

УДК 004.056.5(045) Корченко А.Г., Волянская В.В., Казмирчук С.В., Охрименко А.А.

## СИСТЕМЫ АНАЛИЗА И ОЦЕНКИ РИСКА ПОТЕРЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В работе представлено структурные схемы систем анализа и оценки риска безопасности государственных информационных ресурсов, которые были разработаны на основе логико-лингвистического подхода, предложенных методов, модели интегрированного представления параметров риска, а также методологии синтеза систем анализа и оценки риска потерь информационных ресурсов. На основании предложенных структурных решений разработаны алгоритм и программное средство, которое, в отличие от известных, использует в качестве входных данных различные множества оценочных параметров, что повышает гибкость, удобство использования, интеграцию возможностей и расширяет возможность проектируемых средств АОР функционирующих как в детерминированной, так и в нечеткой, слабоформализованной среде.

Ключевые слова: риск, анализ риска, оценка риска, система анализа и оценки риска, параметры риска, безопасность государственных информационных ресурсов.

Базовым этапом построения комплексной системы защиты информации (КСЗИ) для обеспечения безопасности государственных информационных ресурсов (ГИР), при обработке их с помощью автоматизированной системы (АС), является разработка модели угроз (МУ) [7], методология создания которой, включает в себя анализ и оценку риска (АОР) [6]. На сегодняшний день существует необходимость в эффективных средствах, которые позволили бы в автоматизированном режиме осуществлять АОР. В этой связи целью данной работы является создание систем АОР, позволяющих повысить эффективность формирования МУ.

На основании методологии синтеза систем АОР потерь информационных ресурсов (ИР) [2], которая основана на логико-лингвистическом подходе, предложенных методах [3] и модели интегрированного представления параметров риска (ИППР) [1], разработаны Det-АОР и Fuz-АОР системы, позволяющие проводить оценку при различных исходных величинах, учитывающих не только возможности эксперта четко детерминировать оцениваемые параметры, но и его неуверенность в своих суждениях.

Структурная схема Det-АОР системы содержит (рис. 1): подсистемы обработки первичных параметров (ПСОПП) и формирования данных (ПСФД), модули лингвистического распознавания (МЛР), генерации отчетов (МГО) и служит для АОР при условии, когда эксперт имеет четкие (бинарные) предпочтения относительно значений оцениваемых параметров.

Согласно разработанной методологии (этапы 2-4) [2] строится ПСОПП, 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); модуль инициализации идентифицирующих компонент (МИИК); модуль формирования ключевых данных (МФКД). База данных БДИР содержит соответствующие списки множества  $ИР \in \{ИР_h\} (h = \overline{1, r})$  (где  $h$  – указатель (номер) текущего идентификатора ИР, а  $r$  – количество ИР), БДУ включает множество  $A \in \{A_a\} (a = \overline{1, n})$  (где  $a$  – указатель (номер) текущего идентификатора угрозы [1], а  $n$  – количество угроз) и  $E \in \{E_e\} (e = \overline{1, 7})$  (где  $e$  – указатель (номер) текущего идентификатора события), а БДПП содержит списки множества  $ПП \in \{ПП_p\} (p = \overline{1, c})$  (где  $p$  – указатель (номер) текущего идентификатора проектов пользователей (ПП), а  $c$  – их количество), которая предназначена для хранения полученных результатов от предыдущих АОР в отдельных таблицах, позволяющих использовать ПП при очередной оценке и могут, например, иметь вид и структуру представленную на рис. 2. При

формировании БДИР (активов), например, можно воспользоваться классификацией ресурсов из описания метода СРАММ для профиля Commercial, а при формировании БДУ – классификацией из [9]. Модуль МИИК предназначен для выбора из БДИР и БДУ, соответственно характерные для объекта оценки ИР и  $A_a, E_e$ . Модуль МФКД реализуется согласно этапам 5-7 методологии [2] и предназначен для формирования лингвистических переменных (ЛП): ЛП “СТЕПЕНЬ РИСКА” ( $DR$ ) и “УРОВЕНЬ ОЦЕНОЧНОГО КОМПОНЕНТА  $EK_i$ ” ( $K_{EK_i}$ ), которые определяются соответственно кортежами [3]  $\langle DR, T_{DR}, X_{DR} \rangle$ ,  $\langle K_{EK_i}, T_{K_{EK_i}}, X_{EK_i} \rangle$ , где базовые терм-множества задаются  $m$  термами  $T_{DR} = \bigcup_{j=1}^m T_{DR_j}$

и  $T_{K_{EK_i}} = \bigcup_{j=1}^m T_{K_{EK_{ij}}} (j = \overline{1, m})$ , также здесь осуществляется выбор количества оценочных компонент из их полного множества  $EK_{3Fh} \in \{EK_i\} = \{P, F, L, D, S, V\}$  ( $i = \overline{1, g}$ ,  $i$  – идентификатор оценочного компонента, а  $g$  – количество этих компонент), где 3Fh – шестнадцатеричный код, бинарное значение которого отражает порядковые номера оценочных компонент в множестве [3]. В результате преобразований на выход модуля, поступают  $\{EK_i\}$ , ЛП  $DR$ ,  $K_{EK_i}$  и их терм-множества, а также соответствующие интервалы для последующей классификации и лингвистического распознавания.

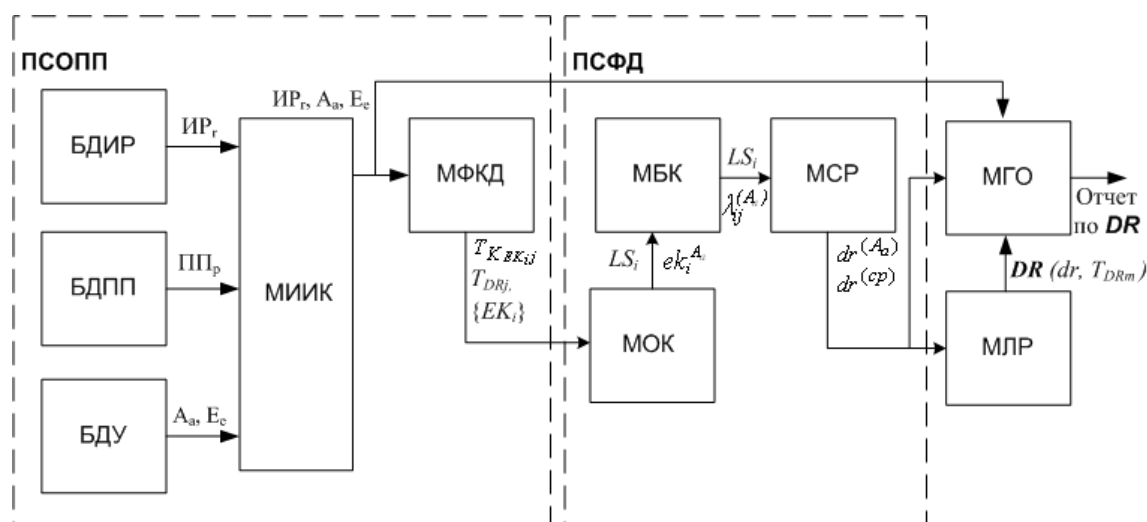


Рис. 1. Структурная схема Det-AOP системы

Далее в ПСФД формируются данные для последующей оценки степени риска (СР). Она содержит: модуль оценки значений оценочных компонент (МОК), который согласно этапам 9 и 8 методологии [2], предназначен соответственно для определения экспертами текущих значений,  $ek_i^{A_a}$ , т.е.  $\{ek_i^A\} = \{ek_P^A, ek_F^A, ek_L^A, ek_D^A, ek_S^A, ek_V^A\}$ , где  $A \in \{A_a\} (a = \overline{1, 5})$  и определения их уровня значимости  $LS_i$ ,  $i = \overline{1, g}$ ; модуль бинарной классификации (МБК), в котором согласно этапу 10 методологии [2] осуществляет формирование значений  $\lambda_{ij}^{(A_a)}$  по выражениям (4) [3] с помощью полученных из МОК результатов  $ek_i^{A_a}$ ; модуль оценки значения СР (МСР), осуществляющий для каждой идентифицированной  $A_a (a = \overline{1, n})$  оценку СР  $dr^{(A_a)}$  по формуле (5) [3] и его среднее значение  $dr^{(cp)}$  по ИР (см. (7) [3]) с учетом результатов классификации текущей вычлены оценочных компонент  $\lambda_{ij}^{(A_a)}$  и их уровня значимости  $LS_i$ .

Модуль МЛР предназначен для лингвистической интерпретации значений  $dr^{(A_a)}$  и  $dr^{(cp)}$  с помощью сформированной ЛП **DR**, на основе ее терм-множеств и интервалов по выражению (6) [3].

Модуль МГО позволяет по результатам работы двух подсистем сгенерировать отчеты оценки СР, в которые заносятся все идентифицированные ИР, *A*, *E*, результаты оценки  $dr^{(A_a)}$ ,  $dr^{(cp)}$  и их лингвистический эквивалент.

Name	Type	Length	Decimals	Allow Null
id	int	11	0	<input type="checkbox"/>
resource	varchar	200	0	<input type="checkbox"/>
threat	varchar	200	0	<input type="checkbox"/>
probability	int	5	0	<input type="checkbox"/>
frequency	decimal	4	2	<input type="checkbox"/>
loss	decimal	4	2	<input type="checkbox"/>
danger	int	5	0	<input type="checkbox"/>
dr	decimal	4	2	<input checked="" type="checkbox"/>

Рис. 2. Пример таблицы ПП

(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	<input type="checkbox"/>	1
name	varchar	200	0	<input type="checkbox"/>	
id_par	int	10	0	<input type="checkbox"/>	

Рис. 3. Структура таблиц БДИР и БДУ

Далее в МФКД формируются ключевые значения ЛП **DR** и  $K_{EK_i}$ , термах  $T_{DR_j}$  и  $T_{K_{EK_i}}$ , соответствующие интервалы для оценки, а также количество  $\{EK_i\}$ . Данные ЛП  $K_{EK_i}$  и  $\{EK_i\}$  передаются в МОК, где производится определение  $ek_i^{A_a}$  (рис. 4).

The screenshot shows the 'Risk Assessment Tool' interface. It is divided into three main sections:

- Выбор актива (Asset Selection):** A tree view with expandable nodes. 'Несетевые серверы' is selected. Other nodes include 'Сетевые серверы', 'Рабочие станции' (with sub-items for portable, stationary, and other), 'Запоминающие устройства', 'Устройства печати', 'Сетевые распределительные компоненты', 'Сетевые шлюзы', and 'Управление сетью и управляющие серверы'.
- Выбор угрозы (Threat Selection):** A list of threats with expandable nodes. 'Физические угрозы' is selected. Other threats include 'Нецелевое использование компьютерного оборудования и сети Интернет сотрудниками организации', 'Угрозы утечки конфиденциальной информации', 'Угрозы утечки информации по техническим каналам', and 'Угрозы несанкционированного доступа' (with sub-items for masquerade, unauthorized access, and audit logs).
- Параметры (Parameters):** Four sliders and input fields:
  - Вероятность (P): 33
  - Затраты и потери (L): 0,07
  - Частота (F): 0,57
  - Опасность (D): 3

A 'Добавить' (Add) button is located at the bottom right.

Рис. 4. Пример работы с МОК

Для этого в модуль дополнительно поступают результирующие величины из МИИК, а именно идентифицированные  $A_a$ . Выходные значения из МОК поступают в МБК для бинарной классификации по каждому  $A_a$  ( $a = \overline{1, n}$ ) [3]. Полученные результаты из МБК передаются на МСР, вследствие чего рассчитывается  $dr^{(A_a)}$  и  $dr^{(cp)}$ . Сформированные в МФКД значения ЛП поступают в МЛР, где осуществляется лингвистическое распознавание полученных  $dr^{(A_a)}$  и  $dr^{(cp)}$ . Далее в МГО формируются отчеты на основе величин из МЛР, МСР и МИИК.

Далее предлагается Fuz-АОР система, которая в отличие от Det-АОР системы, дает возможность оценивать СР при условии, что эксперт не всегда может однозначно определить предпочтения в отношении оцениваемых параметров. Структурная схема такой системы (рис. 5) содержит ПСОПП, подсистему формирования нечетких данных (ПСФНД), а также модули формирования структурированного параметра риска (МФСР) и МГО.

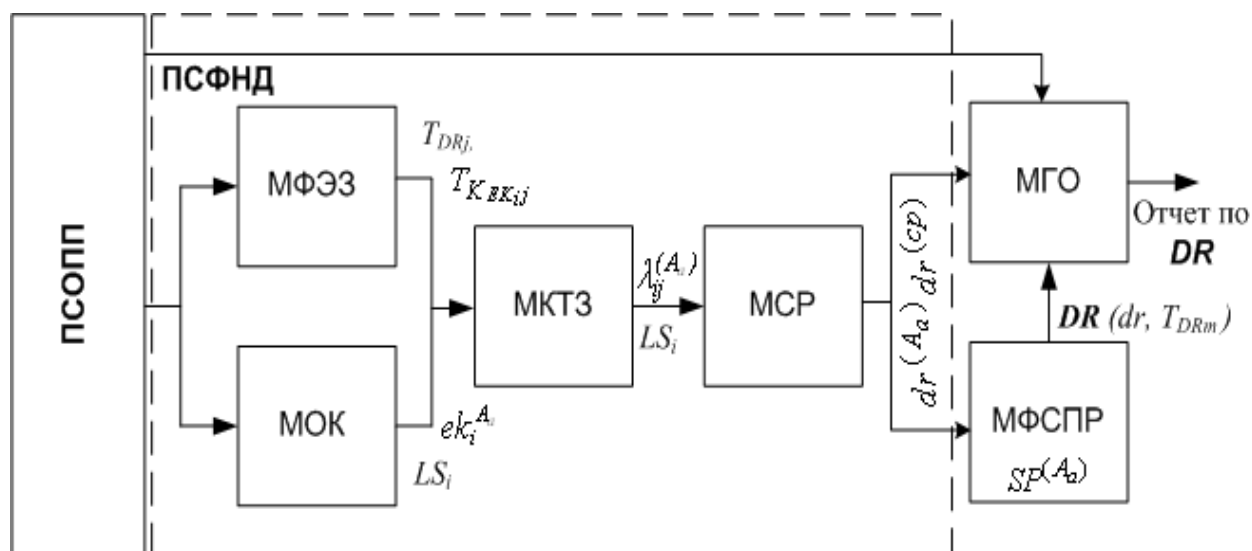


Рис. 5. Структурная схема Fuz-АОР системы

Функции ПСОПП обладают полным изоморфизмом с аналогичной подсистемой в Det-АОР системе, а ПСФНД формирует нечеткие данные, которые дают возможность при исходных величинах учитывать неуверенность эксперта в процессе оценивания СР. Подсистема ПСФНД содержит модули формирования эталонных значений (МФЭЗ), МОК, классификации текущих значений (МКТЗ) и МСР. Модуль МФЭЗ предназначенный для построения функций принадлежности (ФП) эталонных нечетких чисел (НЧ) на основании принятого экспертами решения о количестве термов ЛП (согласно этапам 6 и 7 методологии [2]). Здесь экспертами, на основе выражения (8) [3] и собственных приоритетов, 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  $[b_{11}; b_{21}[, [b_{21}; b_{12}[, [b_{12}; b_{22}[, \dots, [b_{2m-1}; b_{1m}[, [b_{1m}; b_{2m}[$  ( $j = \overline{1, m}$ ) и ФП  $\mu_j(dr)$ , а для  $K_{EK_i}$  –  $[b_{11}; b_{21}[, [b_{21}; b_{12}[, [b_{12}; b_{22}[, \dots, [b_{2m-1}; b_{1m}[, [b_{1m}; b_{2m}[$  ( $j = \overline{1, m}$ ) 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. Модуль МОК имеет то же функциональное предназначение, что и аналогичный модуль в Det-АОР системе, а МКТЗ позволяет получать, как нечеткие значения параметров с помощью МФЭЗ (на основе эталонных значений ЛП  $K_{EK_i}$

сформированными экспертами, осуществляется определение принадлежности  $ek_i^{A_a}$  заданному НЧ, по которому вычисляется значение  $\lambda$  с помощью выражения (9) [3]), так и учитывать четкие (без неопределенностей) значения. Аналогично Det-AOP системе здесь также определяется  $LS_i$ . В результате работы модуля получаем значения  $\lambda_{ij}^{(A_a)}$  для каждой идентифицированной  $A_a$  в МИИК и  $LS_i$ . Модуль МСР имеет изоморфные функции относительно МСР в Det-AOP системе. Данные из него поступают в МФСПР, где на основании вычисленных значений  $dr^{(A_a)}$ ,  $dr^{(cp)}$  и построенных эталонов, с помощью выражения (11) [3] определяется структурированный параметр  $SP^{(A_a)}$ , который позволяет получить как числовое значение СР, так и его лингвистическую интерпретацию, учитывающую неуверенность эксперта при формировании текущих значений оценочных компонент с дальнейшей классификацией посредством параметра  $\lambda_{ij}^{(A_a)}$ . Модуль МГО также как аналогичный модуль в Det-AOP системе предназначен для генерации результирующих отчетов.

Опишем работу Fuz-AOP системы. Функции ПСОПП совпадают с функциями аналогичной подсистемы в Det-AOP системе. Полученные данные из МФКД  $T_{DRj}$ ,  $T_{KEK_{ij}}$ ,  $\{EK_i\}$  поступают на МФЭЗ и МОК. 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 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 согласно выражению (9) [3] 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 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.

На основании предложенных структурных схем Det-AOP и Fuz-AOP систем можно реализовать программные приложения, позволяющие производить АОР потери ГИР в автоматизированном режиме, их базовый алгоритм работы (рис. 6) можно описать следующими этапами:

- 1) Создание нового ПП или открытие существующего;
- 2) Указание имени существующего ПП;
- 3) Открытие ПП с сохраненными настройками и имеющимися данными, которые хранятся в БДПП;
- 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<sub>h</sub>, А<sub>a</sub> и Е<sub>e</sub>;
- 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  $IP_h$  и  $A_a$  для них, информации о  $dr^{(cp)}$  для ИР в числовой и лингвистической форме, а также  $dr^{(Aa)}$  для каждой угрозы в отдельности.

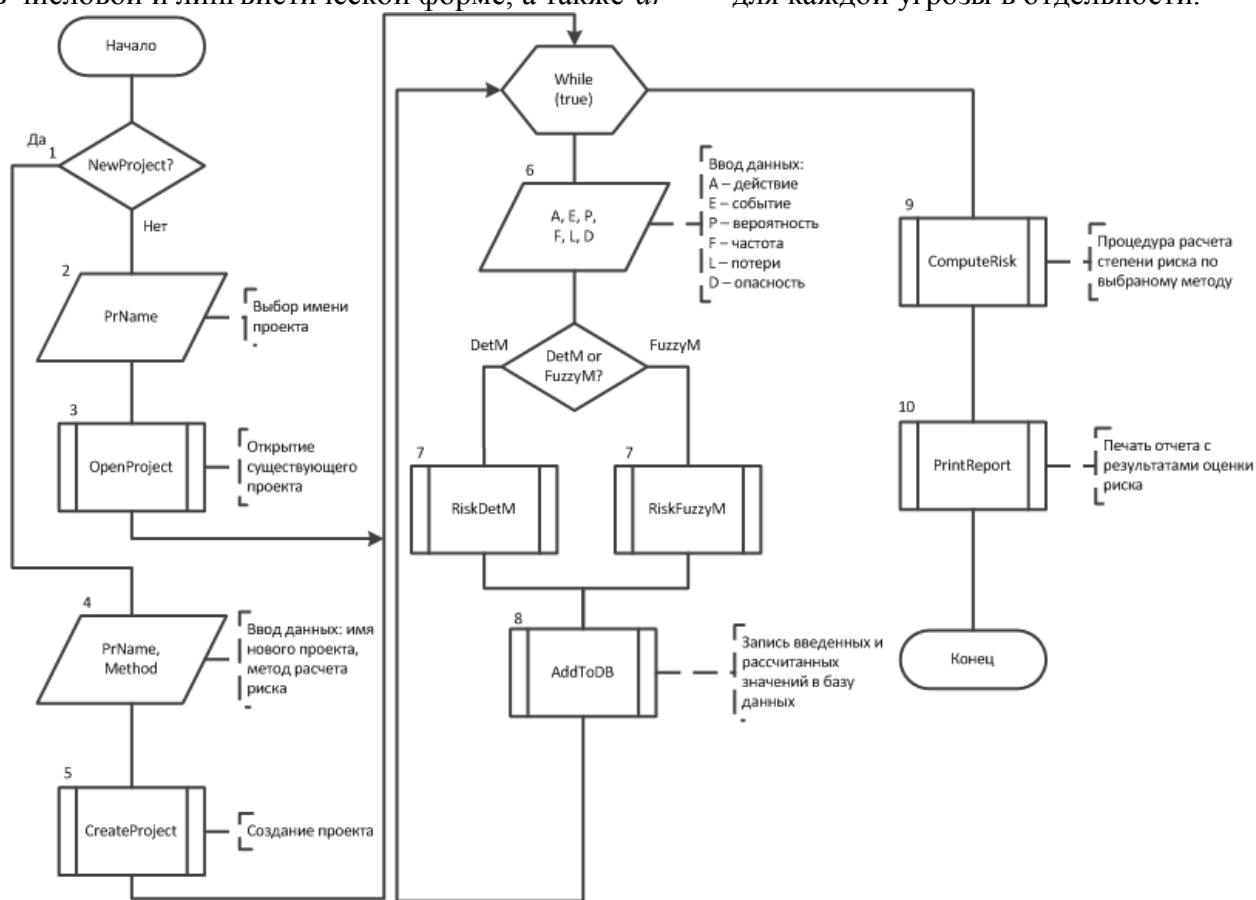
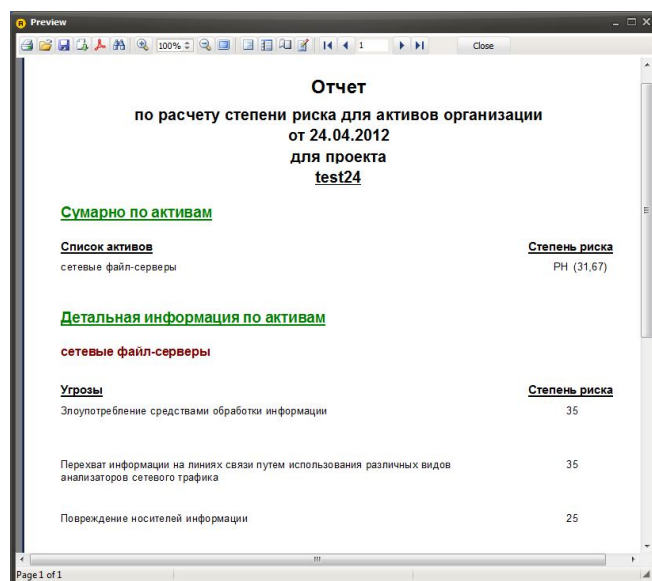


Рис. 6. Базовый алгоритм работы систем АОР потери ГИР

Примеры сформированных отчетов МГО Det-AOP и Fuz-AOP систем представлены соответственно на рис. 7 а и б.



а) Det-AOP система

**Отчет**  
по расчету степени риска для активов организации  
от 22.05.2012  
для проекта  
fuz

Суммарно 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) Fuz-AOP система

Рис. 7. Пример сгенерированного отчета



Рис. 8 Внешний вид главного окна программного продукта

На основе разработанных структур Det-AOP и Fuz-AOP систем созданы программные средства (рис. 8), которые в отличие от известных [4, 5, 8] используют в качестве входных данных различные наборы оценочных параметров, что повышает гибкость, удобство

использования, интеграцию возможностей и расширяет возможность проектируемых средств AOP функционирующих как в детерминированной, так и в нечеткой, слабоформализованной среде.

## ЛИТЕРАТУРА

1. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №1 (50). – С. 96 – 101.
2. Корченко А.Г. Методологию синтеза систем анализа и оценки риска потерь информационных ресурсов / Корченко А.Г., Казмирчук С.В. // Защита информации – 2012. – №2. – С. 24-28.
3. Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / Корченко А.Г., Щербина В.П., Казмирчук С.В. // Защита информации – 2012. – №1. – С. 126-139.
4. Луцкий М.Г. Исследование программных средств анализа и оценки риска информационной безопасности / Луцкий М.Г., Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №3. – С. 97-108.
5. Луцкий М.Г. Современные средства управления информационными рисками / Луцкий М.Г., Иванченко Е.В., Корченко А.Г., Казмирчук С.В., Охрименко А.А. // Защита информации – 2012. – №1. – С. 5-16.
6. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04 грудня 2000 р. № 53.
7. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі Затверджено наказом ДСТСЗІ СБ України від 08 листопада 2005 р. № 125.
8. Скулыш Е.Д. Средства анализа и оценки риска информационной безопасности / Скулыш Е.Д., Корченко А.Г., Горбенко Ю.И., Казмирчук С.В. // Інформаційна безпека. Людина, суспільство, держава – 2011. – №3 (7). – С.31-48.
9. ISO/IEC 27002:2005 Информационные технологии. Свод правил по управлению защитой информации с учетом Технической поправки 1, опубликованной 2007-07-01.

Надійшла: 12.05.2012

Рецензент: д.т.н., проф. Хорошко В.О.