Жекамбаева М.Н., Ахметова С.Т., Алимсеитова Ж.К. Система оценивания рисков на базе метода SecondM. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XV Междунар. научно-техн. конф. – Пенза: ПДЗ, 2015. – С. 111-116.

УДК 004. 056

СИСТЕМА ОЦЕНИВАНИЯ РИСКОВ НА БАЗЕ МЕТОДА SecondM

М.Н. Жекамбаева, С.Т. Ахметова, Ж.К. Алимсеитова

SYSTEM OF ESTIMATION OF RISKS ON THE BASIS OF THE SecondM METHOD

M.N. Zhekambayeva, S.T. Akhmetov, Zh.K. Alimseitova

Аннотация. Параллельно со стремительным развитием и внедрением IT-технологий во все сферы деятельности человечества растет и число угроз, связанных с нарушением конфиденциальности, целостности и доступности информационных ресурсов (ИР), которые обрабатываются с помощью этих технологий. Поэтому безопасность таких ресурсов становится приоритетной задачей как для предпринимательской деятельности, так и для государства в целом. Решать такую задачу целесообразно с помощью системы управления информационной безопасностью (ИБ). Для построения системы необходимо проводить анализ и оценивание рисков ИБ, которые часто характеризуются высокой неопределенностью.

Ключевые слова: риск, анализ риска, оценивание риска, система анализа и оценки риска, базовые характеристики риска, методология синтеза.

Abstract. In parallel with prompt development and introduction of IT technologies in all fields of activity of mankind, also the number of the threats connected with violation of confidentiality, integrity and availability of the information resources (IR) which are processed by means of these technologies grows. The refore safety of such resources becomes a priority task, both for business activity, and for the state in general. Today expediently to solve such problem by means of a control system of the information security (IS). For creation of such system it is necessary to carry out the analysis and estimations of risks of IB which are often characterized by high uncertainty.

Keywords: risk, analysis of risk, estimation of risk, system of the analysis and assessment of risk, basic characteristics of risk, synthesis methodology.

Известен метод анализа и оценивания рисков ИБ SecondM, который позволяет использовать широкий спектр параметров, что повышает гибкость и расширяет возможности проектируемых средств оценивания, функционирующих в нечетко определенной слабоформализованной среде.

На основании метода разработана Second-CAOP система, позволяющая проводить оценку при различных исходных величинах, учитывающих не только возможности эксперта четко детерминировать оцениваемые параметры, но и его неуверенность в своих суждениях.

Далее предлагается Second-CAOP система, которая в отличие от First-CAOP системы дает возможность оценивать уровень риска (УР) при условии, что эксперт не всегда может однозначно определить предпочтения в отношении базо-

вых характеристик. Структурная схема такой системы (рис. 1) содержит подсистемы обработки базовых параметров (ПСОБП), подсистему формирования нечетких данных (ПСФНД), а также модули формирования структурированного параметра риска (МФСПР) и генерации отчетов (МГО).

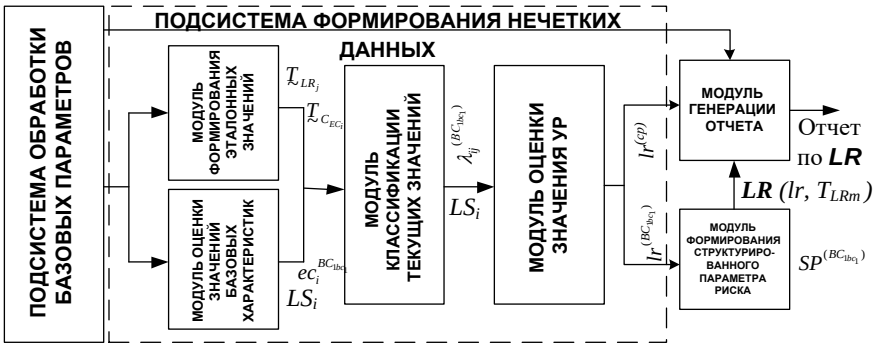

Рис.1. Структурная схема Second-CAOP системы

Функции ПСОБП обладают полным изоморфизмом с аналогичной подсистемой в First-CAOP системе, а ПСФНД формирует нечеткие данные, которые дают возможность при исходных величинах учитывать неуверенность эксперта в процессе оценивания УР. Подсистема ПСФНД содержит модули формирования эталонных значений (МФЭЗ), оценки значений базовых характеристик (МБХ), классификации текущих значений (МКТЗ) и оценки значения УР (МУР). Модуль МФЭЗ предназначен для построения функций принадлежности (ФП) эталонных нечетких чисел (НЧ) на основании принятого экспертами решения о количестве термов лингвистической переменной (ЛП) (согласно этапам 6 и 7 методологии). Здесь экспертами на основе выражения

$$\mu_j(lr)=\begin{cases} L\left(\dfrac{b_{1j}-lr}{b_{1j}-a_j}\right), & lr\in[a_j,b_{1j}];\\ 1, & lr\in[b_{1j},b_{2j}];\\ R\left(\dfrac{lr-b_{2j}}{c_j-b_{2j}}\right), & lr\in[b_{2j},c_j], \end{cases}$$

где $a_j < b_{1j} \le b_{2j} < c_j$ при $j=\overline{1,m}$, $\{a_1, c_m\}=\{\varnothing\}$, а $L(dr)$, $R(dr)$ – функции (невозрастающие на множестве неположительных чисел), которые удовлетворяют свойствам: $L(-dr) = L(dr)$, $R(-dr) = R(dr)$, $L(0) = R(0) = 1$) и собственных приоритетов, определяются эталонные НЧ для ЛП ***LR*** и C_{EC_i} относительно интервалов значений, количество которых зависит от числа используемых термов, например, если их m, то для ***LR*** количество интервалов будет $G = 2m-1$, с общим видом $[b_{11}; b_{21}[$, $[b_{21};b_{12}[$, $[b_{12}; b_{22}[$, …, $[b_{2m-1}; b_{1m}[$, $[b_{1m}; b_{2m}]$ ($j=\overline{1,m}$) и ФП $\mu_j(lr)$, а для C_{EC_i} – $[b_{11}; b_{21}[$, $[b_{21}; b_{12}[$, $[b_{12}; b_{22}[$, …, $[b_{2m-1}; b_{1m}[$, $[b_{1m}; b_{2m}]$ ($j=\overline{1,m}$) и ФП $\mu_j(c_{EC_i})$. В результате работы модуля формируются ЛП ***LR***, C_{EC_i} и их интервалы, а также НЧ и ФП. Модуль МБХ имеет то же функциональное предназначение, что и аналогичный модуль в First-CAOP системе, а МКТЗ позволяет получать как нечеткие значения

параметров с помощью МФЭЗ на основе эталонных значений ЛП C_{EC_i}, сформированных экспертами, осуществляется определение принадлежности $ec_i^{BC_{1bc_1}}$ заданному НЧ, по которому вычисляется значение λ с помощью выражения

$$\lambda_{i1}^{(BC_{1bc_1})}=\begin{cases}1\ при\ ec_i^{BC_{1bc_1}}\in[bi_{11},bi_{12}[;\\ 0\ при\ ec_i^{BC_{1bc_1}}\notin[bi_{11},ci_1[;\\ \mu_1(ec_i^{BC_{1bc_1}})\ при\ ec_i^{BC_{1bc_1}}\in[bi_{12},ci_1[,\end{cases}\qquad \lambda_{ij}^{(BC_{1bc_1})}=\begin{cases}\mu_j(ec_i^{BC_{1bc_1}})\ при\ ec_i^{BC_{1bc_1}}\in[ai_j,bi_{1j}[;\\ 1\ при\ ec_i^{BC_{1bc_1}}\in[bi_{1j},bi_{2j}[;\\ \mu_j(ec_i^{BC_{1bc_1}})\ при\ ec_i^{BC_{1bc_1}}\in[bi_{2j},ci_j[;\\ 0\ при\ ec_i^{BC_{1bc_1}}\notin[ai_j,ci_j[,\end{cases}$$

$$\lambda_{im}^{(BC_{1bc_1})}=\begin{cases}\mu_m(ec_i^{BC_{1bc_1}})\ при\ ec_i^{BC_{1bc_1}}\in[ai_m,bi_{1m}[;\\ 1\ при\ ec_i^{BC_{1bc_1}}\in[bi_{1m},bi_{2m}[;\\ 0\ при\ ec_i^{BC_{1bc_1}}\notin[ai_m,bi_{2m}[,\end{cases}\qquad (j=\overline{2,m-1}).$$

так и учитывать четкие (без неопределенностей) значения.

Аналогично First-CAOP системе здесь также определяется LS_i. В результате работы модуля получаем значения $\lambda_{ij}^{(BC_{1bc_1})}$ для каждой идентифицированной BC_{1bc_1} в МИБХ и LS_i. Модуль МУР имеет изоморфные функции относительно МУР в First-CAOP системе. Данные из него поступают в МФСПР, где на основании вычисленных значений $lr^{(BC_{1bc_1})}$,$lr^{(cp)}$ и построенных эталонов с помощью выражения

$$SP^{(BC_{1bc_1})}=\begin{cases}(lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j})\ при\ \mu_j(lr)=1;\\ (lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j}(\mu_j(lr));\underset{\sim}{T}_{LR_{j+1}}(\mu_{j+1}(lr)))\ при\ \mu_j(lr),\mu_{j+1}(lr)\neq 1,\end{cases}$$

(где $(lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j})$ словесно интерпретируется как – уровень риска $\underset{\sim}{T}_{LR_j}$ с числовым эквивалентом $lr^{(BC_{1bc_1})}$, а $(lr^{(BC_{1bc_1})};\underset{\sim}{T}_{LR_j}(\mu_j(lr));\underset{\sim}{T}_{LR_{j+1}}(\mu_{j+1}(lr)))$, как – уровень риска с числовым эквивалентом $lr^{(BC_{1bc_1})}$ граничит между $\underset{\sim}{T}_{LR_j}$ и $\underset{\sim}{T}_{LR_{j+1}}$ с уверенностью эксперта по границе $\underset{\sim}{T}_{LR_j}$ — $\mu_j(lr)$ и $\underset{\sim}{T}_{LR_{j+1}}$ — $\mu_{j+1}(lr)$), определяется структурированный параметр $SP^{(BC_{1bc_1})}$, который позволяет получить как числовое значение УР, так и его лингвистическую интерпретацию, учитывающую неуверенность эксперта при формировании текущих значений базовых компонент с дальнейшей классификацией посредством параметра $\lambda_{ij}^{(BC_{1bc_1})}$. Модуль МГО также как аналогичный модуль в First-CAOP системе предназначен для генерации результирующих отчетов.

Примеры сформированного отчета МГО Second-CAOP системы представлен на рис. 2.

Отчет
по расчету степени риска для активов организации
от 22.05.2015
для проекта
fuz

Сумарно по активам

Список активов	Степень риска
сетевые серверы БД	РН (0,3), РС (0,7) - 37
портативные, не имеющие постоянного расположения	РН (0,25), РС (0,75) - 37,5
принтер	РВ (0,7), ПР (0,3) - 73

Детальная информация по активам

сетевые серверы БД

Угрозы	Степень риска
Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	35
Злоупотребление средствами аудита	39

портативные, не имеющие постоянного расположения

Угрозы	Степень риска

Рис. 2. Пример сгенерированного отчета

На основе разработанной структуры Second-CAOP системы созданы программные средства, которые в отличие от известных используют в качестве входных данных различные наборы базовых характеристик, что повышает гибкость, удобство использования, интеграцию возможностей и расширяет возможность проектируемых средств анализа и оценивания рисков ИБ, функционирующих как в детерминированной, так и в нечеткой, слабоформализованной среде.

Жекамбаева Майгуль Несипалдиевна
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Казахстан
E-mail: maia.kz@mail.ru

Zhekambayeva M.N.
Kazakh national research technical university name K.I. Satpayev, Almaty, Kazakhstan

Ахметова Санзира Тынымбаевна
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Казахстан

Akhmetova S.T.
Kazakh national research technical university name K.I. Satpayev, Almaty, Kazakhstan

Алимсеитова Жулдыз Кенесхановна
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Казахстан

Alimseitova Zh.K.
Kazakh national research technical university name K.I. Satpayev, Almaty, Kazakhstan