МЕТОДИКА ОЦЕНКИ СТЕПЕНИ СООТВЕТСТВИЯ ПОДРАЗДЕЛЕНИЙ СЛОЖНОЙ СЕТИ ПОКАЗАТЕЛЯМ КОРПОРАТИВНОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Козлов А.Д., Нога Н.Л.
Институт проблем управления им. В.А. Трапезникова РАН
alkozlov@ipu.ru, noga@ipu.ru

Аннотация. Предложена методика оценки степени соответствия подразделений сложной распределенной корпоративной информационной системы показателям информационной безопасности. В результате реализации методики дается сравнительная оценка степени удовлетворения требованиям корпоративной политики информационной безопасности каждого из подразделений с целью дальнейшего принятия *решений руководством корпорации относительно мер по минимизации рисков в результате возможного осуществления угроз информационной безопасности.*

Ключевые слова: информационная безопасность, критерии, ранжирование значений показателей, сравнительная оценка, отношение Парето, максиминная и минимаксная процедуры, счета Борда, расстояние Хэмминга.

Введение

В последнее время одной из важнейших задач организаций, в силу развития цифровизации экономических процессов, является защита информационных ресурсов. Основные требования по обеспечению безопасности этих ресурсов обычно формулируются в документах по корпоративной политике информационной безопасности.

В этом документе в соответствии с принятыми стандартами прописываются правила по сбору, хранению, обработке и доступе к информации, как сотрудников, так и внешних пользователей. Определяется их ответственность на всех этапах прохождения информации. А также, задаются характеристики обрабатываемой информации, формулируются различные организационные, технологические и технические требования к обеспечению информационной безопасности.

Для обеспечения защиты информационных ресурсов компания должна осуществлять постоянный мониторинг состояния информационной безопасности, фиксировать любые неправомерные попытки нарушения доступности, целостности, конфиденциальности информации. По результатам мониторинга и анализа уязвимостей и фактов нарушения, служба безопасности компании должна предлагать руководству компании решения по минимизации возможного ущерба от возникающих угроз информационной безопасности, рекомендовать проведение организационно-технических мероприятий, направленных на повышение уровня защищенности информационных ресурсов компании.

Для организаций (корпораций), имеющих территориально-распределенную структуру задача принятия управленческих решений существенно усложняется, так как одновременно охватить все подразделения довольно трудно. Поэтому важно выявить наиболее критичные подразделения. Сделать это помогает их ранжирование. В работе авторов [1] рассматривался один из методов ранжирования подразделений, но не было дано сравнительной оценки полученных результатов с другими методами.

В настоящем докладе авторы предлагают рассмотреть методы ранжирования и сравнительной оценки подразделений по ряду важных показателей, утвержденных корпоративной политикой информационной безопасности. В результате реализации таких методов будет обеспечена сравнительная оценка степени удовлетворения требованиям информационной безопасности каждого из подразделений и найдены наиболее критичные из них для дальнейшего моделирования разнообразных управленческих ситуаций, генерации на этой основе решений по принятию мер по защите информационных ресурсов корпорации.

1 Постановка задачи

Показатели безопасности будем в дальнейшем рассматривать как некоторые критерии, принимающие значения в определенных интервалах, стандартные границы которых определены как в международных стандартах, так и в различных методических и нормативных документах организации. Каждому подразделению корпорации 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, $i = 1,…,I$; $r_j = r_j(K_1, K_2, ..., K_I)$ — ранг j-го подразделения, $j = 1, …, N$, 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. Похожая задача решается и в рамках 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 из [1] (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 j-го подразделения по отношению к общему числу запросов от этого подразделения;
– S — частота предотвращенных инцидентов безопасности в j-м подразделении по отношению к общему числу выявленных инцидентов в данном подразделении;
– D — относительное количество пользователей в j-м подразделении, выполняющих требования политики безопасности по смене пользовательских паролей.

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	-F	S	D
1	.68	.82	.59
2	.82	.93	,55
3	.91	.87	.58
4	.74	.72	.53
5	.70	.97	.51
6	.55	.56	.60
7	.52	.79	.60
8	.68	.80	.55
9	.60	.65	.57
10	.64	.96	.53

Для дальнейшего оценивания рассмотрим некоторые понятия, которые используются ниже [2-3]. Построим отношение R - обобщенное отношение Парето между подразделениями x и y, такое что

$$xRy <=> \{\forall i K_i(x) \geq K_i(y) + \varepsilon_i \text{ и } \exists i_0 \mid K_{i0}(x) > K_{i0}(y) + \varepsilon_{i0}\},$$

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 – можно интерпретировать как, «быть лучше чем», то есть, xRy означает «x лучше чем y», или «степень удовлетворения требованиям безопасности подразделения x выше, чем у подразделения y» [4, 5]. 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 по степени удовлетворения требованиям безопасности, чем подразделение y, с учетом чувствительности.

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 чувствительности ε = 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

	1	2	3	4	5	6	7	8	9	10
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.

Далее предлагается рассмотреть несколько достаточно простых методов ранжирования подразделений и сравнить их с целью выбора наиболее оптимального метода. Первые два метода основаны на игровых матрицах, третий основан на методе счетов Борда, четвертый — на методе усреднения счетов Борда [6].

2 Метод максиминной процедуры и максимизации выигрышей

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

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

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 $\varepsilon_i = 0.01$ 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

	1	2	3	4	5	6	7	8	9	10	*min*	*w(x)*
8	0	0	0	2	1	2	1	-“-	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 упорядочить 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 лучших показаний (побед) подразделения *x* над другими подразделениями [3]. 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 первого метода

Подразделение	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Ранг (Р1)	3	2	1	6	4	10	8	7	9	5

Итак, мы получили отранжированный ряд подразделений по степени удовлетворения требованиям информационной безопасности с помощью комбинированного метода, основанного на максиминной процедуре и максимизации выигрышей.

3 Метод минимаксной процедуры и минимизации выигрышей

Рассмотрим матрицу *P* из предыдущего раздела, 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 максимумы столбцов (в каждом столбце) (для каждого подразделения) в предпоследней строке Таблицы 5. Для любого $z \in B$, это число (максимум столбца) показывает худшие показатели степени удовлетворения требованиям безопасности *z* по сравнению с «самым плохим» подразделением. Далее выбираем подразделение, которому соответствует минимум из максимумов столбцов, то есть, выбираем подразделение, которое имеет показатели степени удовлетворения требованиям безопасности лучше других подразделений, то есть

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

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

Продемонстрируем это правило на данных из Таблицы 1. Матрица игры в этом случае принимает вид, указанный в Таблице 5 (ε_i = 0.01 для всех i = 1, 2, 3):

Таблица 5. Расширенная матрица игры

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

	1	2	3	4	5	6	7	8	9	10
7	0	1	1	2	1	1	-“-	1	2	1
8	0	0	0	2	1	2	1	-“-	2	2
9	0	1	0	1	1	2	1	1	-“-	1
10	1	1	1	1	1	2	2	1	2	-“-
max	2	2	**1**	3	2	2	2	3	3	2
l(y)	8	8	**5**	16	12	17	14	14	18	13

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, 6, 7, 8, 10}, $C_4(B)$ = {9}. Чтобы упорядочить подразделения в $C_3(B)$ воспользуемся процедурой минимизации выигрышей.

Пусть $l(x, y)$ то же, что и в предыдущем разделе, тогда сумма

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

будет отображать общее количество худших показаний подразделения *y* по сравнению с другими подразделениями. Функция *l(y)* определяет естественный порядок относительно множества *B* при этом, *l(y)* принимает значения, указанные в последней строке Таблицы 5. Теперь множество {1, 4, 5, 6, 7, 8, 10} упорядочивается следующим образом: {1}, {5}, {8, 10}, {4, 7}, {6}. Множества {8, 10}, {4, 7} упорядочиваются аналогично следующим образом: {8}, {10}, {7}, {4}. Итак, получаем следующий ранжированный ряд (Таблица 6):

Таблица 6. Результаты второго метода

Подразделение	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Ранг (Р2)	3	2	1	8	4	9	7	5	10	6

4 Метод счетов Борда

Проведем теперь ранжирование с помощью метода счетов Борда [6]. Определим нижний граничный набор *W(x)* для подразделения *x* как набор подразделений, которые хуже чем *x* относительно *R*, то есть, *W(x)* = {*y*| *xRy*}. Количество подразделений во множестве *W(x)* обозначим через $\|W(x)\|$.

Рассмотрим подразделение $x \in B$ и назначим для *x* счет $t_i(x)$, который является количеством элементов нижнего граничного множества, т.е.,

$$t_i(x) = \|W_i(x)\| = \|\{a \in B | K_i(x) > K_i(a) + \varepsilon_i\}\|.$$

Сумма счетов для каждого $j \in N$ называется счетом Борда *j*-го подразделения

$$t(x) = \sum_{i=1}^{I} t_i(x)$$

.

Найдем счета Борда для подразделений в нашем примере с подразделениями из таблицы 1. Соответствующие счета приводятся в таблице 7 с учетом чувствительности ε_i = 0.01 для всех рассмотренных показателей.

Как видно из таблицы 7: $C_1(B)$={3}, $C_2(B)$={2}, $C_3(B)$={1}, $C_4(B)$={5}, $C_5(B)$={10}, $C_6(B)$={4, 7, 8}, $C_7(B)$={6, 9}. Чтобы упорядочить $C_6(B)$ строим укороченную таблицу 8 счетов Борда только для подразделений 4, 7 и 8. Аналогично поступаем для упорядочения $C_7(B)$={6, 9}.

Таблица 7. Счета Борда для подразделений

Подразделение	t_1 (1-F)	t_2 (S)	t_3 (D)	t
1	4	5	6	15
2	8	7	3	18
3	9	6	5	20
4	7	2	1	10
5	6	8	0	14
6	1	0	7	8

Подразделение	t_1 (1-F)	t_2 (S)	t_3 (D)	t
7	0	3	7	10
8	4	3	3	10
9	2	1	5	8
10	3	8	1	12

Таблица 8. Счета Борда для трех подразделений

Подразделение	t_1 (1-F)	t_2 (S)	t_3 (D)	t
4	2	0	0	2
7	0	1	2	3
8	1	2	1	4

В итоге строим следующий ранжированный ряд (таблица 9):

Таблица 9. Результаты третьего метода

Подразделение	Р3	Подразделение	Р3
1	3	6	9
2	2	7	7
3	1	8	6
4	8	9	10
5	4	10	5

5 Метод усреднения счетов Борда

Построим теперь ранжированный ряд с помощью процедуры усреднения счетов Борда [6]. Счета Борда для каждого подразделения в *B* получаем из таблицы 7. Затем находим среднее этих счетов. Вычеркиваем те подразделения, которые имеют более низкие значения счетов, чем полученное среднее значение. Вычисляем новые счета Борда в уменьшенном множестве подразделений. Находим среднее в этом множестве подразделений. Затем вычеркиваем аналогично подразделения, у которых значения счетов меньше, чем последнее среднее значение. Продолжаем до тех пор, пока не останется какого-либо подразделения, которое можно было бы устранить из нашего уменьшенного множества.

Итак, сначала нужно вычислить

$$\bar{t} = \left(\sum_{a \in B} t(a)\right) \Big/ \|B\| .$$

Затем исключаем $b \in B$, если $t(b) < \bar{t}$ и строим $X = \{a \in B \mid t(a) \geq \bar{t}\}$. Далее применяем ту же самую процедуру к *X*. Продолжим процедуру уменьшения множества до получения $C_1(B)$. Затем исключаем $C_1(B)$ из *B* и применяем всю процедуру снова для получения $C_2(B)$ и т.д.

Теперь применим эту процедуру к данным из таблицы 7. В этом случае $\bar{t}$ = 125/10 = 12,5. Тогда легко получить, что $C_1(B)$ = {3}. После исключения этого подразделения из множества *B* получится укороченная таблица 10.

Действуя по вышеизложенному методу, снова вычисляем из таблицы 10 $\bar{t}$ = 100/9 ≈ 11,1. Следовательно, *X* = {1, 2, 5} и можно получить $C_2(B)$ = {2}. Далее аналогично получаем: $C_3(B)$ = {1}, $C_4(B)$ = {5}, $C_5(B)$ = {8}, $C_6(B)$ = {10}, $C_7(B)$ = {7}, $C_8(B)$ = {4}, $C_9(B)$ = {9}, $C_{10}(B)$ = {6}.

Таблица 10 Счета Борда без третьего подразделения

Подразделение	t_1 (1-F)	t_2 (S)	t_3 (D)	t
1	4	5	6	15
2	8	6	3	17
4	7	2	1	10

Подразделение	t_1 (1-F)	t_2 (S)	t_3 (D)	t
5	6	7	0	13
6	1	0	6	7
7	0	3	6	9
8	4	3	3	10
9	2	1	5	8
10	3	7	1	11

В итоге получаем следующий ранжированный ряд, представленный в таблице 11:

Таблица 11 Результаты четвертого метода

Подразделение	P4	Подразделение	P4
1	3	6	10
2	2	7	7
3	1	8	5
4	8	9	9
5	4	10	6

6 Сравнение результатов 4-х методов

В сравнительной таблице 12 приводятся результаты четырех методов из таблиц 4, 6, 8, 10:

Таблица 12. Сравнение ранжирований

Подразделение	P1	P2	P3	P4	Подразделение	P1	P2	P3	P4
1	3	3	3	3	6	10	9	9	10
2	2	2	2	2	7	8	7	7	7
3	1	1	1	1	8	7	5	6	5
4	6	8	8	8	9	9	10	10	9
5	4	4	4	4	10	5	6	5	6

Как видно из таблицы 12 результаты ранжирований разнятся. Проведем сравнение ранжирований.

Пусть R_1 и R_2 два ранжирования и $\|\rho_{ij}^1\|$ и $\|\rho_{ij}^2\|$ их смежные матрицы, где смежная матрица $\|\rho_{ij}\|$ ранжирования R строится следующим образом:

$\rho_{ij} = 1$ $\Leftrightarrow$ когда *i* предпочтительнее *j* в *R*, иначе равно 0.

Для сравнения ранжирований R_1 и R_2 предлагается использовать известную меру: расстояние Хэмминга. Расстоянием Хэмминга *d(x,y)* между двумя двоичными последовательностями (векторами) *x* и *y* длины *n* называется число позиций, в которых они различны [7, 8]. Расстояние Хэмминга $d(R_1, R_2)$ между R_1 и R_2 в нашем случае определим следующим образом:

$$d(R_1, R_2) = \frac{1}{N \cdot (N-1)} \cdot \sum_{i,j} \left|\rho_{ij}^1 - \rho_{ij}^2\right|.$$

В таблице 13 приводится оценка того, как далеко отстоят полученные ранжирования друг от друга в результате подсчета расстояний Хэмминга. Можно увидеть, что наиболее близкие ранжирования – это полученные методами минимаксной процедуры и счетов Борда, а также методами минимаксной процедуры и усреднения счетов Борда.

Таблица 13. Расстояния Хэмминга между ранжированиями

Метод	1	2	3	4
1	-	0,067	0,056	0,044
2		-	0,022	0,022
3			-	0,044
4				-

Так как расстояние Хэмминга, как мера, является симметрическим, то заполняется только половина таблицы. Необходимо учесть, что эти методы могут дать ранжирования, сильно отличающиеся друг от друга. Однако, в нашем случае все полученные ранжирования достаточно близки друг к другу в терминах расстояния Хэмминга.

Заключение

Задача оценки степени удовлетворения требованиям политики информационной безопасности каждого из подразделений территориально-распределенной организации со сложной структурой — необходимая, хотя и достаточно трудная задача, с которой приходится иметь дело службе информационной безопасности организации. В данной ситуации можно пойти разными путями.

Один из путей — это предложить службе информационной безопасности определить целевую функцию по большому набору переменных, связанных с угрозами, уязвимостями и ущербом, чтобы иметь возможность управлять оказанием различных информационных услуг в зависимости от множества как экономических, так и организационных условий. При этом сотрудники этой службы должны обладать незаурядными способностями по обработке такой информации.

Другой путь предложен в данном докладе. Он позволяет значительно уменьшить информационные требования к сотрудникам службы информационной безопасности организации, предлагая этой службе сформировать функцию выбора, основанную на предлагаемых выше методах ранжирования. В зависимости от задачи, поставленной руководством, например, ввести наказание за допущенные ошибки в процессе обеспечения информационной безопасности подразделений. Или в соответствии с рейтингом по отношению к политике безопасности организации решать задачу оптимального распределения ресурсов организации между подразделениями. Как только службой информационной безопасности организации произведена оценка состояния информационной безопасности в подразделениях, можно принимать соответствующие организационно-технические решения, одобренные руководством организации.

Необходимо отметить, что предложенные методы 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.).

Литература

1. *Козлов А.Д., Нога Н.Л.* Методика ранжирования подразделений распределенной корпоративной системы по степени соответствия политике информационной безопасности / Труды XIII всероссийского совещания по проблемам управления (ВСПУ-2019). М.: ИПУ РАН, 2019. (в печати)
2. *Aleskerov F., Ersel H., Yolalan R.* Multicriterial ranking approach for evaluating bank branch performance. International Journal of Information Technology & Decision Making, Vol. 3, No. 2 (2004), P.321–335,World Scientific Publishing Company.
3. *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). M.: IEEE, 2017. P. 1-5, https://ieeexplore.ieee.org/document/ 8109647
4. *Ларичев О.И.* Теория и методы принятия решений, а также Хроника событий в Волшебных Странах: Учебник. - М.: Логос, 2000. - 296 с.
5. *Подиновский В.В., Ногин В.Д.* Парето-оптимальные решения многокритериальных задач. – 2-е изд. испр. и доп. – М.: ФИЗМАТЛИТ, 2007. – 256 с.

6. *Быстров О.Ф., Поздняков В.Я., Прудников В.М., Перцов В.В., Казаков С.В.* Управление инвестиционной деятельностью в регионах Российской Федерации. - М.: ИНФРА-М, 2008. – 358с.
7. *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)
8. *Alex X. Liu, Ke Shen, Eric Torng.* Large Scale Hamming Distance Query Processing. ICDE Conference, - P.553 — 564, 2011.