

В. В. Золотарев, Е. А. Данилова

О ПРИМЕНЕНИИ ФАКТОРНОГО АНАЛИЗА В ЗАДАЧАХ ОЦЕНКИ ЗАЩИЩЕННОСТИ ЭЛЕМЕНТОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рассматривается возможность применения факторного анализа при оценке состояния защищенности информационных систем. Описывается процедура отбора и классификации факторов, а также расчет влияния факторов на величину результирующего показателя.

Ключевые слова: управление риском, информационный риск, факторный анализ.

Одним из возможных методов анализа защищенности автоматизированных систем является факторный анализ. Этот метод анализа позволяет не только устанавливать причинно-следственные связи между негативными событиями, но и давать им количественную характеристику.

Рассмотрим особенности применения факторной модели оценки защищенности (далее – факторной модели) в задаче оценки защищенности элементов системы электронного документооборота (СЭД). Вместе с тем в предлагаемую модель внесем элементы универсальности, что позволит в общем случае использовать ее для оценки различных элементов как СЭД, так и других автоматизированных систем. Особо отметим применимость предлагаемой модели и решения на ее основе для оценки человеческого фактора.

Описание модели. Пусть существует информационная система IS , которая состоит из N числа элементов E , каждый из которых состоит из K составляющих. Составляющая каждого элемента в определенный промежуток времени может принимать x состояний s с вероятностью r :

$$IS = \{E_l\}, E_l = \left\{ \begin{matrix} s_1^1 & s_2^1 & \dots & s_{x1}^1 \\ s_1^2 & s_2^2 & \dots & s_{x2}^2 \\ \dots & \dots & \dots & \dots \\ s_1^k & s_2^k & \dots & s_{xk}^k \end{matrix} \right\}, \quad (1)$$

где $l \in [1 \dots M]$.

Назовем x количеством степеней свободы элемента. Очевидно, что используя подобную модель системы, можно воспользоваться методом морфологического ящика Цвикки в различных вариантах [1, с. 196]. При этом рассчитать количество причинно-следственных связей между состояниями элементов информационной системы можно рассчитывая их как число размещений с повторениями:

$$k_{\text{сост}} = \left(\sum_{i=1}^N \sum_{j=1}^K x_{s_{ij}} \right)^m, \quad (2)$$

где m – число взаимных связей между элементами. При этом расчете сделан ряд предположений, о которых необходимо упомянуть, поскольку они потенциально ограничивают область применения модели:

– количество степеней свободы необходимо свести к некоторому единому значению, что предполагает стандартный набор состояний составляющих элемента системы;

– необходимо обеспечить полноту исходного набора степеней свободы каждого составляющего элемента системы, что предполагает определенный подход к выбору показателей, определяющих степени свободы;

– частную функцию полезности приходится рассчитывать для каждого элемента системы обособленно, при этом прибегая к упрощению вычислений;

– необходимо обладать информацией о внутренних связях элементов анализируемой системы; для системы с неполной информацией о внутренних связях такой подход без модификации неприменим.

Рассмотрим базовые элементы применяемой факторной модели:

1. Частная функция пригодности элемента E для выполнения основной задачи системы IS (далее – частная функция пригодности):

$$u^*(t) = f(E),$$

где

$$E = \begin{pmatrix} r_1^{(1)}(t) & \dots & r_1^{(x)}(t) \\ r_2^{(1)}(t) & \dots & r_2^{(x)}(t) \\ \dots & \dots & \dots \\ r_m^{(1)}(t) & \dots & r_m^{(x)}(t) \end{pmatrix}, \quad (3)$$

где $r_i^{(j)}(t) = p_i^{(j)}(t) * w_i^{(j)}(t)$; для i -й составляющей в j -м состоянии согласно работе [2]; $i \in [1 \dots K]$, $j \in [1 \dots x]$, $p_i^{(j)}(t)$ – характеризует вероятность непригодности составляющей элемента, находящейся в определенной степени свободы в конкретный момент времени для выполнения заданной функции; $w_i^{(j)}(t)$ – вероятность влияния установленных средств защиты на пригодность составляющей элемента, находящейся в определенной степени свободы в конкретный момент времени. В целом $u^*(t)$, следовательно, характеризует способность конкретного элемента противостоять воздействию. Суть же функции $f(E)$ – вычисление усредненного коэффициента, позволяющего использовать значение u^* для оценки защищенности элемента системы в целом, а не его составляющих, характеризующих значениями $r_i^{(j)}$. Вместе с тем, сохраняя возможность обратной операции разложения на составляющие, можно дополнительно обосновать декомпозицию элемента системы, рассматривая его как набор взаимосвязанных составляющих, что и будет показано далее в примере использования предлагаемой модели.

2. Ориентированный граф $G(V, E)$, представляющий собой модель системы. Вершины – элементы системы –

характеризуются парой $u^*(t)$ и B_e (средней стоимостью средств защиты элемента), а ребра – значением Δu^* , которое показывает соотношение пригодности связанных элементов.

3. Интегральная функция пригодности системы в целом:

$$U(t) = H \sum_{i=1}^N u_i^*(t), \quad (4)$$

где N – количество исследуемых элементов; $H = \{*, +, \max\}$ – множество операций взаимной связи. Выбор конкретной операции определяется видом взаимной связи (или отсутствием таковой) элементов исследуемой системы [2].

В качестве же целевой функции риска можно использовать соотношение

$$R(t) = U(t) \sum_{i=1}^N B_i(t). \quad (5)$$

Таким образом, полезность работы на отрезке времени $[a; b]$ будет равна (согласно функции фон Неймана–Моргенштерна [3]):

$$D = \int_a^b R(t) dt. \quad (6)$$

С учетом формулы (5) для оптимальной конфигурации:

$$\sum_{\tau \in T} D_\tau \rightarrow \min, \quad (7)$$

где T – множество всех анализируемых промежутков времени.

Очевидно, предложенный подход может дополняться критерием связности элементов для выбора оптимальной структуры системы с учетом ранее введенного показателя содержания пар элементов [4]. Рассмотренная факторная модель в совокупности с предложенной функцией пригодности позволяет решать задачу оптимального распределения ресурсов.

Далее рассмотрим отдельные положения предложенного подхода.

Отбор и классификация факторов. Функционирование любой информационной системы происходит в условиях сложного взаимодействия комплекса внутренних и внешних факторов. Фактор – это причина, движущая сила какого-либо процесса или явления, определяющая его характер или одну из основных черт.

Различают множество принципов факторного анализа [5]. Для выполнения поставленной задачи используется детерминированный многофакторный анализ. Чтобы решить задачу учета всего множества факторов, влияющих на информацию, циркулирующую в системе электронного документооборота, предлагается разбить ее на основные составные элементы. При этом для каждого элемента определим возможные состояния, которые он может принимать, затем рассмотрим сочетания этих состояний, создавая базовую модель описания всех возможных частных функций пригодности и моделируя функцию риска в динамике развития системы на основе минимального набора исходных данных.

Используемая модель элемента. Начнем с выделения составляющие элементов системы. Принимая во

внимание, что в работе поставлена цель оценки защищенности элементов системы электронного документооборота, структура которой организационно, технически и с помощью функционально-логических моделей может быть относительно легко описана, основной задачей, определяющей эффективности интегральной оценки, становится описание составляющих элемента. Принимая во внимание выражение (2), уточним задачу как разработку удовлетворяющего выбранным условиям морфологического ящика Цвикки. Итак, с учетом определения автоматизированная система (АС) – это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [6].

На основании определения можем выделить четыре составляющих каждого элемента АС, а именно: технические средства (ТС), программное обеспечение (ПО), персонал (Ч) и организационные меры обработки и защиты информации (различного типа инструкции, регламенты и приказы) (ОМ).

Пусть, учитывая ограничения модели, способность элемента АС выполнять заданные функции описывается статичным набором состояний:

1. Работоспособное (Р) – состояние составляющей элемента АС, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической документации и (или) конструкторской (проектной) документации [7].

2. Неработоспособное – состояние составляющей элемента АС, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно-технической документации и (или) конструкторской (проектной) документации. При этом представим неработоспособные состояния составляющих элемента АС в виде трех категорий:

– отказ (Отк) – событие, заключающееся в нарушении работоспособного состояния составляющей элемента АС, после возникновения которого составляющая элемента АС перестает функционировать и требует постороннего вмешательства для восстановления нормальной работы;

– сбой (С) – самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора [7];

– ошибка (О) – некорректное либо неполное выполнение отдельных задач составляющей элемента АС без потери ее функциональности.

Зададим способ формирования морфологического ящика как исследование сочетаний перечисленного набора состояний составляющих элемента АС. Для проведения оценки защищенности необходимо определить те сочетания, которые могут негативно повлиять на изменение результирующего показателя, т. е. на изменение состояния защищенности информационной системы. При этом введем условия для исключения сочетаний, не несущих в себе интерес для дальнейшего исследования (не влияющих на изменение интеграль-

ного показателя риска или частной функции пригодности элемента).

Исключим следующее:

- взаимосвязи между состояниями одной составляющей элемента АС, приняв, что одновременно в конкретный момент времени возможно только одно состояние составляющей элемента АС;

- взаимосвязь между работоспособными состояниями различных групп элементов как не оказывающих негативного влияния на частную функцию полезности элемента.

Учтем зависимость от порождающего состояния элемента АС, определяющую невозможные технически сочетания состояний морфологического ящика:

- изменение состояния организационных мер (ОМ) может быть вызвано только действиями персонала (Ч);

- состояние отказа технического средства может стать причиной отказа в работе персонала и/или программного обеспечения, но не одновременно;

- при состоянии сбоя технического средства программное обеспечение не может находиться в работоспособном состоянии;

- отказ в работе персонала не может стать причиной изменения состояний других элементов АС.

На основании введенных ограничений можно определить все сочетания состояний элементов АС, изменение которых может привести к изменению состояния защищенности АС (рис. 1). Общее число таких связей можно представить, исключив согласно заданным выше условиям некоторые из них.

Итак, в данном случае получаем 128 сочетаний, которыми можно описать все множество воздействий на элемент АС, при этом довольствуясь минимумом исходных данных, каковыми являются интенсивности отказов отдельных составляющих элемента АС. Полнота и достоверность выявленных связей между состояниями элемен-

тов АС, воздействующих или которые могут воздействовать на информацию, достигается путем рассмотрения множества состояний всех составляющих элемента АС и, как следствие, всех факторов, воздействующих на все элементы АС на всех этапах обработки информации [2].

Расчет вероятности сочетания состояний. Если нам известны вероятности наступления каждого из состояний для всех составляющих элемента АС $P_{sx}(E_i)$, тогда вероятность наступления связанного события P_s можно представить как совместную, при этом применяя следующее выражение и учитывая формулу (1):

$$P_s = r_{si} r_{sj}, \quad (8)$$

где $i, j \in [1..x]$.

При помощи выражения (8) можно рассчитать вероятности возникновения всех 128 связей между состояниями составляющих элемента АС (рис. 1).

Определение зависимостей между состояниями составляющих элемента АС. Связи между состояниями составляющих элемента АС можно представить в виде ориентированного графа GE , вершинами которого будут являться состояния составляющих элемента АС s_{Ei} , ребрами – зависимости между ними (рис. 2).

Исследовав зависимости выбранных состояний друг от друга (рис. 2), сформируем частную функцию полезности элемента на основе факторов (усредненных вероятностей наборов состояний, порождаемых конкретной составляющей элемента АС):

$$u_{E_i}^* = F_1 \cap F_2 \cup F_3 \cap F_4 \cup F_5 \cap F_6 \cap F_7 \cup F_8 \cap F_9 \cap F_{10}, \quad (9)$$

где $u_{E_i}^*$ – частная функция полезности элемента АС; F_1, F_2, \dots, F_{10} – факторы, влияющие на изменение состояния АС; \cap – символ пересечения – если между факторами есть зависимость; \cup – символ объединения – если между факторами нет явной зависимости.

Используя методы математической логики, выражение (9) можно представить в виде

		ТС				ПО				ОМ				Ч			
		Р	О	С	Отк	Р	О	С	Отк	Р	О	С	Отк	Р	О	С	Отк
ТС	Р	■	■	■	■					■	■	■	■	■			
	О	■	■	■	■					■	■	■	■				
	С	■	■	■	■					■	■	■	■				
	Отк	■	■	■	■					■	■	■	■				
ПО	Р	■	■	■	■					■	■	■	■				
	О									■	■	■	■				
	С									■	■	■	■				
	Отк									■	■	■	■				
ОМ	Р	■	■	■	■					■	■	■	■				
	О									■	■	■	■				
	С									■	■	■	■				
	Отк									■	■	■	■				
Ч	Р	■	■	■	■					■	■	■	■				
	О									■	■	■	■				
	С									■	■	■	■				
	Отк									■	■	■	■				

Рис. 1. Морфологический ящик состояний составляющих элемента АС

$$u_{E_i}^* = F_1 F_2 + F_3 F_4 + F_5 F_6 F_7 + F_8 F_9 F_{10}. \quad (10)$$

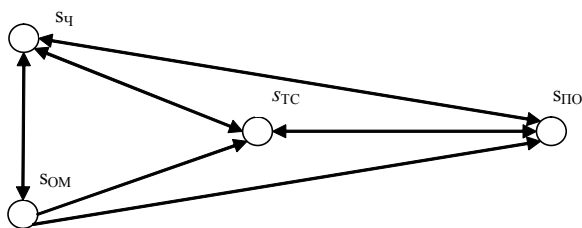


Рис. 2. Граф зависимостей между составляющими элементами информационной системы

Моделирование защищенности элемента исследуемой АС. Для проведения факторного анализа информационных рисков необходимо объект исследования – автоматизированную систему – представить в виде совокупности составляющих элементов. Чем детальнее проработана модель объекта исследования, тем точнее можно определить интегральную функцию полезности, воздействуя при этом некоторые стандартные методы теории надежности, например, метод перебора состояний [8]. Однако стоит помнить, что моделирование объекта исследования стоит производить с позиции целостности и системности, исключая избыточные параметры, не дающие полезной информации для осуществления целей анализа. Объект исследования необходимо рассмотреть с точки зрения логической, технической и структурной схем обработки информации в организации. При факторном анализе может использоваться как отдельно каждая из этих схем, так и все в совокупности, что даст более полную информацию для расчета результирующего показателя, т. е. уровня риска каждого элемента исследуемого объекта. При этом уровень риска каждого из элементов исследуемого объекта представляется в разрезе факторных показателей (с возможной декомпозицией до отдельных состояний составляющих элемента АС). На основании этих данных можно сделать вывод не только о том, какой из элементов наиболее уязвим, но и указать конкретную причину, снижающую уровень информационной безопасности.

Численное моделирование изменения защищенности.

Используя предлагаемый подход, можно осуществить факторное моделирование и оценку защищенности как отдельных элементов АС, так и интегрированного показателя защищенности и риска для всего объекта исследования. Учитывая выражения (6), (7) и следствия указанных соотношений, можно управлять информационной безопасностью объекта, используя минимум исходных данных.

Для примера рассмотрим численное моделирование уровня защищенности центра коллективного доступа системы электронного документооборота организации (т. е., в терминах модели, элемента автоматизированной системы) (см. таблицу, где в скобках указано конечное состояние после реакции элемента на внедрение предложенных мер защиты, рядом – начальное состояние показателя). Интенсивность отказов бралась за конкретный промежуток времени, оговоренный в процессе проведения анализа и составивший 1 операционный месяц (30 суток); расчет интенсивности выполнялся в пересчете на 1 сутки операционного времени центра коллективного доступа на основании отчетов служб технической поддержки организации.

Очевидно, применяемые в данном случае методы обеспечения информационной безопасности элемента системы электронного документооборота не оказали значимого воздействия на систему электронного документооборота в целом, хотя предварительно оценивались руководством организации (исходя из влияния на конкретные составляющие элементов системы) как эффективные. Как видно из примера, предложенный подход позволяет указать на комплексные проблемы элемента системы электронного документооборота, но не позволяет предсказать резкие изменения и единичные нарушения безопасности объекта исследования. Вместе с тем ценность предлагаемого подхода для оперативных, краткосрочных задач управления информационной безопасностью очевидна, как, впрочем, и для моделирования систем защиты без учета влияния нарушителя информационной безопасности (предварительный расчет и выбор оптимальных по стоимости конфигураций средств защиты).

Пример численного моделирования защищенности элемента АС

S_x	P_{ex}	F_1	F_2		u^*
Р(ТС)	0,84(0,94)	0,0328 (0,302)	0,0567 (0,512)		0,0038 (0,0030)
О(ТС)	0,06(0,03)				
С(ТС)	0,1 (0)				
Отк(ТС)	0 (0,03)				
		F_3	F_4		
Р(ПО)	0,68(0,79)	0,0286 (0,0224)	0,0595 (0,0560)		
О(ПО)	0,23(0,09)				
С(ПО)	0,06(0,09)				
Отк(ПО)	0,03(0,03)				
		F_5	F_6	F_7	
Р(ОМ)	0,91(0,97)	0,0157 (0,0123)	0,0254 (0,0227)	0,0436 (0,0421)	
О(ОМ)	0,06(0,03)				
С(ОМ)	0 (0)				
Отк(ОМ)	0,03 (0)				
		F_8	F_9	F_{10}	
Р(Ч)	0,38(0,51)	0,0564 (0,0520)	0,0620 (0,0594)	0,0540 (0,0487)	
О(Ч)	0,5 (0,4)				
С(Ч)	0,06(0,09)				
Отк(Ч)	0,06 (0)				

С помощью предложенного подхода можно учитывать причинно-следственные связи процессов обработки информации, влияющие на уровень защищенности информационных ресурсов. Использование факторного анализа является шагом к получению объективных количественных результатов в процессе управления информационной безопасностью.

Библиографические ссылки

1. Волкова В. Н., Денисов А. А. Теория систем и системный анализ : учебник для вузов. М. : Изд-во «Юрайт», 2010.
2. Применение факторного анализа и эволюционного алгоритма оптимизации для решения задачи управления информационными рисками систем электронного документооборота / В. Г. Жуков [и др.] // Системы управления и информационные технологии. 2009. № 3(37). С. 41–50.

3. Беллман Р. Калаба Р. Динамическое программирование и современная теория управления. М. : Наука, 1969.
4. Антамошкин А. Н., Золотарев В. В. Алгоритм расчета прогнозируемого графика при проектировании распределенных систем обработки и хранения информации // Вестник СибГАУ. 2006. № 1. С. 5–10.
5. Сафонов А. А. Теория экономического анализа : учеб. пособие / под ред. Л. В. Моисеевой. Владивосток : Изд-во Владивост. гос. ун-та экономики и сервиса.
6. ГОСТ 34.003–90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. М. : Изд-во стандартов, 1990.
7. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. М. : Изд-во стандартов, 1989.
8. Половко А. М., Гуров С. В. Основы теории надежности. 2-е изд., перераб. и доп. СПб. : БХВ-Петербург, 2006.

V. V. Zolotarev, E. A. Danilova

ABOUT APPLICATION OF THE FACTORIAL ANALYSIS IN PROBLEMS OF THE AUTOMATED SYSTEMS ELEMENTS SECURITY ESTIMATION

This article considers a possibility of application of the factorial analysis in estimation of information systems security condition. A procedure of selection and classification of factors is described and calculation of influence of factors on size of result indicator is given here as well.

Keywords: risk management, information security risk, factorial analysis.

© Золотарев В. В., Данилова Е. А., 2010

УДК 534.121.1

А. В. Лопатин, П. О. Деев

ОПРЕДЕЛЕНИЕ ОСНОВНОЙ ЧАСТОТЫ КОЛЕБАНИЙ ПРЯМОУГОЛЬНОЙ ТРЕХСЛОЙНОЙ ПЛАСТИНЫ СО СВОБОДНЫМ КРАЕМ¹

Решена задача определения основной частоты колебаний трехслойной пластины, у которой три края жестко закреплены, а один край свободен. Вариационные уравнения движения пластины были получены с помощью принципа Гамильтона. Решение этих уравнений было выполнено методом Канторовича и обобщенным методом Галеркина.

Ключевые слова: трехслойная пластина, частота колебаний, обобщенный метод Галеркина.

Исследование изгибных колебаний трехслойных пластин является важным этапом их проектирования. Трехслойные пластины, совершающие изгибные колебания, обладают самыми разнообразными способами закрепления краев. К настоящему времени большинство решений задач об определении частот колебаний трехслойных пластин получены для случая, когда все четыре края шарнирно закреплены. Большой практический интерес пред-

ставляет задача динамического анализа трехслойной пластины, в которой один из ее краев свободен, а три других жестко закреплены. Для трехслойных пластин рассматриваемая задача не имеет до настоящего времени своего решения. Такая ситуация обусловлена трудностями выбора функций, аппроксимирующих форму пластины в рамках моделей, учитывающих особенности движения трехслойной структуры. Вместе с тем из общей задачи

¹ Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России на 2009–2013 гг.».