УДК 681.5:303.732.4
ББК 32.965
Л 86

Луценко Е.В.
Доктор экономических наук, кандидат технических наук, профессор кафедры автоматизированных систем обработки информации и управления физического факультета Адыгейского государственного университета, тел. (8772) 59-39-11

Коржаков В.Е.
Кандидат технических наук, доцент, зав. кафедрой автоматизированных систем обработки информации и управления физического факультета Адыгейского государственного университета, тел. (8772) 59-39-11, e-mail: korvie@yandex.ru

Системно-когнитивный анализ объектов информационной безопасности

(Рецензирована)

Аннотация

Предлагается математическая модель, основанная на системной теории информации, а также численный метод и специальный программный инструментарий (система «Эйдос»), которые позволяют создавать и эксплуатировать в режиме адаптации и периодического синтеза многофакторные информационные модели объектов информационной безопасности (ОИБ). На основе использования данных моделей могут быть определены точки уязвимости ОИБ и предложены комплексные меры по обеспечению необходимого уровня защищенности ОИБ от угроз.

Ключевые слова: *программный инструментарий - система «Эйдос», информационные модели объектов информационной безопасности, уровни защищенности ОИБ от угроз.*

Lutsenko E.V.
Doctor of Economics, Candidate of Technical Sciences, Professor of Department of Automated Systems of Processing Information and Control at Physical Faculty of Adyghe State University, ph. (8772) 59-39-11

Korzhakov V.E.
Candidate of Technical Sciences, Assistant Professor, Head of Department of Automated Systems of Processing Information and Control at Physical Faculty of Adyghe State University, ph. (8772) 59-39-11, e-mail: korvie@yandex.ru

The system-cognitive analysis of objects of information security

Abstract

The mathematical model basing on the system theory of the information, as well as a numerical method and special program toolkit (system «Eidos») are offered. They allow creation and maintenance of multiple-factor information models of objects of information security (OIS) in a mode of adaptation and periodic synthesis. On the basis of use of these models points of vulnerability of OIS can be defined and the complex measures on maintenance of necessary level of OIS security from threats are proposed.

Key words: *program toolkit - system «Eidos», information models of objects of information security, levels of OIS security from threats.*

Постановка задачи. Пусть существует ряд угроз объекту информационной безопасности (ОИБ). Степень опасности каждой угрозы зависит от значений ряда факторов, повышающих или понижающих защищенность ОИБ от данной угрозы. Факторы, понижающие защищенность ОИБ будем называть *факторами риска*, а повышающими ее – *факторами защищенности*. Интегральная оценка уязвимости и защищенности ОИБ является функцией его защищенности от каждого вида угроз.

Существует несколько вариантов формализации зависимости степени защищенности ОИБ от факторов:

1. Каждая угроза y зависит от одного фактора x, т.е. между степенью угрозы и значениями фактора существуют отношения взаимно-однозначного соответствия. В этом случае эту зависимость можно выразить в виде однозначной функции одного аргумента $y = f(x)$.

2. Каждая угроза y зависит от значений многих факторов $\{x_i\}$. Такую зависимость можно выразить в виде однозначной функции многих аргументов

$$y = f(x_1, ..., x_i).$$

3. Одни и те же факторы $\{x_i\}$ в общем случае оказывают влияние на степень защищенности ОИБ не от одного, а от многих видов угроз $\{y_j\}$. В этом случае каждая угроза является многозначной функцией многих аргументов

$$y_1, ..., y_j = f(x_1, ..., x_i).$$

Задача построения математической модели ОИБ состоит в определении вида функции f *непосредственно на основе эмпирических данных*. На основе этой модели решаются подзадачи:

1. Определение силы и направления действия факторов, влияющих на защищенность ОИБ.
2. Оптимизация системы факторов ОИБ путем исключения несущественных.
3. Оценка адекватности математической модели ОИБ.
4. Идентификация и прогнозирование защищенности ОИБ от системной угрозы.
5. Поддержка принятия решений и выработка рекомендаций по реструктуризации и оптимизации системы безопасности ОИБ.
6. Построение семантических сетей угроз и факторов риска (безопасности).
7. Построение когнитивных диаграмм угроз и факторов риска (безопасности).

Первым шагом на пути построения математической модели является выбор количественной меры, позволяющей измерять степень влияния фактора на исследуемый параметр. К этой мере предъявляется ряд требований [1], основными из которых являются сопоставимость, интерпретируемость и вычислимость на основе непосредственно эмпирических данных.

Традиционный подход к понятию эластичности

Рассмотрим первый вариант формализации зависимости степени защищенности ОИБ от факторов (взаимно-однозначное степени защищенности ОИБ от угрозы y в зависимости от значений фактора x) $y = f(x)$.

Понятие эластичности. *Коэффициент эластичности показывает относительное изменение исследуемого параметра системы под действием единичного относительного изменения некоторого фактора* [2]. Это понятие является обобщением понятия производной с учетом требования безразмерности и сопоставимости.

Эластичность в непрерывном случае. Пусть численное значение некоторого параметра экономической, социально-психологической или организационно-технической системы описывается переменной y, зависящей от фактора x и эта зависимость описывается функцией $y = f(x)$. Тогда степень и направление влияния фактора x на параметр y можно численно измерить производной (1), представляющей собой предел отношения абсолютных изменений величин y и x:

$$y_x = \lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x}. \tag{1}$$

Однако применение производной не очень удобно, т.к. она зависит от *размерности* величин y и x и по этой причине обладает недостаточной *сопоставимостью* в пространстве и времени. Кроме того, сама по себе скорость абсолютного изменения некоторого параметра объекта безотносительно к средней величине этого параметра, содержит недостаточно информации об этом объекте. Например, если на очередных выборах за некоторого кандидата отдано на 500 голосов больше, чем на предыдущих, то важно знать, а *на сколько это процентов больше*.

Поэтому *в экономике* введено понятие *эластичности* функции $y = f(x)$, которое определяется как предел отношения не абсолютных, а *относительных* изменений значений переменных y и x:

$$E_x(y) = \lim_{\Delta x \to 0}\left(\left(\frac{\Delta y}{y}\right) \Big/ \left(\frac{\Delta x}{x}\right)\right) = \lim_{\Delta x \to 0}\left(\frac{\Delta y}{\Delta x}\cdot\frac{x}{y}\right) =$$

$$\lim_{\Delta x \to 0}\frac{\Delta y}{\Delta x}\cdot\frac{x}{y} = \frac{dy}{dx}\cdot\frac{x}{y} = \frac{f^{/}(x)}{\frac{y}{x}} = \frac{f^{/}(x)}{\overline{f}(x)}, \tag{2}$$

$$E_x(y) = \frac{f^{/}(x)}{\overline{f}(x)},\ \textit{где}\ \ f^{/}(x) - \textit{производная, а}\ \ \overline{f}(x) - \textit{среднее функции}\ \ f(x).$$

Так как $d\ln y = dy/y$ и $d\ln x = dx/x$, то эластичность можно представить в виде логарифмической производной

$$E_x(y) = \frac{d\ln(f(x))}{d\ln(x)}. \tag{3}$$

Как исключительно удачное, автор предлагает применить понятие эластичности для исследования и управления не только экономическими, но и социально-психологическими, и организационно-техническими системами, прежде всего объектами информационной безопасности (ОИБ).

Эластичность в дискретном случае. Для численных расчетов необходимо перейти к *дискретному случаю*, в частности для численного взятия производных используем *метод конечных разностей*. В конечных разностях выражение (3) принимает вид:

$$E_x(y) = \frac{\Delta\ln(f(x))}{\Delta\ln x} = \frac{\ln(f(x_2)) - \ln(f(x_1))}{\ln(x_2) - \ln(x_1)} = \frac{\ln(f(x_2)/f(x_1))}{\ln(x_2/x_1)}. \tag{4}$$

Свойства эластичности. Рассмотрим некоторые свойства эластичности, которые, как мы заметили, *удивительным образом* полностью или частично совпадают со свойствами логарифма (таблица 1).

Таблица 1

Свойства эластичности и логарифма

№	Эластичность	Логарифм	Примечание
1.	Эластичность взаимно-обратной функции взаимно-обратна: $E_X(y) = \frac{dy}{dx} \cdot \frac{x}{y} = \frac{1}{\frac{dx}{dy} \cdot \frac{y}{x}} = \frac{1}{E_Y(x)}$	Логарифм взаимно-обратной функции равен той же функции с обратным знаком: $\ln y = -(\ln 1 - \ln y) = -\ln \frac{1}{y}$	Совпадает по модулю (с точностью до знака)
2.	Эластичность произведения двух функций одного аргумента равна сумме эластичностей функций: $E_x(uv) = \frac{d(uv)}{dx} \cdot \frac{x}{uv} = \frac{v\left(\frac{du}{dx}\right) + u\left(\frac{dv}{dx}\right)}{uv} = \frac{du}{dx} \cdot \frac{x}{u} + \frac{dv}{dx} \cdot \frac{x}{v} = E_x(u) + E_x(v)$	Логарифм произведения двух функций одного аргумента равна сумме логарифмов функций: $\ln(uv) = \ln(u) + \ln(v)$	Полностью совпадает
3.	Эластичность частного двух функций одного аргумента равна разности эластичностей функций: $E_X(u/v) = \frac{d(u/v)}{dx} \cdot \frac{x}{u/v} = \frac{v \cdot du - u \cdot dv}{v^2} \cdot \frac{xv}{u} = \frac{du}{dx} \cdot \frac{x}{u} - \frac{dv}{dx} \cdot \frac{x}{v} = E_X(u) - E_X(v)$	Логарифм частного двух функций одного аргумента равна разности логарифмов функций: $\ln(u/v) = \ln(u) - \ln(v)$	Полностью совпадает
4.	Эластичность показательной функции $y = a^X$ пропорциональна показателю степени: $E_X(y) = \frac{da^X}{dx} \cdot \frac{x}{a^X} = a^X \cdot x \cdot \frac{\ln a}{a^X} = x \cdot \ln a$	Логарифм показательной функции $y = a^X$ пропорционален показателю степени: $\ln a^X = x \cdot \ln a$	Полностью совпадает
5.	Область значений эластичности: $-\infty < E < +\infty$	Область значений логарифма: $-\infty < ln < +\infty$	Полностью совпадает

Необходимо отметить, что ряд других свойств эластичности, таких как эластичность суммы функций, эластичность линейной функции и др., *не совпадают* со свойствами логарифма.

Итак, учитывая свойства эластичности 2-5, мы видим, что *многие свойства эластичности такие же, как свойства логарифмической функции*. Это позволяет высказать *гипотезу*, что эластичность каким-то образом связана с количеством информации, т.к. во все выражения для количества информации Хартли-Найквиста-Больцмана, Шеннона и Харкевича входит логарифмическая функция.

Какая же из этих мер информации в наибольшей степени соответствует понятию эластичности? Ключевым в решении этого вопроса является свойство 5 (таблица 1):

область значений мер Хартли-Найквиста-Больцмана и Шеннона изменяется от 0 до $+\infty$; область значений меры Харкевича, как и эластичности, изменяется от $-\infty$ до $+\infty$, как и эластичности. Однако классическая мера семантической целесообразности информации мера Харкевича не удовлетворяет *принципу соответствия* с мерой Хартли в детерминистском случае, поэтому автором данной статьи в работе [3] предложена *системная мера целесообразности информации* (5) (рис. 1), в последующем получившая развитие в работах [4] и [1]:

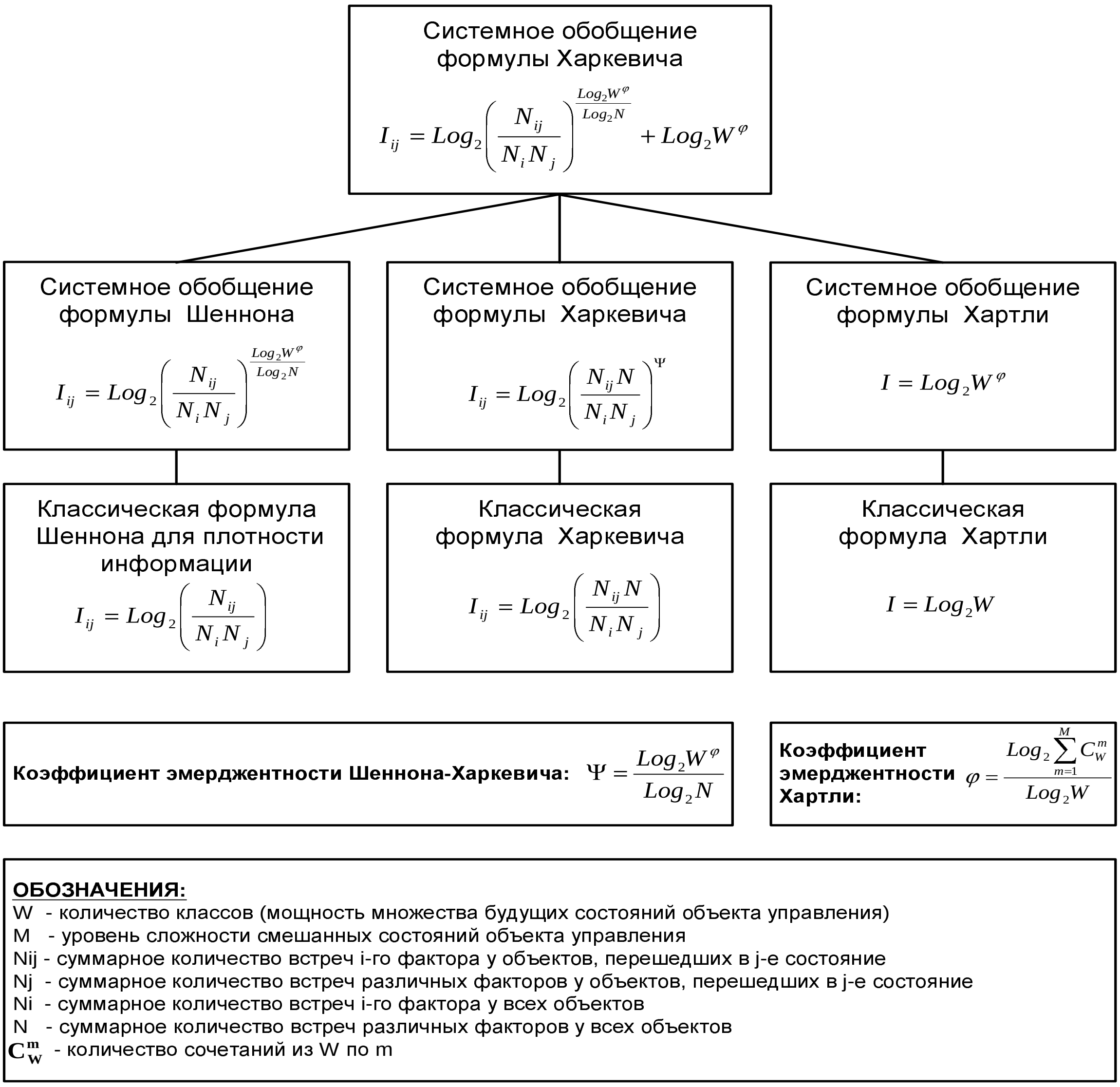

Рис. 1. Генезис выражения для системной целесообразности информации

$$I_{ij} = Log_2\left(\frac{N_{ij}}{N_i N_j}\right)^{\frac{Log_2 W^{\varphi}}{Log_2 N}} + Log_2 W^{\varphi}. \quad (5)$$

В выражении (5) вероятности связаны с абсолютными частотами в соответствии с выражениями (6):

$$P_{ij} = \frac{N_{ij}}{N_i},\ P_i = \frac{N_i}{N},\ P_j = \frac{N_j}{N},$$
$$\textit{где}\ N_i = \sum_{j=1}^{W} N_{ij},\ N_j = \sum_{i=1}^{A} N_{ij},\ N = \sum_{i=1}^{W} \sum_{j=1}^{A} N_{ij}. \tag{6}$$

Учитывая (6) в (5), получим:

$$I_{ij} = \Psi \cdot Log_2 \frac{P_{ij}}{P_j}, \tag{1}$$

где

P_{ij} – вероятность достижения объектом управления j-й цели при условии сообщения ему i-й информации;

P_j – вероятность самопроизвольного достижения объектом управления j-й цели;

Ψ – коэффициент эмерджентности А. Харкевича* (8):

$$\Psi = \frac{Log_2 W^{\varphi}}{Log_2 N}; \tag{2}$$

φ – коэффициент эмерджентности Р. Хартли** (9):

$$\varphi = \frac{Log_2 \sum_{m=1}^{M} C_W^m}{Log_2 W}. \tag{3}$$

По своему смыслу и математической природе понятие эластичности является детерминистским, а предложенная системная мера целесообразности информации – статистической. Поэтому для проведения более детального сравнения этих мер и обеспечения полной их сопоставимости упростим выражение (7) до детерминистского случая. Кроме того, это позволит аналитически вывести выражения этой меры для различных математических функций.

Детерминистская интерпретация системной меры целесообразности информации для математических функций

Пусть целью является значение аргумента.

В статистическом случае вероятность наблюдения некоторого значения функции в точке является пределом, к которому стремится частота при неограниченном возрастании количества наблюдений (10):

$$E_x(y) = \lim_{\Delta x \to 0}\left(\left(\frac{\Delta y}{y}\right) \Big/ \left(\frac{\Delta x}{x}\right)\right) = \lim_{\Delta x \to 0}\left(\frac{\Delta y}{\Delta x} \cdot \frac{x}{y}\right) =$$
$$\lim_{\Delta x \to 0} \frac{\Delta y}{\Delta x} \cdot \frac{x}{y} = \frac{dy}{dx} \cdot \frac{x}{y} = \frac{f^{/}(x)}{\frac{y}{x}} = \frac{f^{/}(x)}{\overline{f}(x)}, \tag{10}$$

$$E_x(y) = \frac{f^{/}(x)}{\overline{f}(x)},\ \textit{где}\ \ f^{/}(x) - \textit{производная, а}\ \ \overline{f}(x) - \textit{среднее функции}\ \ f(x).$$

---

* *Получен в 2002 году Е.В. Луценко в [2] и назван им в честь этого выдающегося отечественного ученого.*

** *Получен в 2002 году Е.В. Луценко в [2] и назван им в честь этого выдающегося отечественного ученого.*

Таблица 2

Свойства эластичности и детерминистской системной меры целесообразности информации

№	Эластичность	Системная мера целесообразности информации	Примечание
1.	Эластичность взаимно-обратной функции взаимно-обратна: $E_X(y) = \frac{dy}{dx} \cdot \frac{x}{y} = \frac{1}{\frac{dx}{dy} \cdot \frac{y}{x}} = \frac{1}{E_y(x)}$	Логарифм взаимно-обратной функции равен той же функции с обратным знаком: $\ln y = -(\ln 1 - \ln y) = -\ln \frac{1}{y}$	Совпадает по модулю (с точностью до знака)
2.	Эластичность произведения двух функций одного аргумента равна сумме эластичностей функций: $E_X(uv) = \frac{d(uv)}{dx} \cdot \frac{x}{uv} = \frac{v\left(\frac{du}{dx}\right) + u\left(\frac{dv}{dx}\right)}{uv} = \frac{du}{dx} \cdot \frac{x}{u} + \frac{dv}{dx} \cdot \frac{x}{v} = E_X(u) + E_X(v)$	Логарифм произведения двух функций одного аргумента равна сумме логарифмов функций: $\ln(uv) = \ln(u) + \ln(v)$	Полностью совпадает
3.	Эластичность частного двух функций одного аргумента равна разности эластичностей функций: $E_X(u/v) = \frac{d(u/v)}{dx} \cdot \frac{x}{u/v} = \frac{v \cdot du - u \cdot dv}{v^2} \cdot \frac{xv}{u} = \frac{du}{dx} \cdot \frac{x}{u} - \frac{dv}{dx} \cdot \frac{x}{v} = E_X(u) - E_X(v)$	Логарифм частного двух функций одного аргумента равна разности логарифмов функций: $\ln(u/v) = \ln(u) - \ln(v)$	Полностью совпадает
4.	Эластичность показательной функции $y = a^X$ пропорциональна показателю степени: $E_X(y) = \frac{da^X}{dx} \cdot \frac{x}{a^X} = a^X \cdot x \cdot \frac{\ln a}{a^X} = x \cdot \ln a$	Логарифм показательной функции $y = a^X$ пропорционален показателю степени: $\ln a^X = x \cdot \ln a$	Полностью совпадает
5.	Область значений эластичности: $-\infty < E < +\infty$	Область значений логарифма: $-\infty < ln < +\infty$	Полностью совпадает

С этой мерой и предлагается ассоциировать эластичность. Использован термин «ассоциировать», а не «отождествить», т.к. не все свойства эластичности совпадают со свойствами системной информационной меры. Несмотря на это, применение данной информационной меры вместо классической эластичности оправдано тем, что эластичность не определена для однозначных функций и многозначных функций многих переменных, а также для нечетких функций, тогда как именно для этого общего случая разработан универсальный численный метод и инструментарий, позволяющие проводить *информационные расчеты влияния факторов на параметры систем на основе непосредственно эмпирических данных*.

Предлагаемая модель, численный метод и инструментарий

Рассмотрим формы представления эмпирических данных для численных расчетов эластичности при трех различных вариантах формализации зависимости степени защищенности ОИБ от факторов, приведенных в постановке задачи (таблицы 2–5).

Вопрос о смысле значений фактора x_i остается открытым и требует решения. В данной статье, как и в работе [1], предлагается в качестве значений фактора рассматривать количество информации, содержащейся в факте наблюдении данного фактора о том, что функция примет определенное значение x.

Таблица 3

Форма представления эмпирических данных для расчета эластичности взаимно-однозначной функции одного аргумента

$f(x)$	$f_1(x_1)$	$f_2(x_2)$	–	$f_w(x_M)$
x_1	x_{11}	–	–	–
x_2	–	x_{22}	–	–
–	–	–	–	–
x_M	–	–	–	x_{MW}

Численный расчет эластичности в этом случае осуществляется на основе выражения (4), модифицированного для этого случая формулы (5):

$$E_x(y) = \frac{\ln(f_2(x_{22}) / f_1(x_{11}))}{\ln(x_{22} / x_{11})}. \tag{4}$$

Таблица 4

Форма представления эмпирических данных для расчета эластичности взаимно-однозначной функции многих аргументов

$f(x_1,\dots,x_M)$	$f_1(x_1,\dots,x_M)$	$f_2(x_1,\dots,x_M)$	…	$f_w(x_1,\dots,x_M)$
x_1	x_{11}	x_{12}	…	x_{1W}
x_2	x_{21}	x_{22}	…	x_{2W}
…	…	…	…	…
x_M	x_{M1}	x_{M2}	…	x_{MW}

Численный расчет эластичности в этом случае осуществляется на основе формулы (4), обобщенной для случая многих переменных (6):

$$E_x(y) = \frac{\partial \ln(f(x_1,\dots,x_M))}{\partial \ln x_i} = \frac{\ln(f_j(x_i) / f_{j-1}(x_{i-1}))}{\ln(x_i / x_{i-1})}. \tag{5}$$

Предлагается эластичность, рассчитанную согласно выражению (6), называть *частной эластичностью*. Введем понятие *интегральной эластичности*, под которой понимается некоторая функция, аргументами которой является частная эластичность ОИБ для всех факторов. Будем различать аддитивную интегральную эластичность для непрерывного и дискретного случая, которая адекватна в том случае, если ни один из факторов не имеет определяющего влияния на уровень защищенности ОИБ (7):

$$IE_x(y) = \int_1^M \frac{\partial \ln(f(x_1,\dots,x_M))}{\partial \ln x_i} di = \sum_{i=2}^{M} \frac{\ln(f_j(x_i) / f_{j-1}(x_{i-1}))}{\ln(x_i / x_{i-1})}, \tag{6}$$

и мультипликативную интегральную эластичность, применимую в случае, когда некоторые из факторов безопасности или риска имеет определяющее (решающее) влияние на общий уровень защищенности ОИБ (8):

$$IE_X(y) = \prod_{i=2}^{M}\left(ТМВУ - \frac{\ln(f_j(x_i) / f_{j-1}(x_{i-1}))}{\ln(x_i / x_{i-1})} \right). \qquad (7)$$

Здесь использовано обозначение для нового, предлагаемого в рамках данной статьи, понятия: *теоретически максимально-возможный ущерб* (ТМВУ), который определяется как эластичность детерминистского фактора, в результате действия которого некоторый жизненно-важный параметр ОИБ принимает неприемлемое значение. Численно ТМВУ равен количеству информации, которое мы получаем о степени защищенности ОИБ из факта о действии данного смертельно-опасного детерминистского фактора. Если встречается хотя бы один подобный фактор – значение мультипликативной интегральной эластичности принимает нулевое значение, если же подобных факторов нет - то оно положительно и тем выше, чем выше защищенность ОИБ.

Предложенная численная мера системной целесообразности информации позволяет вычислить численное значение ТМВУ для любого конкретного ОИБ, о котором есть необходимые *исходные данные*. Если обычные факторы риска могут привести к определенному ущербу ОИБ, то решающие факторы риска могут привести к непоправимому ущербу для ОИБ или его уничтожению. Возможен и смешанный вариант, при котором одни факторы имеют определенное положительное и отрицательное влияние на защищенность ОИБ, а другие имеют решающее значение.

Таблица 5

Форма представления данных для расчета эластичности в случае многозначной функции многих аргументов

$f(x_1,\ldots,x_M)$	$f_1(x_1,\ldots,x_M)$	$f_2(x_1,\ldots,x_M)$	…	$f_w(x_1,\ldots,x_M)$
x_1	x_{11}	x_{12}	…	x_{1W}
x_2	x_{21}	x_{22}	…	x_{2W}
…	…	…	…	…
x_M	x_{M1}	x_{M2}	…	x_{MW}

Численный расчет частной эластичности в этом случае осуществляется с использованием выражения (6), а интегральной эластичности ОИБ по каждому параметру – по формулам (7) или (8). Многозначность в данном случае выражается в том, что одно и то же сочетание факторов (т.е. некоторое определенное сочетание факторов) обуславливает некоторые различные значения *каждого параметра* защищенности (уязвимости) ОИБ и всего объекта в целом.

Математическая модель эластичности, основанная на системной теории информации. В классической теории информации Шеннона, созданной на основе обобщения результатов Больцмана, Найквиста и Хартли, само понятие информации определяется на основе теоретико-множественных и комбинаторных представлений на основе анализа поведения классического макрообъекта, который может переходить только в четко фиксированные альтернативные редуцированные состояния. Однако, квантовые объекты и сложные активные рефлексивные системы могут оказываться одновременно в двух и более альтернативных для классических объектов состояниях. Та-