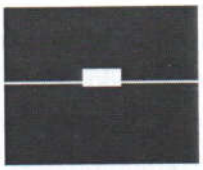

ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

I.V. Anikin

Fuzzy Assessment of Information Security Risk Factors

Keywords: information security risks, fuzzy logic, analytic hierarchy process

We suggested some methods for information security risk factors assessment. These methods are based on the expert judgments, analytic hierarchy process and fuzzy logic. Implementation of these methods enables quantitative evaluation of risk values under uncertainty, gaps and qualitative character of information about threats and vulnerabilities.

И.В. Аникин

НЕЧЕТКАЯ ОЦЕНКА ФАКТОРОВ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Проблема оценки и управления рисками информационной безопасности (ИБ) в настоящее время достаточно остро стоит для корпоративных информационных сетей (КИС). Решение вопросов выбора системы защиты информации (СЗИ) в КИС с позиций существующих рисков позволяет строить СЗИ, эффективные с точки зрения приемлемости затрат на их создание, с одной стороны, и размера ущерба от реализации угроз, с другой.

В настоящее время известно множество стандартов и руководств, регламентирующих вопросы оценки и управления рисками ИБ [1 – 4]. При этом среди существующих можно выделить методы качественной и количественной оценки рисков. Первая группа методов предполагает введение порядковых шкал для оценки факторов риска, а также матриц для оценки уровней риска ИБ. Основной задачей при этом является экспресс-оценка рисков, нацеленная на быстрое определение актуальных угроз. Вторая группа методов предполагает использование непрерывных числовых интервалов для оценки факторов риска ИБ. При этом одни из основных задач – детальный анализ процессов, происходящих в КИС, и формирование экономических оценок по защите информации на основе уровней рисков ИБ. К преимуществам второй группы методов следует отнести то, что формируемые оценки рисков более хорошо интерпретируются в рамках экономических моделей, на основании данных оценок проще реализовать математический аппарат формирования оптимальной совокупности защитных мер. В связи с этим практическое применение данных методов более актуально.

Рассматривая риск ИБ $R(V,T)$ как возможный ущерб, наносимый КИС, в результате реализации некоторой угрозы T через уязвимость V, можно выделить три основных фактора [1]:

$Poss(T)$ – количественная оценка возможности реализации угрозы T через заданную уязвимость V;

$Poss(V)$ – количественная оценка возможности использования уязвимости V;

$Impact(T)$ – количественная оценка ущерба от реализации угрозы T.

Оценка риска ИБ в данном случае будет выполняться согласно выражению

$$R(V,T) = Poss(V) \circ Poss(T) \circ Impact(T). \quad (1)$$

Основными сложностями количественной оценки данных факторов риска ИБ являются следующие особенности исходных данных:

- качественный характер большинства частных показателей факторов риска ИБ;
- неопределенность и нечеткость исходной информации;
- противоречивость оценок факторов риска, даваемых экспертами.

Это приводит к необходимости разработки технологии и методов количественной оценки факторов риска ИБ в условиях выше указанных сложностей. Их преодоление позволит экспертам формировать более объективные оценки рисков ИБ, чем классические экспертные оценки, как правило, используемые на практике.

Для учета качественного характера частных показателей факторов риска ИБ в разрабатываемой технологии применяют метод анализа иерархий (МАИ), а для учета неопределенности, нечеткости и противоречивости информации – методы теории нечетких множеств.

Дальнейшая структура статьи выглядит следующим образом. В разделе 1 предлагается технология оценки рисков ИБ, включающая в себя основные решаемые задачи и используемые методы. Данные методы описываются в последующих разделах статьи. В разделе 2 описан метод количественной оценки ущерба от реализации угроз в виде нечетких чисел. В разделе 3 представлен метод нечеткой оценки возможности реализации угроз. В разделе 4 предлагается метод нечеткой оценки возможности использования уязвимостей. В разделе 5 описан программная реализация ранее предложенных методов, а также решается задача оценки рисков ИБ, связанных с заражением вредоносным ПО узлов нескольких департаментов корпоративной сети университета.

Технология оценки рисков ИБ в КИС

Технология оценки рисков ИБ в КИС, включающая в себя основные решаемые задачи, формируемые модели, а также методы оценки факторов риска ИБ, входящие в состав математического и алгоритмического обеспечения, представлены на рис. 1.

Задача моделирования КИС для оценки и управления рисками ИБ решалась в [5]. При этом рассматривались различные виды активов КИС: информационные активы, АРМ, телекоммуникационное оборудование и ИТ-сервисы. Кроме того, строились:

– модель КИС, учитывающая взаимодействие активов и включающая в себя теоретико-множественные модели использования информационного обеспечения КИС, технического обеспечения КИС, использования ИТ-сервисов;

– модель угроз КИС в виде классического трехдольного графа;

– теоретико-множественную модель защитных мер КИС.

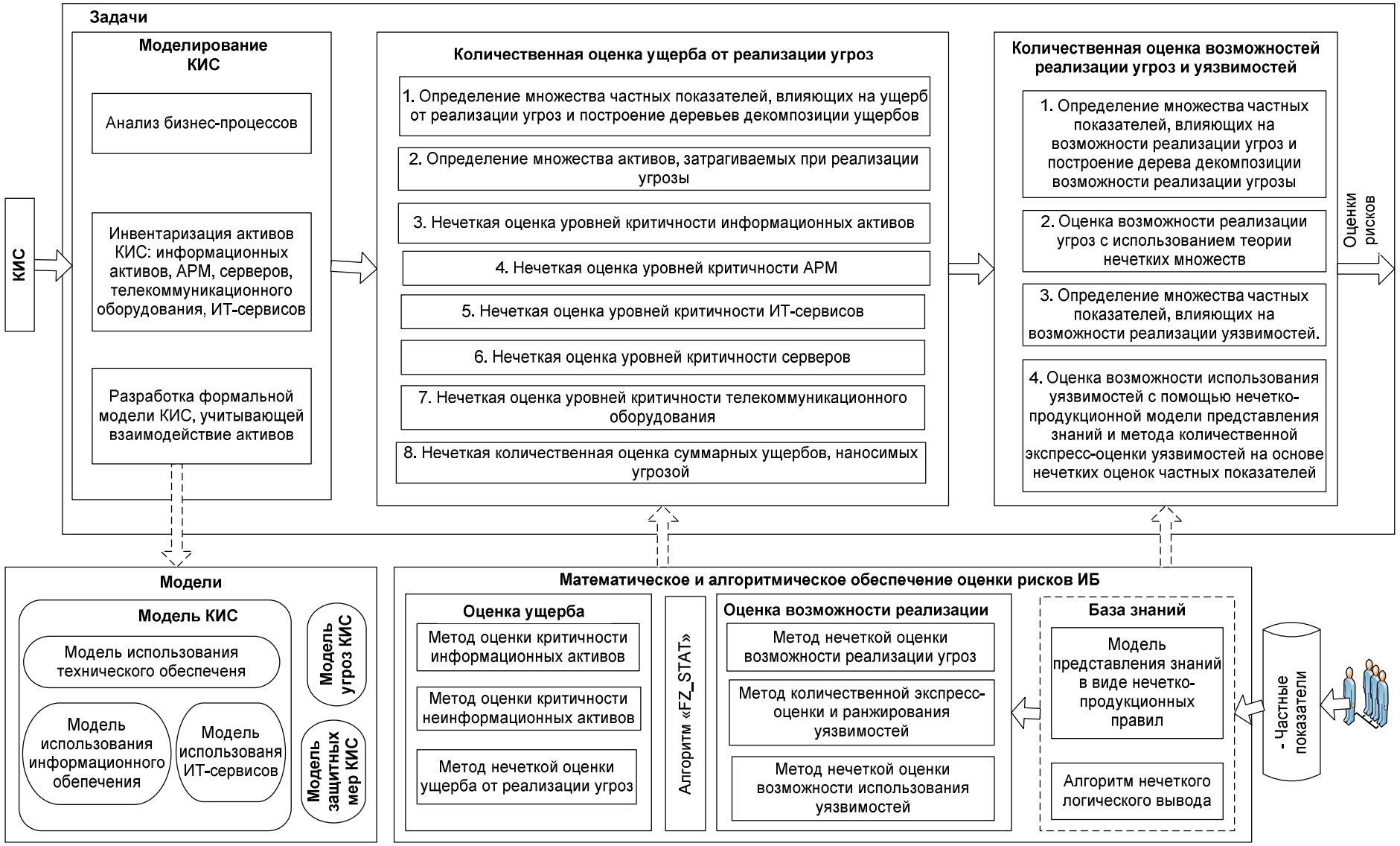

Рис. 1. Технология оценки рисков ИБ

Для количественной оценки ущерба от реализации угроз, оценки возможности реализации угроз и уязвимостей в условиях качественного характера большинства частных показателей факторов риска, неопределенности и нечеткости исходной информации, а также противоречивости оценок факторов риска, даваемых экспертами, должны быть разработаны соответствующие методы. Данные методы предлагаются в следующих разделах статьи.

Метод количественной оценки ущерба от реализации угроз

Количественная оценка ущерба от реализации угроз основывается на нечетких оценках критичности разнотипных активов. При этом выполняется следующая последовательность шагов:

нечеткая оценка критичности информационных активов;

нечеткая оценка критичности неинформационных активов;

нечеткая оценка ущерба от реализации угрозы на основе нечетких оценок критичности активов.

Для реализации данных шагов в условиях выше перечисленных сложностей были разработаны соответствующие методы.

Метод нечеткой оценки критичности информационных активов включает в себя три основных этапа.

Этап 1. Составление перечня информационных ресурсов КИС. Один из подходов к решению данной задачи может быть основан на анализе формализованных описаний бизнес-процессов КИС и выявлении входов-выходов их бизнес-функций, представляющих собой такие информационные ресурсы.

Этап 2. Определение множества частных показателей, влияющих на ущерб от реализации угроз. По результатам практического внедрения предлагаемого метода в различные КИС, экспертным путем было выделено множество из 29 различных частных показателей ущерба $\{\gamma_1, \dots, \gamma_{29}\}$. При этом для ряда КИС экспертным путем может быть отобрана только часть из них. Примерами частных показателей ущерба являются:

– ущерб авторитету организации;

– ущерб от публикации негативных материалов в прессе;

– ухудшение эмоционального климата в коллективе;

– снижение конкурентоспособности организации;

– ущерб, вызванный необходимостью проведения дополнительных исследований и др.

Большинство из данных частных показателей имеют качественный характер, в связи с чем, для их количественной оценки, в дальнейшем используется метод анализа иерархий (МАИ) [6]. Вид четырехуровневых иерархий (деревьев декомпозиции ущерба) представлен на рис. 2.

Этап 3. Количественная оценка критичности информационных активов. На данном этапе решаются следующие задачи:

– формируется экспертная группа, с привлечением которой будет выполняться анализ деревьев декомпозиции ущерба;

– формируются деревья декомпозиции ущерба для исследуемой группы информационных активов по конфиденциальности, целостности и доступности;

– выполняется оценка приоритетов информационных активов с использованием деревьев декомпозиции ущерба и метода анализа иерархий;

– формирование нечетких приоритетов информационных активов на основе полученных экспертных оценок. При этом используется алгоритм формирования функции принадлежности FZ_STAT, предложенный в работе [7];

– формирование нечетких оценок критичности информационных активов по конфиденциальности, целостности и доступности на основе полученных ранее нечетких приоритетов.

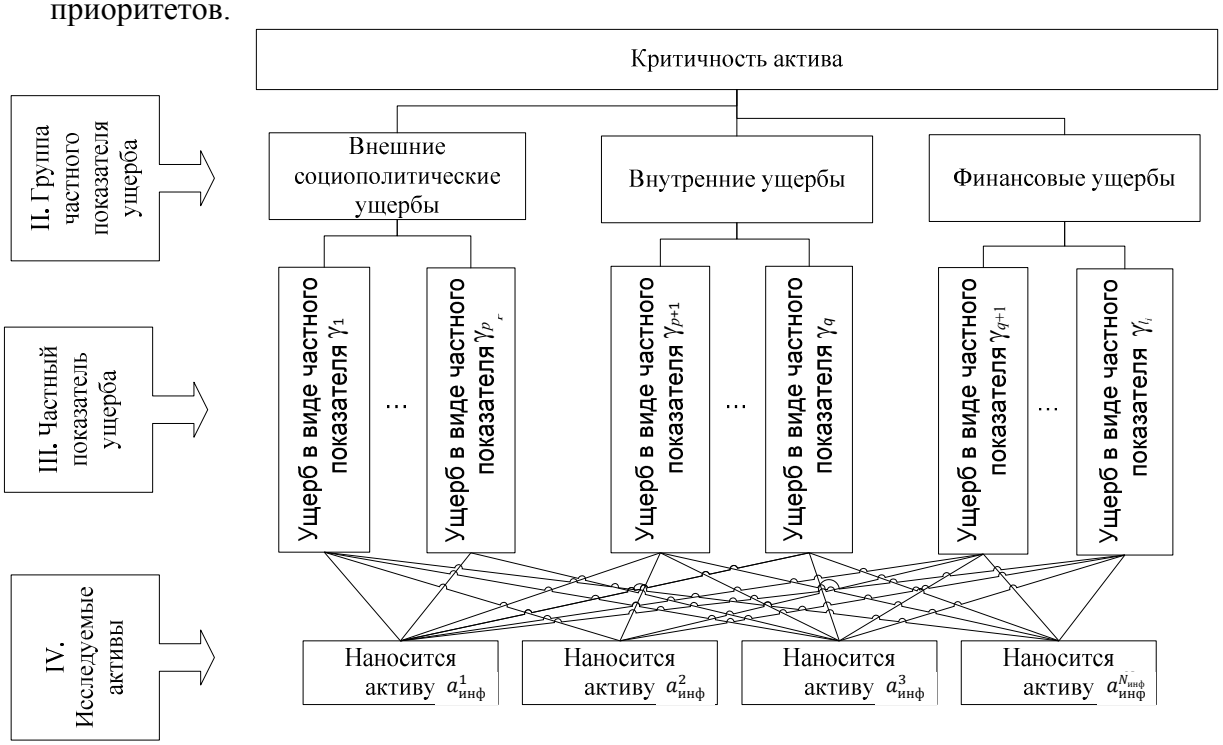

Рис. 2. Вид иерархии, используемой для оценки критичности актива

Метод нечеткой оценки критичности неинформационных активов предполагает формирование оценок для активов в следующей последовательности: Оценка уровней критичности АРМ → Оценка уровня критичности ИТ-сервисов → Оценка уровней критичности серверов → Оценка уровня критичности телекоммуникационного оборудования. Данные оценки осуществляются в нечетком виде на основании полученных оценок критичности информационных активов, с помощью разработанной модели КИС, с привлечением группы экспертов, МАИ и алгоритма FZ_STAT.

В вышеприведенной последовательности оценки критичности активов под *ИТ-сервисами* КИС понимаются процессы предоставления пользователям ресурсов информационных технологий для обеспечения выполнения ими своих бизнес функций. Множество ИТ-сервисов КИС также включает в себя и множество приложений (ПО), реализуемых в КИС.

Метод нечеткой оценки ущерба от реализации угрозы использует полученные ранее нечеткие оценки критичности активов, а также классическую модель угроз в виде трехдольного графа. При оценке ущерба экспертным путем определяются и используются показатели в виде нечетких чисел $\widetilde{pc}^{\,j}(T_i)\in[0,1]$, $\widetilde{pi}^{\,j}(T_i)\in[0,1]$, $\widetilde{pd}^{\,j}(T_i)\in[0,1]$ – проценты разрушения актива по конфиденциальности, целостности и доступности соответственно, при реализации угрозы T_i. Результатом работы метода является нечеткая оценка фактора риска $Impact(T_i)$.

Метод нечеткой оценки возможности реализации угроз

Метод нечеткой оценки возможности реализации угроз в условиях ранее обозначенных сложностей включает в себя два основных этапа.

Этап 1. Определение множества частных показателей, влияющих на возможности реализации угроз. Множество $\left\{\alpha_1\left(T_i\right),...,\alpha_{p_i}\left(T_i\right)\right\}, i=\overline{1,m}$, характеризующее различные частные показатели, влияющие на возможности реализации угроз T_i, формируется экспертным путем. Например, для угрозы МАСКАРАД было выделено десять частных показателей согласно подходу к оценке данной угрозы, представленному в стандарте CRAMM, а также в [1]. Перечень данных показателей включает в себя:

- количество раз за последние три года, когда сотрудники организации пытались получить НСД к хранящейся в информационной системе информации с использованием прав других пользователей;
- тенденция в статистике такого рода попыток несанкционированного проникновения в информационную систему;
- факт хранения в информационной системе информации (например, личных дел), которая может представлять интерес для сотрудников организации и побуждать к НСД к ней;
- факты нападения, угроз, шантажа, давления на сотрудников со стороны посторонних лиц;
- наличие среди персонала группы лиц или отдельных лиц с недостаточно высокими моральными качествами;
- наличие в системе информации, несанкционированное изменение которой может принести прямую выгоду сотрудникам;
- наличие в информационной системе пользователей, обладающих техническими возможностями совершить подобные действия;
- наличие других способов просмотра информации, позволяющих злоумышленнику добраться до нее более простыми методами, чем с использованием «маскарада»;
- наличие других способов несанкционированного изменения информации, позволяющих злоумышленнику достичь желаемого результата более простыми методами, чем с использованием «маскарада;
- количество раз за последние три года, когда сотрудники пытались получить НСД к информации, хранящейся в других подобных системах организации.

Многие из данных показателей также имеют качественный характер, для их дальнейшей количественной оценки используется МАИ.

Этап 2. Нечеткая оценка возможности реализации угроз на основе количественной оценки частных показателей. Данные оценки предлагается выполнять с помощью опросных листов с вопросами $Q_j\left(T_i\right)$ и выборочными вариантами ответов $Answer_{jk}\left(T_i\right), k=\overline{1,k_j\left(T_i\right)}$. За каждый ответ начисляется определенное количество баллов в виде нечеткого числа. Анализ общего нечеткого количества набранных баллов $\widetilde{P}_i=\sum_{j=1}^{p_i}\overline{point}_{js_j}\left(T_i\right)$, набираемых экспертом по результатам ответа на все вопросы $Q_j\left(T_i\right)$, $j=1,..,p_i$ теста, позволяет определить возможность реализации угрозы. Для формирования опросных листов и соответствующих нечетких значений баллов используются процедуры экспертного опроса, МАИ, алгоритм FZ_STAT. Вид иерархий, используемых для формирования нечетких баллов опросных листов, представлен на рис. 3.

По результатам ответов на вопросы опросного листа формируется показатель $Poss(T_i)$ – нечеткая количественная оценка возможности реализации угрозы T_i через заданную уязвимость V_i.

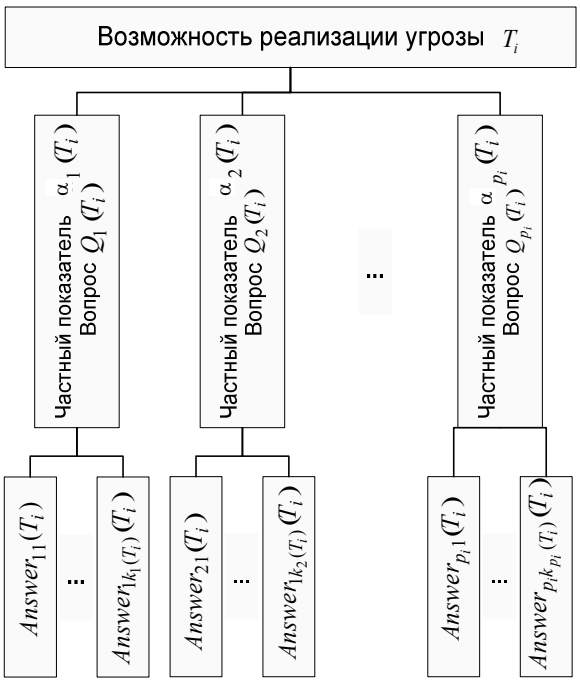

Рис 3. Вид иерархии, используемой для формирования нечетких баллов

Использование МАИ в предложенных методах оценки факторов риска позволяет учесть качественный характер частных показателей, в то время как использование нечетких оценок позволяет учесть нечеткий характер исходной информации и противоречивость экспертных оценок.

Метод нечеткой оценки возможности использования уязвимостей

Метод нечеткой оценки возможности использования уязвимостей базируется на метриках известного метода CVSSv3 и устраняет ряд его недостатков (внутренняя природа основана на использовании качественных шкал, необходимость определения значений всех базовых метрик, невозможность формирования нечетких оценок). Разработанный метод основан на использовании новой нечетко-продукционной модели представления знаний вида (2) и схемы нечеткого логического вывода [7], позволяющая эксперту формировать нечеткие оценки частных показателей, принимать решения в условиях отсутствия части информации об уязвимости, учитывающая важность частных показателей:

$$\begin{aligned}&\text{«ЕСЛИ } P_1^j \text{ есть } \tilde{A}_1^j \ (w_1^j) \text{ И } \ldots \text{ И } P_{s_j}^j \text{ есть } \tilde{A}_{s_j}^j \ (w_{s_j}^j)\\ &\text{ТО Степень уязвимости есть } \tilde{L}^j \text{» } [CF^j]\end{aligned} \tag{2}$$

где $P^j = \{P_i^j\} \subset P, i = \overline{1, r_j}$ – множество частных показателей уязвимостей, заданных в виде лингвистических переменных, на которые накладываются ограничения в условиях правила R^j; $A^j = \langle \tilde{A}_1^j, \ldots, A_{r_j}^j \rangle$ – значения частных показателей уязвимостей (значения лингвистических переменных), определяющих нечеткие ограничения на параметры

множества P^j; $w^j = \left\langle w_1^j, w_{r_j}^j \right\rangle$ – веса нечетких ограничений $\widetilde{A}_i^j$ на параметры P_i^j в антецеденте правила R^j; $CF^j \in [0;1]$ – степень уверенности эксперта в универсальности правила; $\widetilde{L}^j$ – значение лингвистической переменной «Степень уязвимости» при заданных значениях частных показателей в правиле R_j.

Функции принадлежности значений лингвистических переменных $\widetilde{A}_1^j$ формировались на основе метрик CVSS.

По результатам нечеткого логического вывода на базе знаний с правилами вида (2) формируется нечеткая оценка $Poss(V_j)$ возможности использования уязвимости V_j.

Практическое применение предложенного метода позволяет не только преодолеть недостатки CVSSv3, но и учесть при оценке уязвимостей неопределенность и нечеткость исходной информации.

На основании полученных нечетких оценок факторов риска $Poss(T_i)$, $Poss(V_j)$, $Impact(T_i)$ с помощью выражения (1) формируется нечеткая оценка риска ИБ, связанного с угрозой T_i, реализуемой через уязвимость V_j.

Программная реализация методов и результаты экспериментов

Для реализации выше представленных методов был разработан комплекс программ.

1. Программный продукт оценки критичности активов КИС на платформе Microsoft .NET 4, языке C#, реализующий следующие функции:

– оценку критичности информационных активов (рис. 4), при этом используется программная реализация метода анализа иерархий и алгоритма FZ_STAT;
– моделирование КИС для оценки их критичности (рис. 5);
– управление активами КИС и видами ущербов;
– оценку критичности неинформационных активов.

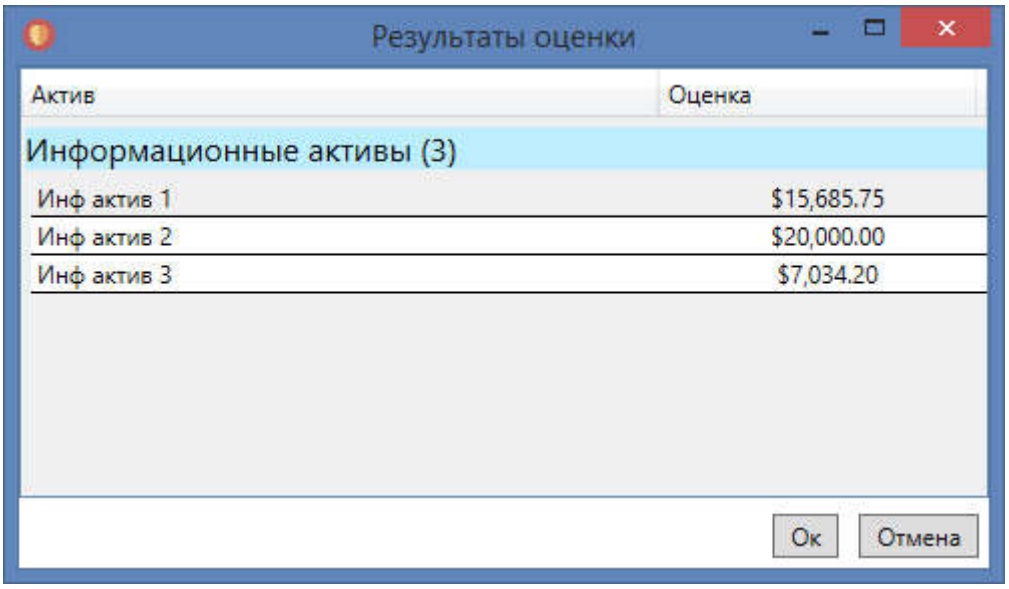

Рис. 4. Диалоговое окно с результатами оценки активов

2. Программный продукт нечеткой оценки возможности реализации угроз на языке C# в среде VisualStudio, реализующий следующие функции:

– формирование опросных листов для оценки возможности реализации угроз, использующее метод анализа иерархий и алгоритм FZ_STAT;

– оценка возможности реализации угроз с помощью сформированных опросных листов.

3. Программный продукт количественной оценки возможности использования уязвимостей в среде Delphi, реализующий следующие функции:

– формирование базы знаний для оценки уязвимостей (рис. 5);

– использование базы знаний для оценки уязвимостей.

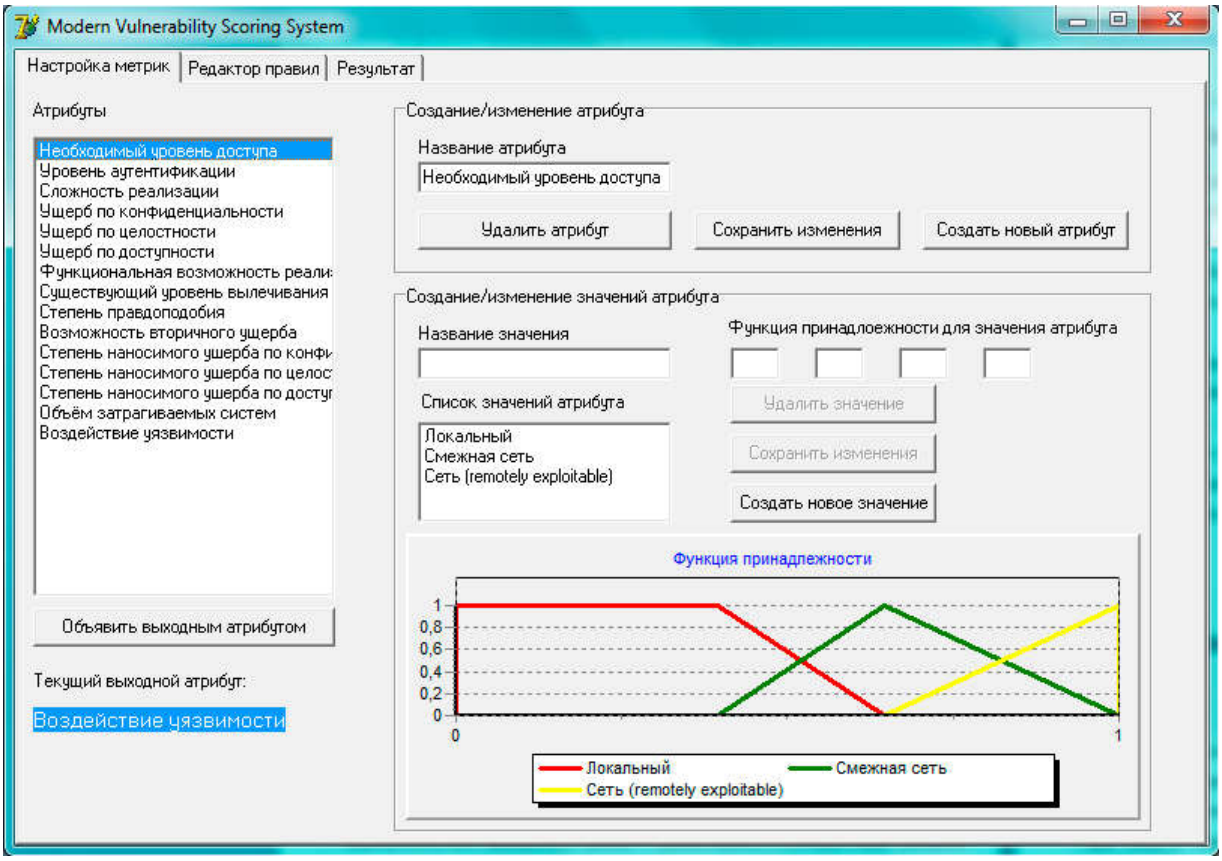

Рис. 5. Диалоговое окно формирования базы знаний для оценки уязвимостей

В качестве простого примера была рассмотрена задача оценки рисков ИБ, связанных с заражением вредоносным ПО узлов нескольких департаментов корпоративной сети университета. В качестве способа оценки рисков использовался двухфакторный подход (без учета информации о возможных уязвимостях). Результаты количественной оценки рисков ИБ представлены в табл.

Таблица. Результаты оценки рисков ИБ

Угроза	Ущерб	Возможность реализации угрозы	Риск
Заражение вирусами узла в департаменте «Отдел кадров»	$\overline{3055}$	$\overline{0,61}$	$\overline{1864}$
Заражение вирусами узла в департаменте «Бухгалтерия»	$\overline{16300}$	$\overline{0,61}$	$\overline{9943}$
Заражение вирусами узла в департаменте «Приемная комиссия»	$\overline{7499}$	$\overline{0,61}$	$\overline{4391}$

Заключение

Предлагаемая технология и методы позволяют осуществить количественную оценку факторов риска ИБ, а также самих рисков ИБ в КИС в условиях качественного характера большинства частных показателей факторов риска, неопределенности и нечеткости исходной информации, а также противоречивости оценок факторов риска, даваемых экспертами. Использование полученных количественных оценок риска ИБ позволит решать различные оптимизационные задачи выбора наилучшей совокупности защитных мер применительно к конкретной КИС.

В настоящее время ведется работа по применению выше предложенных методов к решению задачи оценки и дальнейшему управлению рисками ИБ в крупных КИС.

СПИСОК ЛИТЕРАТУРЫ:

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: АйТи, 2004.
2. NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012.URL: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (дата обращения: 10.02.2015).
3. Karabacak B. and Sogukpinar I., ISRAM: information security risk analysis method. Computers&Security. 2005. 24 (2), pp. 147–159.
4. Alberts C., Dorofee A. Managing information security risks. The OCTAVESM approach. Addison Wesley, 2002. P. 512.
5. Аникин И.В. Метод нечеткой оценки критичности активов корпоративной информационной сети // Информационные системы и технологии. 2015. № 4 (90). С. 111–120
6. Аникин И.В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности // Вестник Казанского государственного технического университета им. А.Н. Туполева. 2006. № 3. С. 11–18.
7. Аникин И.В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике // Информация и безопасность. 2014. Т.17. № 3. С. 468–471.

REFERENCES:

1. Petrenko S.A., Simonov S.V. Information risks management. Economy of Information Security. M.: IT, 2004. 392 P.
2. NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012. URL: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (дата обращения: 10.02.2015).
3. Karabacak B. and Sogukpinar I., ISRAM: information security risk analysis method. Computers&Security. 2005. 24 (2), pp. 147-159.
4. Alberts C., Dorofee A. Managing information security risks. The OCTAVESM approach. Addison Wesley, 2002. P. 512.
5. Anikin I.V. Assets fuzzy evaluation method for computer networks // Information systems and technologies. 2015. № 4 (90). Pp. 111-120
6. Anikin I.V. AHP application for information security risks analysis and assessment // Vestnik of Kazan Technical University. 2006. № 3. Pp. 11-18.
7. Anikin I.V. Fuzzy risk assessment method for vulnerabilities // Information and Security. 2014. T.17. № 3. Pp. 468–471.