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 117997, Москва, Стремянный пер., д. 36.
E-mail: Sizov.VA@rea.ru

Александр Андреевич Дрожкин
программист-разработчик группы компаний «МультиСофт».
Адрес: группа компаний «МультиСофт», 111396, Москва, ул. Алексея Дикого, д. 3.
E-mail: morgfrimen@yandex.ru

Information about the authors

Valery A. Sizov
Doctor of Technical, Professor,
Professor of the Department for Applied Information Technology and Information Security for Institute of of Mathematics, Information Systems and Digital Economy of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 117997, Russian Federation.
E-mail: Sizov.VA@rea.ru

Alexander A. Drozhkin
Developer Programmer of the MultiSoft Group.
Address: MultiSoft Group,
3 Alexei Dikiy Str., 111396, Moscow, Russian Federation.
E-mail: morgfrimen@yandex.ru