ИНФОРМАТИКА, УПРАВЛЕНИЕ И СИСТЕМНЫЙ АНАЛИЗ

УДК 519.863 ***EDN: MPWBAG***

СТРАТЕГИЯ УПРАВЛЕНИЯ РЕСУРСОМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ПРОБЛЕМНО-ОРИЕНТИРОВАННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

П.Н. Бураго
ORCID: **0000-0002-8010-906X** e-mail: **burago.pasha@yandex.ru**
Нижегородский государственный технический университет им. Р.Е. Алексеева
Нижний Новгород, Россия

В.П. Хранилов
ORCID: **0000-0003-1317-5320** e-mail: **hranilov@nntu.ru**
Нижегородский государственный технический университет им. Р.Е. Алексеева
Нижний Новгород, Россия

А.И. Эгамов
ORCID: **0000-0002-3630-7237** e-mail: **albert.egamov@itmm.unn.ru**
Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского
Нижний Новгород, Россия

Рассмотрена задача распределения ресурсов для обеспечения информационной безопасности корпоративных проблемно-ориентированных информационных систем в течение определенного времени (периода). В реальной ситуации ее математическая модель сводится к задаче дискретной оптимизации – модифицированной задаче о назначениях, к которой неприменимы алгоритмы и методы решения, используемые в классическом варианте. Для поиска оптимального решения при определенных условиях применим эвристический метод, основанный только на знании изначальной стоимости средств защиты информации. Проанализированы частные случаи выбора оптимальной стратегии решения и условия, при которых она будет квазиоптимальной. Показана эффективность использования данной стратегии.

Ключевые слова: дискретная оптимизация, задача о назначениях, средства защиты информации, эвристическая стратегия.

ДЛЯ ЦИТИРОВАНИЯ: Бураго, П.Н. Стратегия управления ресурсом информационной безопасности корпоративных проблемно-ориентированных компьютерных систем / П.Н. Бураго, В.П. Хранилов, А.И Эгамов // Труды НГТУ им. Р.Е. Алексеева. 2024. № 3. С. 7-13. EDN: MPWBAG

STRATEGY FOR INFORMATION SECURITY RESOURCE MANAGEMENT OF CORPORATE PROBLEM-ORIENTED COMPUTER SYSTEMS

P.N. Burago
ORCID: **0000-0002-8010-906X** e-mail: **burago.pasha@yandex.ru**
Nizhny Novgorod State Technical University n.a. R.E. Alekseev
Nizhny Novgorod, Russia

V.P. Khranilov
ORCID: **0000-0003-1317-5320** e-mail: **hranilov@nntu.ru**
Nizhny Novgorod State Technical University n.a. R.E. Alekseev
Nizhny Novgorod, Russia

A.I. Egamov
ORCID: **0000-0002-3630-7237** e-mail: **albert.egamov@itmm.unn.ru**
Nizhny Novgorod State University N.I. Lobachevsky
Nizhny Novgorod, Russia

Abstract. The article considers the task of allocating financial resources to ensure the information security of corporate problem-oriented information systems for a certain period of time. In a real situation, its mathematical model is reduced to a discrete optimization problem – a modified assignment problem, but the algorithms and solution methods that are applied to the classical assignment problem are not applicable. A heuristic method based only on knowledge of the initial cost of information security tools can be used to find the optimal solution under certain conditions. The special cases in which it is possible to choose the optimal strategy and the conditions under which it will be quasi-optimal are analyzed. The example is given that clearly demonstrates the effectiveness of proposed heuristic strategy.

Key words: discrete optimization, assignment problem, information security tools, heuristic strategy.

FOR CITATION: P.N. Burago, V.P. Khranilov, A.I. Egamov. Strategy for information security resource management of corporate problem-oriented computer systems. Transactions of NNSTU n.a. R.E. Alekseev. 2024. № 3. Pp. 7-13. EDN: MPWBAG

Введение

Большинство задач, связанных с распределением ресурсов, относится к сфере дискретной оптимизации, где невозможно использование градиентных методов, имеющих главное значение в непрерывной оптимизации. В то же время решение таких задач, в силу конечного числа объектов, часто можно найти полным перебором вариантов. Дискретная математика способна предоставить совокупность методов и алгоритмов, относящихся к т.н. *конечной математике*, изучающей конечные числовые структуры. Данное направление получает интенсивное развитие вместе со стремительным развитием компьютерной техники и ее постоянно растущим быстродействием, которое позволяет быстро и качественно обработать практически любое конечное множество. Дискретная оптимизация [1] объединяет такие важные прикладные задачи, как «транспортная задача», «задача о рюкзаке», «задача о коммивояжере» и т.п. В их число входит и «задача о назначениях» [2], которая находит непосредственное применение при решении различных современных математико-экономических проблем.

Обеспечение устойчивого функционирования, безопасности и защиты информации является одним из приоритетных направлений деятельности для руководства любой промышленной компании, в бизнес-модели которой задействованы цифровые активы. Однако стремление к предельной коммерциализации и максимальной прибыли должно быть тесно связано с минимизацией убытков вследствие угроз информационной безопасности (ИБ), а также в связи с неоптимальным финансированием функции ИБ. В данной статье рассмотрена модель выбора оптимального алгоритма распределения инвестиций, выделенных на обеспечение ресурса информационной безопасности компании с учетом угроз и рисков.

2. Постановка задачи

Рассмотрим задачу распределения приоритетов при выборе и покупке различных средств защиты, необходимых для обеспечения информационной безопасности компонентов информационного ландшафта компании и минимизации затрат на обеспечение комплексной защиты. Предположим, существует некая проблемно-ориентированная организация, у которой есть n различных групп информационных активов. Они подвержены различным видам информационных угроз и в данной задаче являются объектами защиты:

- внешний сетевой периметр;
- внутренняя сеть;
- бэк-офисные системы;
- бизнес-системы;
- серверное оборудование;
- СУБД;
- АРМы работников и эксплуатационного персонала;
- интеграционные компоненты;
- инструменты виртуализации и контейнеризации;
- прочее.

В категорию «прочее» могут быть отнесены любые специфические для различных отраслей активы, например, для судоходной отрасли – информационные системы на судах, для финансовой отрасли – банкоматы и платежные терминалы, для телекоммуникационной компании – технологический сегмент сетей связи и т.п.

Альтернативно в данной задаче в качестве таких групп информационных активов могут быть рассмотрены информационные бизнес-системы, состоящие, в том числе, из различных компонентов:

- сетевой инфраструктуры;
- серверного оборудования;
- АРМ;
- СУБД;
- приложений;
- прикладного ПО;
- интеграционных компонентов.

Для обеспечения ИБ каждой группы активов нужно внедрить одно или несколько средств защиты информации (СЗИ). На их закупку и внедрение выделен определенный конечный бюджет, однако расходовать его можно только поэтапно, чтобы равномерно распределить затраты на ИБ для организации по временному периоду, например, в течение года, и избежать вопросов со стороны контролирующих органов, например, совета директоров. Также разовая покупка всех необходимых средств защиты может привести к неоптимальным затратам и простою приобретенных СЗИ, так как ресурсы подразделения ИБ ограничены, и одновременное внедрение всех данных СЗИ не представляется возможным.

Подобная задача о поэтапном выделении финансовых средств также может быть применима для организаций малого и среднего бизнеса, в которых руководитель выделяет их на обеспечение ИБ из полученной прибыли один раз в месяц. Основным риском в данной задаче являются: недоступность актива (группы активов) в связи с реализовавшимся инцидентом ИБ и финансовые потери (включая недополученную прибыль), которые понесет организация в связи с недоступностью определенного актива (группы активов). Стоимость группы активов может быть оценена финансовым подразделением в виде прогноза на предстоящий финансовый период на основании информации о полученной прибыли за текущий период. Под стоимостью актива в данном случае подразумевается прибыль, которую данный актив гене-

рирует за ограниченный отчетный период. Целью является минимизация убытков, которые организация понесет в случае полной или частичной недоступности данного актива.

3. Математическая модель минимизации ресурсов

Пусть имеется n информационных активов организации и средств защиты предприятия. Занумеруем их от 1 до n. Покупка СЗИ для них осуществляется на периодической основе. Предположим, цена СЗИ для i-й группы активов в j-й период равна c_{ij} рублей, $c_{ij} > 0$. Таким образом, определяется матрица C порядка $n \times n$, а на обеспечение всей СЗИ организации будет потрачено $f(\eta) = \sum_{j=1}^{n} c_{\eta(j)j}$, где η – перестановка чисел от 1 до n, число $\eta(j)$ означает номер актива, для обеспечения информационной безопасности которого в j-м периоде купили и внедрили соответствующее СЗИ. Задача руководителя подразделения ИБ состоит в том, чтобы минимизировать функцию $f(\eta)$.

При известной платежной матрице C представленная задача сводится к известной задаче о назначениях. Исторически первым и наиболее популярным из методов решения задачи о назначениях является венгерский алгоритм, разработанный Харальдом Куном в 1955 г. [3, 4]. В реальной жизни изначально (до начала первой покупки) вся матрица C неизвестна, она заполняется в начале каждого периода – в начале j-го периода становится известен j-й столбец. Поэтому для практического решения поставленной задачи нужны другие, эвристические алгоритмы [5]. Схожая задача минимизации финансовых трат на компоненты для защиты от киберугроз рассматривалась в [6], а задача максимизации выхода конечного продукта прибыли на предприятии и агропромышленного комплекса изучалась в [7-9].

Ниже приводится эвристическая стратегия, которая при условии равного отношения цен СЗИ всех групп активов для каждой пары смежных периодов покупок (отношение зависит только от j) является оптимальной. Для ее использования достаточно знания только начальных цен СЗИ групп активов (первого столбца матрицы C).

Для определенности предположим, что все c_{i1} различны. Обозначим $B_{ij} = \frac{c_{ij}}{c_{i1}}$, $i = \overline{1,n}$, $j = \overline{1,n}$ и найдем оптимальную стратегию для руководителя ИБ, минимизирующую траты на покупку средств защиты.

4. Эвристическая стратегия

Рассматривается частный случай, когда изменение отношения стоимости активов для каждой пары смежных периодов зависит только от номера периода, т.е.:

$$B_{ij} = b_j,\ i = \overline{1,n}. \quad (1)$$

Условие равного отношения цен СЗИ всех групп активов для каждой пары смежных периодов покупок и условие (1) эквивалентны. Действительно,

$$\theta_j = \frac{c_{i\,j+1}}{c_{ij}} = \frac{c_{i1}B_{ij+1}}{c_{i1}B_{ij}} \Rightarrow B_{ij+1} = \theta_j B_{ij},$$

так как $B_{i1} = 1$ при любом $i = \overline{1,n}$, топараметры B_{ij} зависят только от j и выполняется условие (1). С другой стороны, при выполнении условия (1) верны равенства $\frac{c_{i\,j+1}}{c_{ij}} = \frac{c_{i1}B_{ij+1}}{c_{i1}B_{ij}} = \frac{b_{j+1}}{b_j}$, при всех $i = \overline{1,n}$. Эквивалентность доказана.

При этих условиях целевая функция имеет вид:

$$f(\eta) = \sum_{j=1}^{n} c_{\eta(j)1} b_j . \qquad (2)$$

Известно [10]:

Перестановочное неравенство. Имеются два m *-мерных вектора* $\overline{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_m)^T$ *и* $\overline{\beta} = (\beta_1, \beta_2, ..., \beta_m)^T$ *. Их скалярное произведение* $\overline{\alpha} \cdot \overline{\beta} = \sum_{i=1}^{m} \alpha_i \beta_i$

минимально, если выполняются неравенства: $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_m$ *и* $\beta_1 \leq \beta_2 \leq ... \leq \beta_m$;

максимально, если выполняются неравенства: $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_m$ *и* $\beta_1 \geq \beta_2 \geq ... \geq \beta_m$.

Расставим слева направо числа b_j в порядке возрастания, а числа c_{i1} – в порядке убывания. Перестановка μ чисел от 1 до n такая, что $\mu(j)$ – это номер в конечной последовательности, описанной выше, параметра b_j при расчете слева направо. Перестановка γ чисел от 1 до n такая, что $i = \gamma(s)$, если число c_{i1} в последовательности стоит на s-ом месте. Отсюда следует, что $\gamma^{-1}(i) = \mu(j)$, если номера мест в соответствующих последовательностях чисел b_j и c_{i1} равны. Таким образом, описанные выше перестановки отвечают случаю, когда значение функции в формуле (2) минимально.

Поэтому для исходной матрицы C оптимальная перестановка $\eta^*(j) = \gamma(\mu(j))$ и, чтобы минимизировать $f(\eta)$, осуществлять покупки нужно согласно правилу: в j-м периоде покупать оборудование для $\gamma(\mu(j))$-й группы активов.

Для удобства можно переставить строки матрицы C так, чтобы $\gamma(\mu(j))$-я строка была бы j-й строкой. Получим матрицу $\widetilde{C}$ с элементами $\widetilde{c}_{ij} = \widetilde{c}_{i1} b_j$, в этом случае оптимальной будет являться тождественная перестановка.

5. Частные случаи применения

Использование предложенного метода эффективно, когда априори известно расположение относительно друг друга построенной по возрастанию членов последовательности b_j. Приведем два примера.

На практике нередко встречается случай, когда выполняется условие (1), и цены на СЗИ всех групп активов монотонно возрастают, т.е. последовательность b_j монотонно возрастает, что означает $\mu \equiv \varepsilon$, а значит $\eta^*(j) = \gamma(j)$, необходимо придерживаться следующей стратегии (ее можно назвать «по убыванию элементов первого столбца»): осуществлять покупки нужно соответственно убыванию начальной цены c_{i1}, т.е. начинать с самого дорогого СЗИ первого столбца и заканчивать покупкой самого дешевого.

Предположим, что выполняется условие (1) и известно, что вначале в течение k периодов цена на СЗИ для всех групп активов будет падать, а потом взлетит, начиная с $(k+1)$-го периода, будет выше изначальной и после только возрастать. Этот вариант развития событий тоже часто встречается на практике, особенно при небольших k. Согласно вышеописанному методу, оптимальным является следующий вариант закупок. Вначале покупается СЗИ для той группы активов, чья начальная цена является k-ой по счету, если начальные цены расставить в порядке убывания. Затем для того, у которого начальная цена расположена на $(k-1)$-ом месте, … , в k-й период покупается СЗИ для группы активов с максимальной начальной ценой. Начиная с $(k+1)$-го периода покупки осуществляются по убыванию начальной цены СЗИ оставшихся $n-k$ групп активов.

6. Пример

Нетрудно заметить, что подобной стратегией (в этом случае она, как правило, будет квазиоптимальной) можно пользоваться и когда условие (1) не выполняется, но для каждого j, $j=\overline{1,n}$,все B_{ij}при любомi, $i=\overline{1,n}$, принадлежат малой окрестности некоторой точки $\tilde{b}_j$, т.е., когда влияние на цену блоков оказывает, в основном, временной параметр. Приведем пример применения вышеописанной методики в случае невыполнения условия (1). Для получения квазиоптимального решения желательно, чтобы «разброс» B_{ij} был небольшим, и почти все значения B_{ij} при фиксированном j лежали бы по одну сторону от числа 1, т.е. почти все значения B_{ij} при фиксированном j были бы не больше начальной цены или не меньше ее. В табл. 1 приведены цены, которые могут быть потрачены для защиты от киберугроз информационных групп активов одной крупной промышленной организации в каждый из восьми месяцев 2022 г., т.е. фактически задана матрица C. В начале 2022 г., естественно, известны цены только за январь и некая информация о поведении цен в 2021 г. (например, что они всегда не убывали).

Таблица 1.
Цены на СЗИ группы активов за 8 периодов 2022 г. (млн руб.)

Table 1.
Prices for information security tools of the asset group for 8 periods of 2022 (million rubles)

		I	II	III	IV	V	VI	VII	VIII
1	**СЗИ – Внешний сетевой периметр**	1	11.5	12	12	12.5	12.5	13	14
2	**СЗИ – Внутренняя сеть**	27.5	28.5	29.8	30	31	31	32	33
3	**СЗИ – Бизнес-системы**	34.5	35.5	35.5	35.5	36.5	36.5	36.5	37
4	**СЗИ – Серверное оборудование**	30	30	31	31.5	32.5	33.5	34	35
5	**СЗИ – СУБД**	34	34	35.5	36	36.8	37.7	38.5	39
6	**СЗИ – Интеграционные компоненты**	7	7	7.2	7.4	7.5	7.6	7.8	8
7	**СЗИ – Бэк-офисные системы; АРМы работников и Инструменты виртуализации**	8	8.4	8.8	9	9.2	9.4	9.8	10
8	**СЗИ – Прочее**	32	33	34	34.7	34.8	35.5	36.5	37.5

Таким образом, применение стратегии «по убыванию элементов первого столбца» позволяет получить значение целевой функции – 195.3. Вычисления по венгерскому алгоритму (в данной модификации задачи не реализуемого на практике) апостериори дают оптимальный результат, равный 193.1, т.е. относительная погрешность предложенного в статье метода – 1.14 %. Эти результаты показывают, что предложенная эвристическая стратегия в данном случае является квазиоптимальной.

Рассмотрим другие интуитивно понятные стратегии. Стратегия покупок, основанная на тождественной перестановке (выбираются элементы, стоящие на главной диагонали матрицы), дает в результате – 198.2. Стратегия покупок, основанная на перестановке элементов тождественной перестановки в обратном порядке (выбираются элементы, стоящие на побочной диагонали), дает в результате – 198.6. Стратегия покупок, когда на каждом этапе выбирается минимальный элемент из «невыбранных» до этого момента строк, дает в результате – 200.9. Стратегия покупок, когда на каждом этапе выбирается максимальный элемент из «невыбранных» до этого момента строк, дает в результате также 195.3, так как при этой страте-

гии принцип выбора элемента столбца схож с принципом выбора стратегии «по убыванию элементов первого столбца». Эти результаты свидетельствуют об эффективности представленной стратегии, которая при определенных условиях имеет несомненное право на практическое применение.

7. Заключение

Рассмотрена задача распределения ресурса информационной безопасности корпоративной проблемно-ориентированной информационной системы в течение определенного времени (8 периодов), которая при определенной информации сводится к модифицированной задаче о назначениях. Ее постановка не позволяет найти оптимальное решение априори. Показан оптимальный результат при распределении ресурсов при некоторых дополнительных условиях. Предложена эвристическая стратегия, позволяющая получить оптимальный (или квазиоптимальный) результат. Дополнительные условия не являются искусственными. На примере реального предприятия продемонстрирована эффективность данной стратегии.

Библиографический список

1. **Леонтьев, В.К.** Дискретная оптимизация // ЖВМ и МФ. 2007. Т. 47. № 2. С. 338-352.
2. **Rainer, B.** Assignment problems / B. Rainer, M. Dell'Amico, S. Martello – Society for Industrial and Applied Mathematics. USA, Philadelphia, 2009. 382 p.
3. **Kuhn, H.W.** The Hungarian Method for the assignment problem. Naval Research Logistics Quarterly. 1955. 2. Pp. 83-97.
4. **Банди, Б.** Основы линейного программирования / Б. Банди – М.: Радиоисвязь, 1989. – 176 с.
5. **Попов, В.Б.** Глава 7. Метаэвристические алгоритмы для задач экономической оптимизации и прогнозирования // Информационная экономика: развитие, управление, модели: коллективная монография. Симферополь, 2017. С. 401-416.
6. **Khranilov, V.P., Burago, P.N., Egamov, A.I.** Mathematical Model DDS for Information Security Management of the Organization. E3S Web of Conferences. 2024. № 537. 09009.
7. **Balandin, D.V.** Mathematical Modelling and Optimization of Scheduling for Processing Beetin Sugar Production / D.V. Balandin et al. / In book: Balandin D., Barkalov K., Meyerov I. (eds). Communications in Computer and Information Science. 2022. № 1750. Pp. 227-238.
8. **Баландин, Д.В.** Математическая модель и комбинированный квазиоптимальный алгоритм процесса переработки сахарной свеклы / Д.В. Баландин и др. // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2023 (2). С. 62-76.
9. **Egamov, A.I.** Mathematical Model of Processing Batches of Raw Materials Taking into Account Ripening Process // In book: Balandin D., Barkalov K., Meyerov I. (eds) Communications in Computer and Information Science. 2023. № 1914. Pp. 190-205.
10. **Радзивиловский, Л.В.** Обобщение перестановочного неравенства и монгольское неравенство // Математическое просвещение. 2006. Вып. 10. С. 210-224.

Дата поступления
в редакцию: 18.05.2024

Дата принятия
к публикации: 31.07.2024