УДК 004.056.5

МЕТОДИКА РАНЖИРОВАНИЯ ПОДРАЗДЕЛЕНИЙ РАСПРЕДЕЛЕННОЙ КОРПОРАТИВНОЙ СИСТЕМЫ ПО СТЕПЕНИ СООТВЕТСТВИЯ ПОЛИТИКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Д. Козлов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: alkozlov@ipu.ru

Н.Л. Нога
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: noga@ipu.ru

Ключевые слова: политика информационной безопасности, критерии, ранжирование значений показателей, сравнительная оценка, отношение Парето, максиминная процедура.

Аннотация: Предложена методика ранжирования подразделений распределенной корпоративной информационной системы по ряду показателей информационной безопасности, в результате реализации которой дается сравнительная оценка степени удовлетворения требованиям корпоративной политики информационной безопасности каждого из подразделений для дальнейшего принятия решений руководством корпорации относительно мер по минимизации ущерба в результате реализации угроз информационной безопасности.

1. Введение

В условиях цифровизации экономики информация становится одним из самых ценных ресурсов любой компании (корпорации). Защита этих ресурсов – одна из важнейших задач. Как правило, основные требования к обеспечению безопасного сбора, обработки и доступа к информации формулируются и документально закрепляются в «политике (информационной) безопасности организации».

В этом документе определяется характер обрабатываемой информации, правила ее обработки и хранения, права доступа, как сотрудников организации, так и внешних пользователей, ответственность различных категорий сотрудников и подразделений компании, а также другие организационные и технические требования к обеспечению информационной безопасности.

В целях обеспечения защиты информационных ресурсов необходим постоянный мониторинг состояния информационной безопасности, фиксация любых неправомер-

ных попыток нарушения доступности, целостности, конфиденциальности информации. Фиксируя и анализируя факты нарушений, компания может оперативно принимать управляющие решения для минимизации возможного ущерба от угроз информационной безопасности.

Для организаций (корпораций), имеющих сеть территориально-распределенных подразделений задача принятия управляющих решений существенно усложняется, так как одновременно охватить все подразделения невозможно. Важно выявить наиболее критические точки. Сделать это помогает ранжирование подразделений.

В докладе предлагается к рассмотрению методика ранжирования и сравнительной оценки подразделений по ряду важных показателей, установленных корпоративной политикой информационной безопасности. В результате реализации такой методики будет обеспечена сравнительная оценка степени удовлетворения требованиям информационной безопасности каждого из подразделений для дальнейшего моделирования разнообразных управленческих ситуаций, генерации на этой основе решений по принятию мер по защите информационных ресурсов корпорации.

2. Постановка задачи и реализация методики

Вышеуказанные показатели рассматриваются в дальнейшем как некоторые критерии, принимающие значения из определенных интервалов, стандартные границы которых определяются как в ГОСТах, так и в различных методических и нормативных документах организации. Каждому подразделению поставим в соответствие некоторый ранг r, в зависимости от значений этих критериев, и выстроим все ранги, например, по возрастанию. Будем считать, что чем выше ранг, тем выше степень удовлетворения требованиям информационной безопасности.

Пусть B – множество рассматриваемых подразделений, куда входят подразделения, обозначенные как $x, y, z,...$; I – количество рассматриваемых показателей, K_i – i-й показатель, $i = 1,\ldots,I$; $r_j = r_j(K_1, K_2, ..., K_N)$ – ранг j-го подразделения, $j = 1, \ldots, N$, где N - количество рассматриваемых подразделений. В предположении, чем больше значение ранга, тем лучше обстоят дела с обеспечением информационной безопасности подразделения, необходимо отсортировать ранги по возрастанию.

Замечание. Эту же задачу можно решать и для одного подразделения, но за разные отчетные периоды, для определения степени удовлетворения требованиям информационной безопасности подразделения в динамике.

Предположим, что мы оцениваем подразделение x по i показателям, то есть,

$$K_1(x), K_2(x), ..., K_i(x).$$

Далее проведем реализацию методики на примере (рассматривается одна из корпораций с разветвленной сетью подразделений в качестве примера) оценки 10 подразделений по 3 критериям (показателям), которые указывают степень удовлетворения требованиям информационной безопасности подразделения по каждому показателю. Выберем следующие показатели:

- F – частота появления неправомерных запросов, поступивших из i-го подразделения по отношению к общему числу запросов от этого подразделения;
- S – частота выявленных инцидентов безопасности в i-м подразделении по отношению к общему числу выявленных инцидентов в корпорации;
- D – частота выявления вирусов (вредоносных программ) в i-м подразделении по отношению к общему числу выявленных вирусов в корпорации.

В Таблице 1 задаются соответствующие оценки полученных значений показателей, в первом случае вычтенных из единицы, с округлением до двух знаков после запятой.

Таблица 1. Оценки подразделений.

Подразделение	**1-*F***	***S***	***D***
1	0.68	0.82	0.59
2	0.82	0.93	0,55
3	0.91	0.87	0.58
4	0.74	0.72	0.53
5	0.70	0.97	0.51
6	0.55	0.56	0.60
7	0.52	0.79	0.60
8	0.68	0.80	0.55
9	0.60	0.65	0.57
10	0.64	0.96	0.53

Для дальнейшего оценивания рассмотрим некоторые понятия, которые используются ниже [1]. Построим отношение R – обобщенное отношение Парето между подразделениями x и y, такое что

$$xRy \Leftrightarrow \{\forall i\ K_i(x) \geq K_i(y) + \varepsilon_i \text{ и } \exists i_0 \left| K_{i_0}(x) > K_{i_0}(y) + \varepsilon_{i_0} \right.\},$$

где x и y – подразделения из множества B, K_i – i-ый показатель, относительно которого оценено подразделение, $i = 1..., I$; ε_i – параметр «чувствительности» (погрешности) - пороговое значение, соответствующее каждому i-му показателю.

Отношение R – интерпретируется как, «быть лучше чем», то есть, xRy означает «x лучше чем y», или «степень удовлетворения требованиям безопасности у подразделения x выше, чем у подразделения y». Т.е. отношение xRy выполняется, если для какого-нибудь показателя подразделение x имеет больший или равный чем y вес, принимая во внимание чувствительность ε, и, по крайней мере, для одного показателя подразделение x имеет строго более высокие результаты, чем подразделение y, с учетом ε.

Отношение R строится по всем показателям $\{K_i(x)\}$, $i = 1..., I$, и является строгим частичным порядком, то есть, строгим и транзитивным бинарным отношением.

Для вышеприведенного примера отношение R, построенное при $\varepsilon = 0.02$, приводится в Таблице 2.

Таблица 2. Результаты отношения R

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	0	0	0	0	0	0	0	0	1	0
2	0	0	0	1	0	0	0	1	0	0
3	0	0	0	1	0	0	0	1	1	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0

Из таблицы 1 легко видно, что подразделение {1} имеет большие значения всех показателей чем подразделение {9}, следовательно, в пересечении строки отделения {1} с колонкой для подразделения {9} ставится 1; то же самое верно для подразделения

{2} по отношению к подразделениям {4} и {8}. И то же самое верно для подразделения {3} по отношению к подразделениям {4}, {8} и {9}. Подразделения {1}, {2} и {3} находятся в границе Парето, но подразделение {4} – Парето доминируется подразделениями {2} и {3}.

Однако, не удается сравнить все подразделения друг с другом, используя отношение R, так как может быть ситуация, когда не удовлетворяется условие транзитивности. Действительно, в вышеприведенном примере подразделение {2} «лучше», чем подразделение {4}, но подразделение {1} не может быть сравнено с этими двумя подразделениями (см. Таблицу 1).

В этом случае можно поступить следующим образом. Проведем аппроксимацию отношения R через некоторый слабый порядок W – строгое, переходное и не транзитивное переходное бинарное отношение. Таким образом, для любых двух подразделений или один лучше, чем другой, или они оба равны в терминах окончательной оценки операций. Обозначим лучшую группу подразделений как $C_1(B)$. Тогда, после того, как из сравнения исключаются лучшие подразделения, применяя ту же самую процедуру, может быть найдена вторая наилучшая группа подразделений. Эта группа обозначается как $C_2(B)$. Продолжая этот процесс, можно получить последовательность наборов $C_3(B)$, $C_4(B)$, $C_5(B)$ и т.д., пока не будут распределены все подразделения.

Для проведения ранжирования воспользуемся методом, основанным на игровых матрицах, например на максиминной процедуре и максимизации выигрышей.

Построим обобщенную матрицу игры P, такую что $\forall x, y \in B$,

$$P = \{l(x,y)\} \text{ с } l(x,x) = \infty, \text{ и } l(x,y) = \{l \,|\, K_i(x) > K_i(y) + \varepsilon_i\},$$

где строки и столбцы матрицы P соответствуют множеству подразделений в B. На пересечении x-ой строки и y-го столбца помещено число $l(x,y)$, равное числу показателей (критериев), в которых подразделение x имеет более высокие значения степени удовлетворения требованиям безопасности, чем подразделение y, с учетом ошибки измерения.

Отмечаем минимумы строк (в каждой строке) (для каждого отделения) в предпоследнем столбце Таблицы 3. Для любого подразделения $z \in B$, минимум строки показывает степень удовлетворения требованиям безопасности z по сравнению с «самым жестким» соперником. Затем выбираем подразделение, которое имеет максимум в этих минимумах. Оно и соответствует наилучшему подразделению, то есть

$$x \in C_1(B) \Leftrightarrow l(x,y) = \max_{m \in B}\{\min_{n \in B}\{l(m,n)\}\} \text{ для некоторого } y \in B.$$

Затем исключаем x из множества B и повторяем процедуру снова, получая $C_2(B)$ и т.д.

Проиллюстрируем этот метод на данных, приведенных в Таблице 1. Расширенная матрица игры в этом случае принимает вид, указанный в Таблице 3 (где чувствительность ε_i = 0.01 для всех i = 1, 2, 3):

Таблица 3. Расширенная матрица игры

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	***min***	***w(x)***
1	∞	1	0	2	1	2	2	2	3	2	0	15
2	2	∞	1	3	2	2	2	2	2	2	1	18
3	2	2	∞	3	2	2	2	3	2	2	2	20
4	1	0	0	∞	2	2	1	1	2	1	0	10
5	2	1	1	1	∞	2	2	2	2	1	1	14
6	0	1	1	1	1	∞	1	1	1	1	0	8
7	0	1	1	2	1	1	∞	1	2	1	0	10
8	0	0	0	1	1	2	2	∞	2	2	0	10
9	0	1	0	1	1	2	1	1	∞	1	0	8

10	1	1	1	1	1	2	2	1	2	∞	1	12

Таким образом, $C_1(B) = \{3\}$. Исключая подразделение {3} из рассмотрения, получаем далее лучшее $C_2(B) = \{2\}$, затем $C_3(B) = \{1, 4, 5, 10\}$, $C_4(B) = \{8\}$, $C_5(B) = \{6, 7, 9\}$. Чтобы ранжировать подразделения в $C_3(B)$ и $C_5(B)$ воспользуемся процедурой максимизации выигрышей.

Пусть $l(x, y)$, как и выше, равно числу показателей, в которых подразделение x имеет более высокие значения, чем подразделение y, тогда сумма

$$w(x) = \sum_{y, y \neq x} l(x, y)$$

будет выражать общее количество побед подразделения x над другими подразделениями [1]. Функция $w(x)$ определяет естественный порядок относительно множества B, при этом, $w(x)$ принимает значения, указанные в последнем столбце расширенной матрицы игры в Таблице 3. Теперь множество {1, 4, 5, 10}ранжируется следующим образом: {1}, {5}, {10}, {4} в порядке убывания. А множество {6, 7, 9} ранжируется таким образом: {7} и {6, 9}. Последнее множество ранжируем, вернувшись к предыдущей максиминной процедуре, где рассматриваются только подразделения {6} и {9}. Тогда получаем следующее упорядочивание: {9} и {6} в порядке убывания. Получаем следующий ранжированный ряд (Таблица 4):

Таблица 4. Результаты реализованного метода

Подразделение	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Ранг	3	2	1	6	4	10	8	7	9	5

Итак, мы получили отранжированный ряд подразделений по степени удовлетворения требованиям информационной безопасности с помощью метода, основанного на максиминной процедуре и максимизации выигрышей. Конечно, лучше получить такой ряд несколькими методами [1] и провести затем сравнение результатов, используя, например, достаточно известную меру – расстояние Хемминга [2]. Но методы сравнения ранжирований требуют дополнительного исследования и в данном докладе не рассматриваются.

3. Заключение

Предложенную методику можно применять к любой сложной сетевой структуре, как государственных органов, так и частных корпораций, что позволяет учитывать региональные особенности подразделений (количество и квалификацию сотрудников в подразделении, удаленность и т.п.).

Список литературы

1. Kozlov A., Lebedev V. The methods of ranking and comparative assessment of branches of a distributed corporate system // Proceedings of the 10th International Conference "Management of Large-Scale System Development" MLSD '2017. P. 1-5, https://ieeexplore.ieee.org/document/ 8109647
2. Hamming distance: The number of digit positions in which the corresponding digits of two binary words of the same length are different (Federal Standard 1037C).