ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ

УДК 004.8

ОЦЕНКА ЭФФЕКТИВНОСТИ ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

Е. А. Андреева, Я. А. Галустьян
Омский государственный технический университет, г. Омск, Россия
Научный руководитель: Данилова О.Т., к.ф.–м.н., доцент

Аннотация. **В данной статье представлен подход к оценке взаимосвязи защитных мер, уязвимостей и угроз. Оценка проводилась с применением графовой модели с полным перекрытием, что позволило сформировать матрицу парных сравнений. Приоритеты для выбранных наборов защитных мер, уязвимостей и угроз определены по методу парных сравнений. Полученное значение остаточной вероятности реализации всех возможных угроз позволяет судить о защищенности системы в целом.**

Ключевые слова: безопасность, оценка эффективности, метод иерархий.

DOI: 10.25206/2310-4597-2019-1-184-187

I. ВВЕДЕНИЕ

На данный момент существует множество методик оценки угроз безопасности. В данной работе представлено использование метода парных сравнений для количественной оценки угроз защищаемому объекту. Данный метод не приводит к «правильному» решению, а лишь определяет суть проблемы и требования к ее решению

Оценка эффективности систем защиты информации в Российской Федерации опираются на руководящие документы, изданные ФСТЭК, а также на ГОСТы, например ГОСТ Р ИСО/МЭК 15408-1-2012 и другие. Так же на основе требований, предъявляемых к данной системе защиты, при помощи используемого метода была количественно определена оценка эффективности этих требований применительно к данной системе [1].

II. ПОСТАНОВКА ЗАДАЧИ

Для достижения поставленных целей в качестве объекта исследования была выбрана автоматизированная система (АС). Источниками осуществления инцидентов информационной безопасности являются уязвимости, приводящие к реализации угроз. Угрозы информационной безопасности проявляются через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости.

Основной задачей исследования является выявление требований, предъявляемых к системе защите определенного объекта информатизации, а также оценка эффективности использования данных требований.

III. ТЕОРИЯ

Суть метода заключается в сравнении изучаемых факторов между собой. Цель сравнения – выявить наиболее приоритетный фактор.

Основным элементом, показывающим эффективное взаимодействие между факторами, является матрица парных сравнений. При сравнении пары факторов необходимо установить, какой из факторов лучше (хуже) другого по отношению к их воздействую на общую для них характеристику, выражая данную связь количественной оценкой.

Данная матрица парных сравнений должна удовлетворять следующим требованиям:

– на главной диагонали матрицы всегда ставится 1, т.к. $a_{ij}=a_{ji}$,при $j=i$;

– должно выполняться условие, что, если при сравнении i–го элемента матрицы с j–м элементом ставится оценка a_{ij}, то при обратном сравнении – a_{ji}, т.е. $a_{ji}=1/a_{ij}$ [2].

Общее представление матрицы парных сравнений отображено в табл. 1.

ТАБЛИЦА 1
ОБЩЕЕ ПРЕДСТАВЛЕНИЕ МАТРИЦЫ ПАРНЫХ СРАВНЕНИЙ

Факторы	$\mathbf{A_1}$	$\mathbf{A_2}$	**...**	$\mathbf{A_n}$
$\mathbf{A_1}$	1	a_{12}		a_{1n}
$\mathbf{A_2}$	a_{21}	1		a_{2n}
...			...	
$\mathbf{A_n}$	a_{n1}	a_{n2}		1

Для сравнения факторов чаще всего используется шкала относительной значимости, которая представляет собой ряд числовых значений от 1 до 9. Данное представление шкалы относительной значимости приведено в таблице 2 [3].

ТАБЛИЦА 2
ПРЕДСТАВЛЕНИЕ ШКАЛЫ ОТНОСИТЕЛЬНОЙ ЗНАЧИМОСТИ

Описание отношения первого объекта ко второму	**Лингвистическая переменная**
Абсолютное (подавляющее) превосходство	9
Очевидное превосходство	7
Сильное (существенное) превосходство	5
Умеренное (слабое) превосходство	3
Равная значимость	1

IV. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

В рассмотренной системе были выявлены наиболее вероятные уязвимости, приводящие к реализации соответствующих угроз.

Для определения взаимосвязей между уязвимостями (r_i), угрозами (o_i) и требованиями по обеспечению защитных мер (d_i) обратимся к теоретико-графовому подходу в виде модели с полным перекрытием (рис. 1).

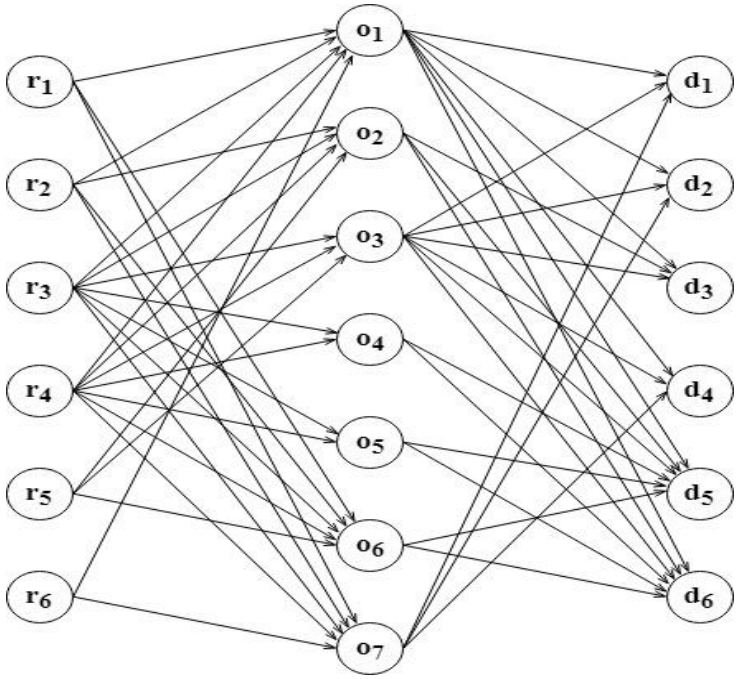

Рис. 1. Граф взаимодействия защитных мер, угроз и уязвимостей

В представленной модели вершины графа представляют собой совокупности:

1) требований к системе защиты

$$D = \{d_1; d_2; d_3; d_4; d_5; d_6\};$$

2) возможных угроз

$$O = \{o_1; o_2; o_3; o_4; o_5; o_6; o_7\};$$

3) предполагаемых уязвимостей

$$R = \{r_1; r_2; r_3; r_4; r_5; r_6\}.$$

Далее следует перейти к формированию матрицы парных сравнений, весовые коэффициенты в которой будут представлены значениями вероятностей реализации угроз при выявлении соответствующей им уязвимостей. Последовательность исполнения такой задачи производится в следующем порядке [3, 4].

1. Вычисление показателя важности каждого из факторов a_i по формуле:

$$a_i = \sum_{j=1}^{n} a_{ij}, \text{где } i = 1, \dots, n \quad (1)$$

2. Определение суммарного показателя важности всех факторов a_j:

$$a_c = \sum_{i=1}^{n} a_i \quad (2)$$

3. Расчет весовых коэффициентов факторов P_i производится по следующей формуле:

$$P_i = \frac{a_i}{a_c}, \text{где } i = 1,2, \dots, n \quad (3)$$

В табл. 3 представлены значения, определенные по результатам расчетов, для выбранных перечней угроз, уязвимостей и защитных мер.

ТАБЛИЦА 3
ПЕРЕЧЕНЬ УГРОЗ, УЯЗВИМОСТЕЙ И ЗАЩИТНЫХ МЕР

№	Наименование	Значение
	Угрозы	
1	Несанкционированный доступ (НСД) к защищаемой информации	0,2
2	Негативное воздействие на программно–технические компоненты информационной системы (ИС)	0,1
3	Внесение неисправностей, уничтожения технических и программно технических компонентов ИС путём физического воздействия	0,05
4	Хищение (утрата) носителей информации и производственных отходов	0,15
5	Компрометация технологической (аутентификационной) информации путём визуального несанкционированного просмотра и подбора с использованием штатных средств	0,25
6	Выведение компьютера из строя	0,15
7	Осуществление НСД к информации при ее передаче	0,1
	Уязвимости	
1	Недостаток разграничения доступа	0,15
2	Наличие вредоносного программного обеспечения	0,25
3	Недостаток организации технической защиты информации от НСД	0,15
4	Невнимательность сотрудников	0,25
5	Сбои в работе аппаратного и программного обеспечения	0,1
6	Реализация протоколов сетевого взаимодействия и каналов передачи данных	0,1
	Защитные меры	
1	Требования по защите информации от НСД	
2	Требования к межсетевым экранам	
3	Требования к средствам вычислительной техники от НСД	
4	Требования к антивирусным средствам	
5	Требования к политике безопасности	
6	Требования к персоналу	

Согласно полученным результатам расчетов определена зависимость угроз при выявлении определенной уязвимости (рис. 2), позволяющая визуализировать значения наиболее значимых угроз защищаемому объекту.

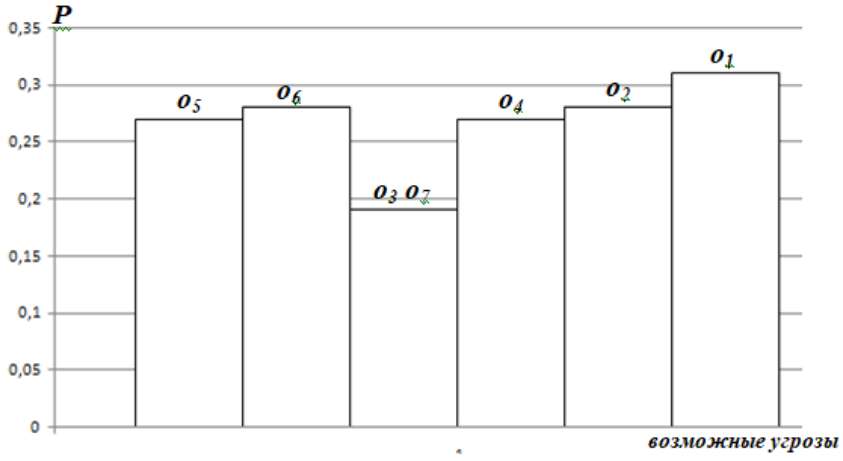

Рис. 2. Гистограмма реализации угроз

Количественная оценка значения остаточной вероятности реализации всех возможных угроз позволит судить о защищенности системы в целом. Данная вероятность рассчитывается по следующей формуле [4]:

$$P_{ост} = 1 - \prod_{i=1}^{6}\left[1 - o_{0,j}\left(1 - \prod_{k=0}^{5}(1 - H_{j,k})\right)\right], \quad (4)$$

где o_j - вероятность осуществления соответствующей угрозы.

В данном выражении матрица вероятностей $H = ||h_{jk}||$ с учетом полученных в результате вычислений значениями выглядит следующим образом:

$$H = \left|\left|h_{ji}\right|\right| = \begin{vmatrix} 0{,}27 & 0{,}28 & 0{,}20 & 0{,}12 & 0{,}19 & 0{,}26 \\ 0{,}25 & 0{,}27 & 0{,}06 & 0{,}14 & 0{,}28 & 0{,}23 \\ 0{,}05 & 0{,}05 & 0{,}19 & 0{,}02 & 0{,}05 & 0{,}05 \\ 0{,}03 & 0{,}03 & 0{,}08 & 0{,}27 & 0{,}03 & 0{,}03 \\ 0{,}01 & 0{,}01 & 0{,}09 & 0{,}27 & 0{,}01 & 0{,}01 \\ 0{,}21 & 0{,}23 & 0{,}19 & 0{,}09 & 0{,}27 & 0{,}11 \\ 0{,}18 & 0{,}13 & 0{,}19 & 0{,}10 & 0{,}17 & 0{,}31 \end{vmatrix}$$

где h_{jk} – вероятность реализации j-й угрозы от соответствия k-му требованию.

V. ВЫВОДЫ И ЗАКЛЮЧЕНИЕ

Исследования в сфере информационной безопасности приводят к выводу о том, что нельзя с уверенностью говорить о полной безопасности компьютерных систем. Каждая отдельно взятая угроза может привести к реализации определенного ущерба − морального или материального, а защита и противодействие обеспечивает снижение данного ущерба значительно или частично. Полученное в работе численной значение остаточной вероятности реализации всех возможных угроз для представленного примера $P_{ост}=0{,}46$, что позволяет сделать вывод о необходимости применения выделенных требований к защитным мерам.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введ. 2009-10-01. М.: Стандартинформ, 2014. 58 с.

2. Саати Т., Кернс К. Аналитическое планирование. М.: Радио и связь, 1991. 224 с.

3. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. 278 с.

4. Постников В. М., Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев // Наука и образование: научное издание МГТУ им. Н. Э. Баумана. 2015. № 6. С. 267–287. DOI: 10.7463/0615.0780334.

5. Постников В. М., Спиридонов С. Б. Выбор весовых коэффициентов локальных критериев на основе принципа арифметической прогрессии // Наука и образование: научное издание МГТУ им. Н. Э. Баумана. 2015. № 9. С. 237–249. DOI: 10.7463/0915.0802449.