BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 354 (2015), 226 – 230

THE RESEARCH OF SYSTEM ASSESSMENT OF RISKS OF INFORMATION SAFETY

A. G. Korchenko[1], S. V. Kazmirchuk[1], S. A. Gnatyuk[1], N. A. Seilova[2], Zh. K. Alimseitova[2]

[1] National Aviation University, Kiev, Ukraine;
[2] Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan.
E-mail: seilova_na@mail.ru

Key words: risk analysis, risk assessment, information security, threat model.

Abstract. It is shown that the basic phase to building a comprehensive information security system to ensure the security of information resources in processing them using information and telecommunication systems, is the development of threat models, development methodology which includes risk analysis and assessment. In order to evaluate and analyzes the risks in the automatic mode, you must use the software. Examines and analyzes of the software based on DetM and FuzM methods.

УДК 681.32 2

ИССЛЕДОВАНИЕ СИСТЕМЫ ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. Г. Корченко[1], С. В. Казмирчук[1], С. В. Гнатюк[1], Н. А. Сейлова[2], Ж. К. Алимсеитова[2]

[1] Национальный авиационный университет, Киев, Украина;
[2] Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан

Ключевые слова: анализ рисков, оценка рисков, защита информации, модели угроз.

Аннотация. Показано, что базовым этапом построения комплексной системы защиты информации для обеспечения безопасности информационных ресурсов, при обработке их с помощью информационно-телекоммуникационной системы, является разработка модели угроз, методология создания которой включает в себя анализ и оценку риска. Для того, чтобы проводить оценку и анализ рисков в автоматическом режиме необходимо использовать программное обеспечение. Рассматривается и проводится анализ программного обеспечения, основанного на DetM и FuzM методах.

Базовым этапом построения комплексной системы защиты информации (КСЗИ) для обеспечения безопасности информационных ресурсов (ИР), при обработке их с помощью информационно-телекоммуникационной системы (ИТС), является разработка модели угроз (МУ), методология создания которой включает в себя анализ и оценку риска (АОР).

На сегодняшний день существует необходимость в эффективных средствах, которые позволили бы в автоматизированном режиме осуществлять АОР. В этой связи целью данной работы является создание системы АОР, позволяющих повысить эффективность формирования МУ.

Для реализации процесса АОР, как одного из этапов при построении КСЗИ и системы менеджмента информационной безопасности, предлагается использовать новое программное решение соответствующих систем оценивания, которые основаны на логико-лингвистическом подходе, DetM и FuzM методах, методологии синтеза систем АОР потерь ИР и модели интегрированного представления параметров риска.

Указанное программное решение дает возможность на практике осуществлять оценивание при различных исходных величинах, а также учитывать возможность четкого детерминирования экспертом оцениваемых параметров и условия, когда эксперт сомневается в однозначности своих приоритетов. В соответствующей системе, при оценивании в нечетких условиях для интерпретации описаний естественного языка используют лингвистические переменные (ЛП), например, DR=«СТЕПЕНЬ РИСКА», с определенным количеством термов, которые отображаются нечеткими числами (НЧ) относительно интервалов значений, количество которых зависит от числа используемых термов.

Базовый алгоритм работы системы можно описать следующими этапами: 1) Создание нового проекта пользователей (ПП) или открытие существующего; 2) Указание имени существующего ПП; 3) Открытие ПП с сохраненными настройками и имеющимися данными, которые хранятся в базы данных (БД) ПП; 4) Указание имени нового ПП и осуществление выбора метода DetM или FuzM; 5) Создание проекта с выбранными параметрами, реализуется созданием таблицы ПП в БД и загрузка пустого проекта; 6) Выбор ИР, А и указание значения $ek_i^{A_a}$; 7) Оценка $dr^{(A_a)}$ для указанного набора ИР$_h$, А$_a$ и Е$_e$; 8) Запись в БД пользовательских данных и рассчитанного $dr^{(A_a)}$; 9) Расчет $dr^{(cp)}$ для каждого ИР указанного в ПП; 10) Генерация отчетов с указанием всех ИР$_h$ и А$_a$ для них, информации о $dr^{(cp)}$ для ИР в числовой и лингвистической форме, а также $dr^{(A_a)}$ для каждой угрозы в отдельности.

Рассмотрим работу системы более детально. Она дает возможность использовать готовые ПП из БД ПП. Здесь используется три БД под управлением СУБД MySQL, первая (resources) из которых содержит ИР, вторая (threat) – перечень угроз (У) (действий) и третья – ПП.

После определения ПП, осуществляется выбор метода, по которому будет реализоваться оценивание (рисунок 1). В дальнейшем на вход поступают исходные данные (ИД), которые выбираются экспертом.

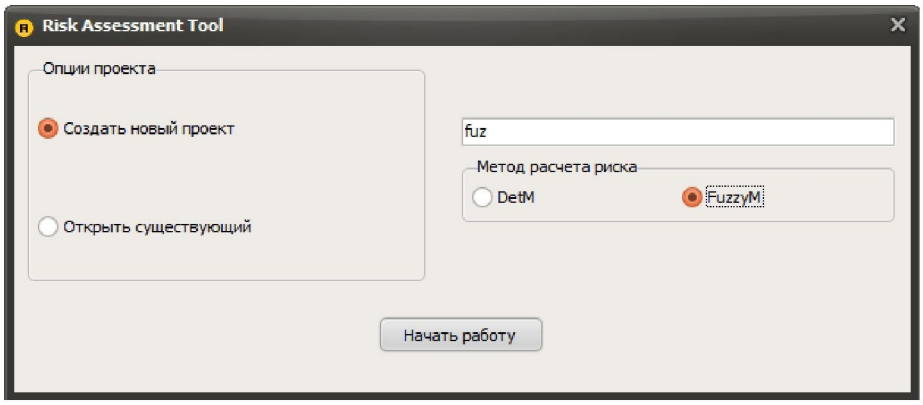


Рисунок 1 – Внешний вид главного окна программного продукта

При выборе DetM метода, далее в модуле формирования ключевых данных (МФКД) формируются ключевые значения ЛП ***DR*** и K_{EK_i}, термах T_{DRj} и $T_{K\,EK_{ij}}$, соответствующие интервалы для оценки, а также количество $\{EK_i\}$. Данные ЛП K_{EK_i} и $\{EK_i\}$ передаются в модуль оценки значений оценочных компонент (МОК), где производится определение $ek_i^{A_a}$ (рисунок 2).

Для этого в модуль дополнительно поступают результирующие величины из модуля инициализации идентифицирующих компонент (МИИК), а именно идентифицированные А$_a$. Выходные значения из МОК поступают в модуль бинарной классификации (МБК) для бинарной классификации по каждому A_a $(a=\overline{1,n})$. Полученные результаты из МБК передаются на модуль оценки значения степени риска (МСР), вследствие чего рассчитывается $dr^{(A_a)}$ и $dr^{(cp)}$. Сформированные в МФКД значения ЛП поступают в модуль лингвистического распознавания (МЛР),

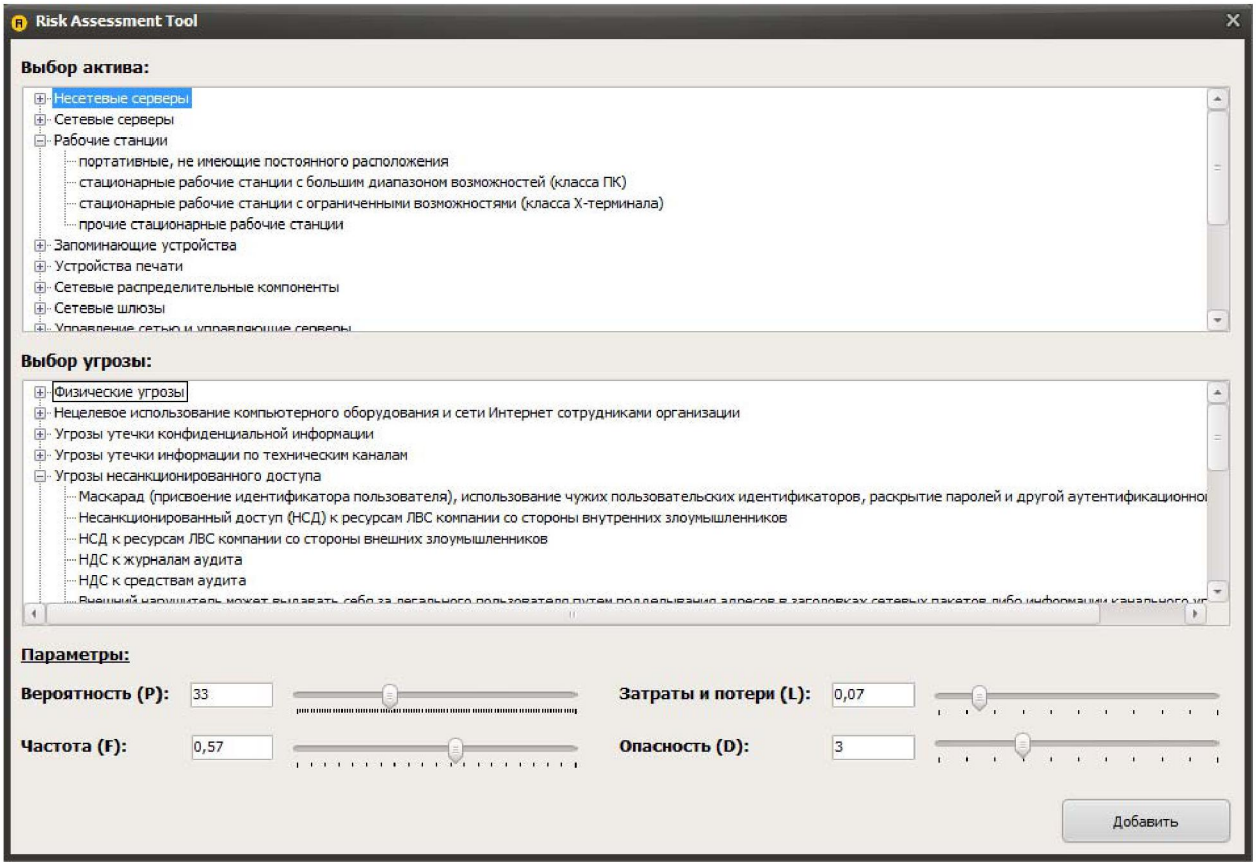


Рисунок 2 – Пример работы с МОК

где осуществляется лингвистическое распознавание полученных $dr^{(A_a)}$ и $dr^{(cp)}$. Далее в модуле генерации отчетов (МГО) формируются отчеты на основе величин из МЛР, МСР и МИИК.

Далее рассмотрим работу системы при выборе FuzM метода, который в отличие от DetM, дает возможность оценивать степень риска при условии, что эксперт не всегда может однозначно определить предпочтения в отношении оцениваемых параметров.

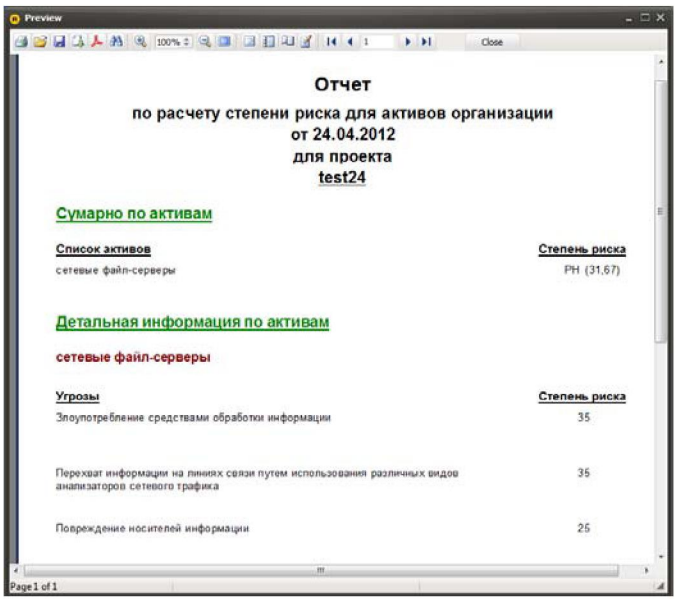
При выборе данного метода подключается модуль формирования эталонных значений (МФЭЗ), который предназначенный для построения функций принадлежности (ФП) эталонных нечетких чисел (НЧ) на основании принятого экспертами решения о количестве термов ЛП. Здесь экспертами определяются эталонные НЧ для ЛП ***DR*** и K_{EK_i} относительно интервалов значений, количество которых зависит от числа используемых термов, например, если их m, то для ***DR*** 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 $\mu_j(dr)$, а для K_{EK_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 $\mu_j(k_{EK_i})$. В результате работы модуля формируются ЛП ***DR***, K_{EK_i} и их интервалы, а также НЧ и ФП.

Сформированные в МФЭЗ значения ЛП K_{EK_i}, эталоны НЧ, ФП $\mu_j(k_{EK_i})$ и интервалы значений ЛП используются в МОК, для последующей оценки $ek_i^{A_a}$ каждого определенного $\{EK_i\}$. Полученные ИД передаются в модуль классификации текущих значений (МКТЗ), где производится классификация значений $ek_i^{A_a}$ с помощью результирующих исходящих значений из МФКД и МФЭЗ. Также в МКТЗ происходит сравнение нечетких эталонных с текущими значениями и

формируются $\lambda_{ij}^{(A_a)}$. Из МКТЗ полученные $\lambda_{ij}^{(A_a)}$ поступают в МСР, где для каждого A_a определяется $dr^{(A_a)}$ и $dr^{(cp)}$. Далее ИД передаются на модуль формирования структурированного параметра риска (МФСПР), где определяется $SP^{(A_a)}$, а в МГО формируется результирующий отчет по данным из МСР, МФСПР и МИИК.

Все необходимые данные и результаты заносятся в соответствующую БД и резервируются для обеспечения большей надежности, которая позволяет оперативно изменять ИД без модификации программного кода и структуры системы.

Примеры сформированных отчетов МГО при выборе DetM и FuzM представлены соответственно на рисунке 3 а и б.



Preview

Отчет

по расчету степени риска для активов организации
от 24.04.2012
для проекта
test24

Сумарно по активам

Список активов	Степень риска
сетевые файл-серверы	РН (31,67)

Детальная информация по активам

сетевые файл-серверы

Угрозы	Степень риска
Злоупотребление средствами обработки информации	35
Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика	35
Повреждение носителей информации	25

Page 1 of 1

а) DetM

Отчет

по расчету степени риска для активов организации
от 22.05.2012
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

б) FuzM

Рисунок 3 – Пример сгенерированного отчета