Ахметов Б.С., Корченко А.Г., Казмирчук С.В., Жекамбаева М.Н. Система оценивания рисков на базе метода FirstM. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XV Междунар. научно-техн. конф. – Пенза: ПДЗ, 2015. – С. 105-110.

УДК 004. 056

СИСТЕМА ОЦЕНИВАНИЯ РИСКОВ НА БАЗЕ МЕТОДА FirstM

Б.С. Ахметов, А.Г. Корченко, С.В. Казмирчук, М.Н. Жекамбаева

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

B. S. Akhmetov, A.G. Korchenko, S. V. Kazmirchuk, M. N. Zhekambayeva

Аннотация. Исследование показало, что в основном для анализа и оценивания рисков используются статистические данные об инцидентах и угрозах информационной безопасности (ИБ). Во многих странах на государственном уровне подобная статистика не ведется, что ограничивает возможности существующих средств для национального использования. Исследуемый инструментарий устанавливает эксперту определенные ограничения (на используемый набор параметров) и не дает ему возможности применения для оценивания более широкого спектра величин. Известен метод анализа и оценивания рисков ИБ FirstM, который позволяет использовать широкий спектр параметров, что повышает гибкость и расширяет возможности проектируемых средств оценивания, функционирующих в детерминированной среде. На основании предложенного метода разработана First-CAOP система, позволяющая проводить оценку при различных исходных величинах, учитывающих возможности эксперта четко детерминировать оцениваемые параметры.

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

Abstract. Research showed that generally for the analysis and estimation of risks statistical data on incidents and threats of the information security (IS) are used. In many countries at the state level the similar statistics isn't conducted that limits possibilities of the existing means for national use. Also it should be noted that the studied tools set to the expert certain restrictions (on the used set of parameters) and don't give it the chance of application for estimation of wider range of sizes. The method of the analysis and estimation of risks of IB FirstM which allows to use a wide range of parameters that increases flexibility is known and expands possibilities of the projected means of estimation functioning in the determined environment. On the basis of the offered method First-SAOR the system allowing to carry out an assessment at various initial sizes considering possibilities of the expert accurately to determine the estimated parameters.

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

Структурная схема First-CAOP системы содержит (рис. 1): подсистемы обработки базовых параметров (ПСОБП) и формирования данных (ПСФД), модули лингвистического распознавания (МЛР), генерации отчетов (МГО) и служит для анализа и оценивания рисков при условии, когда эксперт имеет четкие (бинарные) предпочтения относительно значений базовых характеристик. Согласно существующей методологии (этапы 2–4) строится ПСОБП, которая служит для подготовки данных, основанных на суждениях экспертов для ПСФД и состоит из: базы данных (БД) ИР (БДИР), БД угроз (БДУ) и БД проектов пользователей (БДПП); модуля инициализации базовых характеристик (МИБХ); модуля формирования ключевых данных (МФКД). База данных БДИР содержит соответствующие списки множества $IR \in \{IR_h\}(h = \overline{1,r})$(где h – указатель (номер) текущего идентификатора информационного ресурса (ИР), а r – количество ИР), БДУ

включает множество $\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i}\ (bc_1 = \overline{1,n})$ (где bc_1 – указатель (номер) текущего идентификатора угрозы, а n – количество угроз) и $\mathrm{BC}_2 = \bigcup_{i=1}^{bc_2} BC_{2i}\ (bc_2 = \overline{1,7})$ (где bc_2 – указатель (номер) текущего идентификатора события), а БДПП содержит списки множества $UP \in \{UP_p\}(p = \overline{1,c})$ (где p – указатель (номер) текущего идентификатора проектов пользователей (ПП), а c – их количество), которая предназначена для хранения полученных результатов от предыдущих оценок в отдельных таблицах, позволяющих использовать ПП при очередной оценке, и которые могут, например, иметь вид и структуру, представленную на рис. 2. При формировании БДИР (активов), например, можно воспользоваться классификацией ресурсов из описания метода CRAMM для профиля Commercial, а при формировании БДУ – классификацией из ISO/IEC 27002:2005. Модуль МИБХ предназначен для выбора из БДИР и БДУ соответственно характерных для объекта оценки IR и BC_{1bc_1}, BC_{2bc_2}. Модуль МФКД реализуется согласно этапам 5–7 методологии и предназначен для формирования лингвистических переменных (ЛП): ЛП «УРОВЕНЬ РИСКА» (***LR***) и «УРОВЕНЬ EC_i» (C_{EC_i}), которые определяются соответственно кортежами $<LR, T_{LR}, X_{LR}>$, $<C_{EC_i}, T_{C_{EC_i}}, X_{EC_i}>$, где базовые терм-множества задаются m термами $\underset{\sim}{T}_{LR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{LR_j}$ и $\underset{\sim}{T}_{C_{EC_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{C_{EC_i}j}$ ($j = \overline{1,m}$), также здесь осуществляется выбор количества базовых характеристик из их полного множества $\boldsymbol{EC}_{Fh} \in \{EC_i\} = \{BC_3, BC_4, BC_5, BC_6\}$ ($i = \overline{1,g}$, i – идентификатор оценочного компонента, аg – количество этих компонент), где Fh – шестнадцатеричный код, бинарное значение которого отражает порядковые номера базовых характеристик в множестве. В результате преобразований на выход модуля поступают $\{EC_i\}$, ЛП ***LR***, C_{EC_i} и их терм-множества, а также соответствующие интервалы для последующей классификации и лингвистического распознавания.

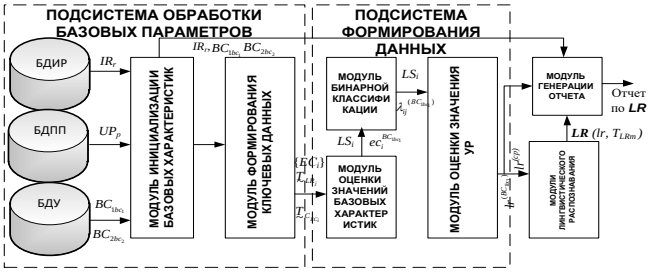

Рис. 1. Структурная схема First-CAOP системы

Далее в ПСФД формируются данные для последующей оценки уровня риска (УР). Она содержит: модуль оценки значений базовых характеристик (МБХ), который согласно этапам 9 и 8 методологии, предназначен соответственно для определения экспертами текущих значений, $ec_i^{BC_{1bc_1}}$,т.е. $\{ec_i^{BC_{1bc_1}}\} = \{ec_{BC_3}^{BC_{1bc_1}}, ec_{BC_4}^{BC_{1bc_1}}, ec_{BC_5}^{BC_{1bc_1}}, ec_{BC_6}^{BC_{1bc_1}}\}$, где $\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i}\ (bc_1 = \overline{1,5})$ и определения их уровня значимости $LS_i i = \overline{1,g}$; модуль бинарной классификации (МБК), в котором согласно этапу 10 методологии осуществляется формирование значений $\lambda_{ij}^{(BC_{1bc_1})}$ по выражениям:

$$\lambda_{ij}^{(BC_{1bc_1})} = \begin{cases} 1, \text{при } ec_i^{BC_{1bc_1}} \in [\, c_{EC_i(j-1)}; c_{EC_i j}[, \\ 0, \text{при } ec_i^{BC_{1bc_1}} \notin [\, c_{EC_i(j-1)}; c_{EC_i j}[. \end{cases}$$

С помощью полученных из МБХ результатов $ec_i^{BC_{1bc_1}}$; модуль оценки значения УР (МУР), осуществляющий для каждой идентифицированной $BC_{1bc_1}\ (bc_1 = \overline{1,n})$ оценку УР $lr^{(BC_{1bc_1})}$ по формуле

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m}\left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right),$$

где lr_j=90-20(j-1) $\lambda_{ij}^{(BC_{1bc_1})}$ определяется по формуле (4) для каждой BC_{1bc_1} $(bc_1 = \overline{1,n})$, а LS_i $(i = \overline{1,g})$ – по формуле (2) или (3) $(j = \overline{1,m})$, и его среднее значение $lr^{(cp)}$ по ИР $lr^{(cp)} = (\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})}) / m$. С учетом результатов классификации вычислены базовые характеристики $\lambda_{ij}^{(BC_{1bc_1})}$ и их уровень значимости LS_i.

Модуль МЛР предназначен для лингвистической интерпретации значений $lr^{(BC_{1bc_1})}$ и $lr^{(cp)}$ с помощью сформированной ЛП ***LR*** на основе ее терм-множеств и интервалов по выражению

$$\underset{\sim}{T}_{LR} = \begin{cases} HP, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_{\min}; lr_1[\\ PH, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_2; lr_3[\\ PC, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_4; lr_5[\\ PB, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_6; lr_7[\\ OP, \text{ при } lr^{(BC_{1bc_1})} \in [lr_8; lr_{\max}] \end{cases}.$$

Модуль МГО позволяет по результатам работы двух подсистем сгенерировать отчеты оценки УР, в которые заносятся все идентифицированные IR_h, BC_{1bc_1}, BC_{2bc_2}, результаты оценки $lr^{(BC_{1bc_1})}$, $lr^{(cp)}$ и их лингвистический эквивалент.

Name	Type	Length	Decimals	Allow Null
id	int	11	0	☐
resource	varchar	200	0	☐
threat	varchar	200	0	☐
probability	int	5	0	☐
frequency	decimal	4	2	☐
loss	decimal	4	2	☐
danger	int	5	0	☐
dr	decimal	4	2	☑

Рис. 2. Пример таблицы ПП

Система функционирует следующим образом. В МИБХ из БДИР и БДУ поступают исходные данные (ИД), которые выбираются экспертом. Имеется возможность применения готовых ПП из БДПП. Здесь используется три БД под управлением СУБД MySQL, первая (resources) из которых содержит ИР, вторая (threat) – перечень угроз (действий) и третья – ПП (две первых БД имеют одинаковую структуру, представленную на рис. 3).

Name	Type	Length	Decimals	Allow Null	
id	int	10	0	☐	🔑1
name	varchar	200	0	☐	
id_par	int	10	0	☐	

Рис. 3. Структура таблиц БДИР и БДУ

Далее в МФКД формируются ключевые значения ЛП LR и C_{EC_i}, термах $\underset{\sim}{T}_{LR_j}$ и $\underset{\sim}{T}_{C_{EC_i}}$, соответствующие интервалы для оценки, а также количество $\{EC_i\}$. Данные ЛП C_{EC_i} и $\{EC_i\}$ передаются в МБХ, где производится определение $ec_i^{BC_{1bc_1}}$ (рис. 4). Для этого в модуль дополнительно поступают результирующие величины из МИБХ, а именно идентифицированные BC_{1bc_1}. Выходные значения из МБХ поступают в МБК для бинарной классификации по каждому BC_{1bc_1} $(bc_1 = \overline{1,n})$. Полученные

результаты из МБК передаются на МУР, вследствие чего рассчитывается $lr^{(BC_{lbq})}$ и $lr^{(cp)}$. Сформированные в МФКД значения ЛП поступают в МЛР, где осуществляется лингвистическое распознавание полученных $lr^{(BC_{lbq})}$ и $lr^{(cp)}$. Далее в МГО формируются отчеты на основе величин из МЛР, МУР и МИБХ.

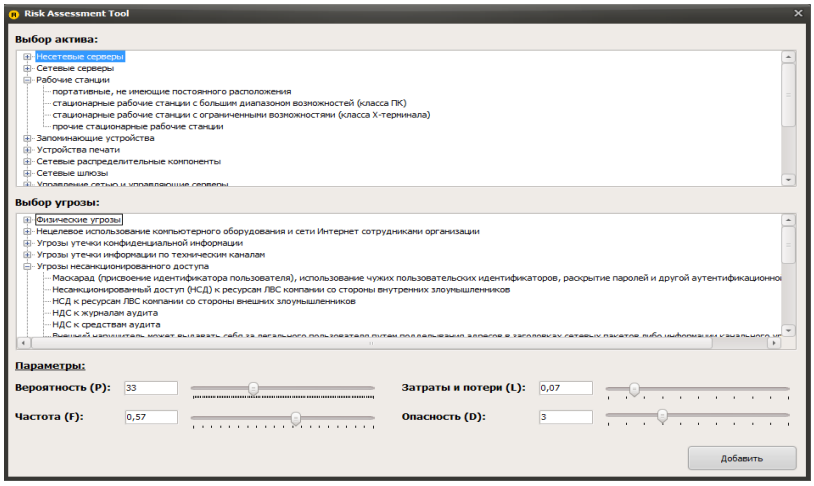

Рис. 4. Пример работы с МБХ

На основе разработанной структуры First-CAOP системы можно создавать 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 в детерминированной среде.

Ахметов Бахыджан Сражатдинович
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Казахстан
E-mail: b_akhmetov@ntu.kz

Akhmetov B.S.
Kazakh National Research Technical University of K.I. Satpayev, Almaty, Kazakhstan

Корченко Александр Григорьевич
Национальный авиационный университет, Украина

Korchenko A.G.
National Aviation University, Ukraine

Казмирчук Светлана Владимировна
Национальный авиационный университет, Украина

Kazmirchuk S.V.
National Aviation University, Ukraine

Жекамбаева Майгул Несипалдыкызы
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Казахстан

Zhekambayeva M.N.
Kazakh National Research Technical University of K. I. Satpayev, Almaty, Kazakhstan