МЕТОДИКА ОПРЕДЕЛЕНИЯ ЭКСПЕРТНЫХ ОЦЕНОК УЯЗВИМОСТЕЙ АКТИВОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ОТ ВЕРОЯТНЫХ УГРОЗ

Вашакидзе Г.А., магистрант
Паслен В.В., Ph.D. техн. наук, доцент
Щербов И.Л., ст. преподаватель
Якушина А.Е., ст. преподаватель
Донецкий национальный технический университет, Украина

Участники конференции,
Национального первенства по научной аналитике,
Открытого Европейско-Азиатского первенства по научной аналитике

Рассмотрен алгоритм количественной оценки уязвимости активов информационно-телекоммуникационной системы (ИТС). Предложена методика проведения экспертных оценок уязвимостей активов ИТС от вероятных угроз. Разработано программное обеспечение для расчета весовых коэффициентов a_k, c_k, i_k, s_k уязвимости активов ИТС.

Ключевые слова: *информационно-телекоммуникационная система, методы оценки риска, алгоритм принятия риска, экспертные оценки.*

The quantitative assessment algorithm of telecommunication system assets exposure is considered. The methods of expert estimation performance were proposed. Software for estimation of weight ratio a_k, c_k, i_k, s_k of telecommunication system assets exposure was developed.

Keywords: *telecommunication system, risk assessment methods, risk acceptance algorithm, expert estimation.*

Постановка задачи

Разработка эффективных моделей и методов управления безопасностью информационно-телекоммуникационных систем (ИТС) с целью противодействия кибернетической преступности в современном мире, является актуальной проблемой.

Для решения данной проблемы, в первую очередь, необходимо решить следующие задачи:

1. Разработать алгоритм принятия риска при создании системы защиты ИТС.
2. Предложить методику определения экспертных оценок уязвимостей активов ИТС от вероятных угроз.

Анализ состояния проблемы и решение задачи

Вопросы методики оценки риска и разработки алгоритма принятия риска экспертами при создании системы защиты ИТС детально рассмотрены в работах [1, 2].

Построение методики оценки риска строится на основе архитектуры защиты для систем, обеспечивающих связь между оконечными устройствами (рис.1), описанной в [3].

Рис. 1. Архитектура защиты систем, обеспечивающих связь между оконечными устройствами.

Учитывая архитектуру защиты систем, обеспечивающих связь между оконечными устройствами, предлагается количественную оценку уязвимости конкретного актива ИТС от одной угрозы определять по формуле:

$$T_k = \frac{(c_k+i_k+a_k+s_k)}{4} * z_k * p_k, \quad (1)$$

c_k, i_k, a_k, s_k – весовой коэффициент уязвимости актива (конфиденциальности, целостности, доступности и наблюдаемости соответственно) от k-ой угрозы, определяется экспертом;

z_k - вероятность защиты актива от k-ой угрозы определенным средством защиты;

p_k - частота появления k-ой угрозы относительно совокупности возможных угроз для актива.

На основании разработанных методики оценки риска и алгоритма принятия риска предлагается следующий метод определения экспертных оценок уязвимостей активов ИТС от вероятных угроз при определении весовых коэффициентов c_k, i_k, a_k, s_k.

На первом этапе для каждого из активов ИТС, группой экспертов дается оценка угрозы в соответствии с тремя параметрами:

- вероятность появления угрозы (p_k);
- вероятность преодоления средств защиты угрозой (z_k);
- вероятность использования уязвимостей ИТС (v_k).

Когда эти параметры равны нулю, то будем считать, что актив полностью защищен от данной угрозы, а в случае, когда параметры равны единице – угроза будет реализована и активу будет нанесен ущерб.

Итак, графически угрозу можно представить некоторой точкой в трехмерном пространстве, и чем дальше она от начала координат, тем выше ее значимость для данного актива, то есть общая оценка угрозы будет исчисляться, как длина отрезка линии, соединяющей начало координат и полученную точку. Для оценки угрозы будем использовать следующую формулу:

$$t_k = \sqrt{p_k^2 + z_k^2 + v_k^2} \quad (2)$$

Графически этот результат приведен на рисунке 2.

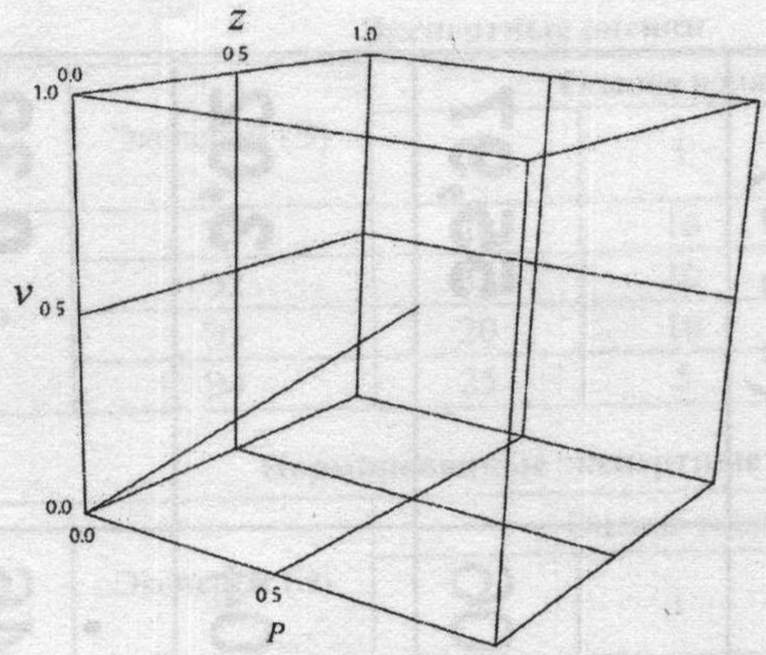

Рис. 2. Оценка k-й угрозы для m-го актива

График всех k-х угроз m-го актива приведен на рисунке 3.

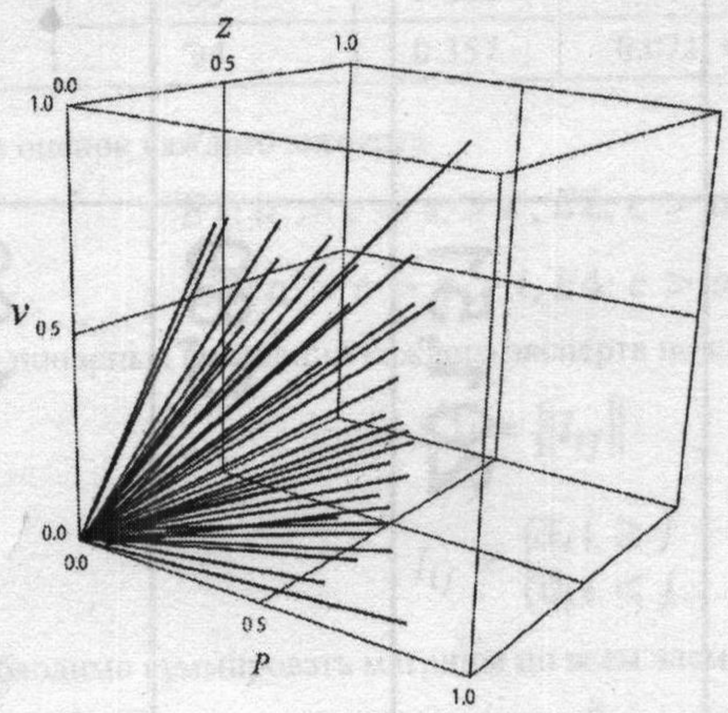

Рис. 3. Совокупность угроз для актива m

Для более наглядного представления совокупность угроз для актива m отразим как поверхность рисунок 4.

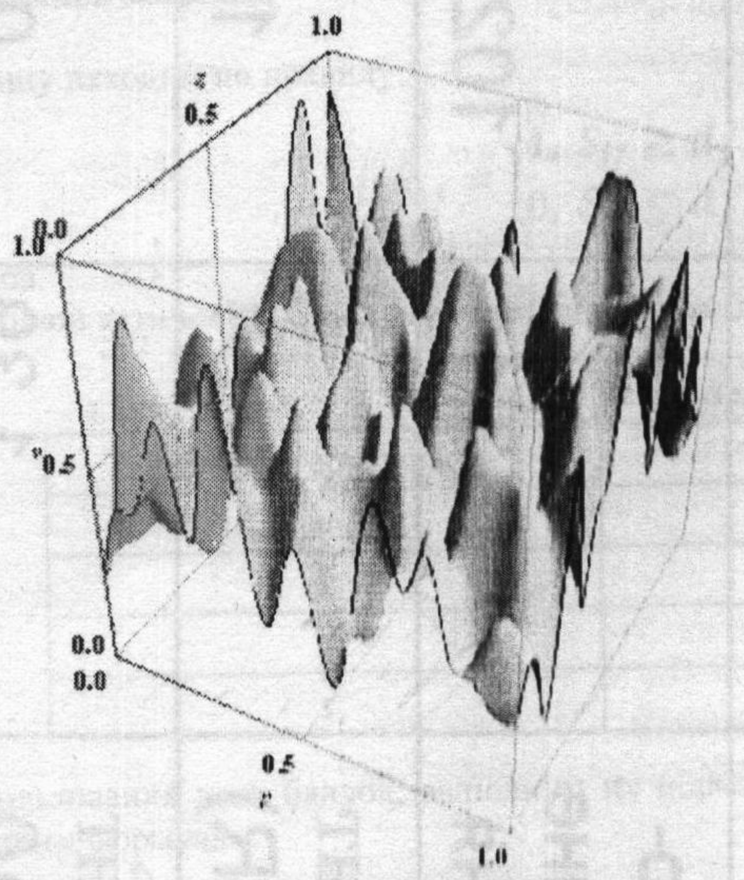

Рис. 4. Поверхность угроз для одного актива.

Проведя последовательную оценку уязвимости активов эксперты (Э) на основании знаний и полученных данных проставляют баллы вероятным угрозам по 100 бальной шкале, при этом разбивают оценку на различные свойства актива. В таблице 1, приведен пример экспертной оценки одной угрозы. Оценка в 100 баллов соответствует угрозе для которой t_k = 1,73.

Для дальнейшего анализа проводим стандартизацию (нормирование) экспертных оценок. Для примера рассмотрим угрозу «Анализ протоколов». Нормирование экспертных оценок для этой угрозы приведены в таблице 2.

Примем во внимание факт, что оценки экспертов согласованы. В этом случае для построения обобщенной экспертной оценки используем метод попарных сравнений.

Экспертные оценки Табл.1.

Угроза	Эксперты (Э)	Оценка влияния угрозы на свойства активов				
		c	i	a	s	Количество баллов
Анализ протоколов	Э1	20	10	30	20	80
	Э2	35	10	25	20	90
	Э3	20	10	25	15	70
	Э4	25	5	20	20	70

Нормированные экспертные оценки Табл.2.

Угроза	Эксперты (Э)	Оценка влияния угрозы на свойства активов				
		c	i	a	s	Количество баллов
Анализ протоколов	Э1	0.25	0.125	0.375	0.25	1
	Э2	0.39	0.1	0.282	0.228	1
	Э3	0.286	0.143	0.357	0.214	1
	Э4	0.357	0.071	0.286	0.286	1

Выполним ранжирование оценок каждого эксперта:

$$E1: a > c = s > i\,, E2: c > a > s > i,$$

$$E3: a > c > s > i, E4: c > a = s > i$$

Далее составим матрицы попарных сравнений каждого эксперта по следующим формулам:

$$E1 = \|I_{ij}\| \tag{3}$$

где

$$I_{ij} = \begin{cases} 1, i \geq j \\ 0, i < j \end{cases}$$

На следующем шаге необходимо суммировать матрицы по всем элементам, то есть формула имеет вид:

$$S_{ij} = \sum_{k=1}^{k} I_{ij_k} \tag{4}$$

где
S_{ij} – элементы суммированной матрицы;
k – номер эксперта.
Результирующую матрицу находим по правилу:

$$R_{ij} = \begin{cases} 1,\ S_{ij} \geq d/2 \\ 0,\ S_{ij} < d/2 \end{cases}$$

где
d – количество экспертов.
По каждой характеристикой активов ИТС получаем результат в баллах - табл.3.

Результат Табл.3

Характеристика	Баллы
c	4
i	1
a	4
s	2

Для дальнейшего использования этих баллов, выполним их нормирование в соответствии с найденной ранее общ оценки угрозы, по следующим формулам:

$$\begin{cases} c_н = \dfrac{c * t_k}{c + i + a + s} \\ i_н = \dfrac{i * t_k}{c + i + a + s} \\ a_н = \dfrac{a * t_k}{c + i + a + s} \\ s_н = \dfrac{s * t_k}{c + i + a + s} \end{cases}$$

То есть:

$$c_н + i_н + a_н + s_н = t_k$$

Полученные баллы необходимо внести в формулу 1, благодаря которой получим уязвимость актива от данной угрозы.

Для решения этой задачи было создано программное обеспечение (ПО) в среде Delphi 7. Интерфейс программного обеспечения представлен на рисунке 5.

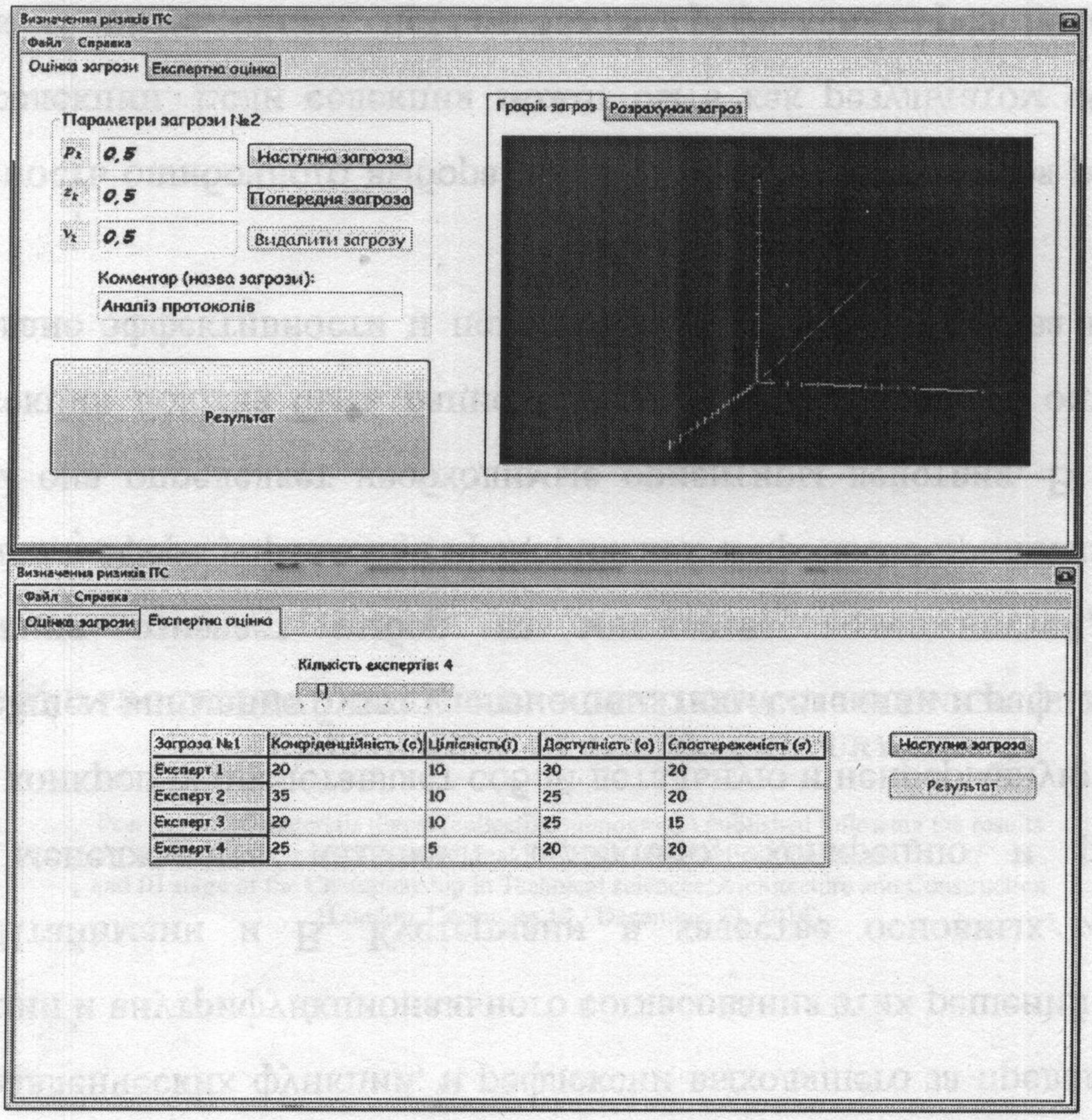

Рис. 5. Интерфейс программного обеспечения.

В данном ПО реализован рассмотренный алгоритм расчета весовых коэффициентов a_k, c_k, i_k, s_k с возможностью автоматического создания отчета полученных результатов.

Вывод.

1. Определены необходимые входные данные для расчета весовых коэффициентов характеристик активов ИТС.
2. Предложена методика определения экспертных оценок уязвимостей активов ИТС от вероятных угроз.
3. Разработано ПО для расчета весовых коэффициентов a_k, c_k, i_k, s_k с возможностью автоматического создания отчета полученных результатов.

Литература:

1. Вашакідзе Г А., Пасльон В В., Щербов І.Л., Якушина А.Є., Методика оценки рисков для активов информационно-телекоммуникационных // The development of technical sciences, building sciences and architecture in the context of the needs of society alteration. Peer-reviewed materials digest (collective monograph) published following the results of the LXXIII International Research and Practice Conference and III stage of the Championship in Technical sciences, Architecture and Construction. - Лондон, 2013. С- 42-45.

2. Щербов І.Л., Воропаєва В.Я., Вашакідзе Г.А, Алгоритм прийняття ризику з метою забезпечення безпеки ИТС // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 2(27). - Донецьк, ДонНТУ, 2014. С - 164-173.

3. Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами (ITU-T X.805 «Security architecture for systems providing end-to-end communications»).