DOI: 10.18372/2225-5036.22.11105

ИНТЕГРИРОВАННАЯ АДАПТИВНАЯ СИСТЕМА ОЦЕНИВАНИЯ РИСКОВ БЕЗОПАСНОСТИ РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Светлана Казмирчук[1], Андрей Гололобов[1], Марина Мовчан[2], Людмила Рыбалка[1]

[1]Национальный авиационный университет, Украина
[2]Европейский университет, Украина

КАЗМИРЧУК Светлана Владимировна, к.т.н.

Год и место рождения: 1985 год, г. Алматы, Республика Казахстан.
Образование: Национальный авиационный университет, 2006 год.
Должность: доцент кафедры безопасности информационных технологий с 2012 года.
Научные интересы: информационная безопасность, системы менеджмента информационной безопасности, защита программного обеспечения, комплексные системы защиты информации, управление информационными рисками.
Публикации: более 90 публикаций, среди которых монографии, учебные пособия, научные статьи, материалы и тезисы докладов конференций.
E-mail: sv.kazmirchuk@gmail.com

ГОЛОЛОБОВ Андрей Юрьевич

Год и место рождения: 1983 год, г. Киев, Украина.
Образование: НТУ Украины «Киевский политехнический институт», 2006 год.
Должность: соискатель кафедры безопасности информационных технологий.
Научные интересы: информационная безопасность, программирование.
Публикации: более 17 печатных работ, среди которых научные статьи, материалы и тезисы докладов конференций.
E-mail: b2d@ukr.net

МОВЧАН Марина Сергеевна

Год и место рождения: 1989 год, г. Киев, Украина.
Должность: студентка кафедры кибербезопасности и управления защитой информационных систем с 2015 года.
Научные интересы: информационная безопасность.
Публикации: материалы и тезисы докладов на научных конференциях.
E-mail: marsmovchan@gmail.com

РЫБАЛКА Людмила Павловна

Год и место рождения: 1996 год, г. Донецк, Украина.
Должность: студент кафедры безопасности информационных технологий с 2013 года.
Научные интересы: информационная безопасность.
Публикации: материалы и тезисы докладов на научных конференциях.
E-mail: fish96@list.ru

Аннотация. *В основу систем менеджмента информационной безопасности положена процедура управления рисками, которая включает в себя процессы их анализа и оценивания. На сегодняшний день существует множество средств оценивания рисков. В их основу, как правило, заложено использование статистических*

данных об инцидентах, связанных с нарушением безопасности ресурсов информационных систем. На предприятиях не всегда налажен процесс сбора таких данных. Существует необходимость в интегрированных средствах, которые позволили бы в автоматизированном режиме осуществлять оценивание рисков и реализовывать оценку как в четко детерминированной, так и нечеткой, слабоформализованной среде. В связи с этим, на основании модели синтеза систем оценивания рисков безопасности ресурсов информационных систем, интегрированного метода, а также методов инкрементирования и декрементирования порядка лингвистической переменной было предложено структурное решение интегрированной адаптивной системы анализа и оценивания рисков. На его основе разработаны алгоритм и программное средство, которое, в отличие от известных, использует в качестве входных данных различные множества оценочных параметров, что обеспечивает высокую гибкость и удобство использования как в детерминированной, так и в нечеткой, слабоформализованной среде.

***Ключевые слова**: риск, оценивание рисков, система оценивания рисков, характеристики риска, безопасность ресурсов информационных систем*.

Вступ

Международный стандарт ISO 27001:2013 [1] регламентирует порядок создания систем менеджмента информационной безопасности (ИБ). В основу таких систем положена процедура управления рисками ИБ, которая включает в себя процессы их анализа и оценивания. На сегодняшний день существует множество средств оценивания рисков (ОР), которые представлены методическим, программным и другим обеспечением [2]. В их основу, как правило, заложено использование статистических данных [2] об инцидентах, связанных с нарушением ИБ ресурсов информационных систем (РИС). На предприятиях не всегда налажен процесс сбора таких данных.

В связи с этим, существует необходимость в интегрированных средствах, которые позволили бы в автоматизированном режиме осуществлять ОР как в четко детерминированной, так и нечеткой, слабоформализованной среде. В этой связи целью данной работы является создание соответствующей интегрированной системы ОР ИБ РИС.

На базе модели синтеза систем ОР безопасности РИС [3], которая основана на логико-лингвистическом подходе, предложенных методах [4-6] и бистабильной интегрированной кортежной модели характеристик риска (БИМ) [7], разработана интегрированная адаптивная система ОР ИБ РИС (ИАСОР). Такая система позволит осуществлять оценивание при различных исходных величинах, учитывающих возможности эксперта четко детерминировать оцениваемые параметры и его неуверенность в своих суждениях, а также импортировать с других баз и трансформировать эталонные лингвистические переменные (ЛП) без участия экспертов соответствующей предметной области.

Структурная схема ИАСОР содержит (рис. 1) подсистемы формирования входных данных (ПФВД) и их обработки (ПОД), а также модули формирования структурированного параметра (МФСП) и генерации отчета (МГО). Система одновременно оперирует четкими и нечеткими параметрами с возможностью варьирования порядком ЛП, а изменение количества терм-множеств нечетких входных данных позволяет осуществлять адекватное ОР.

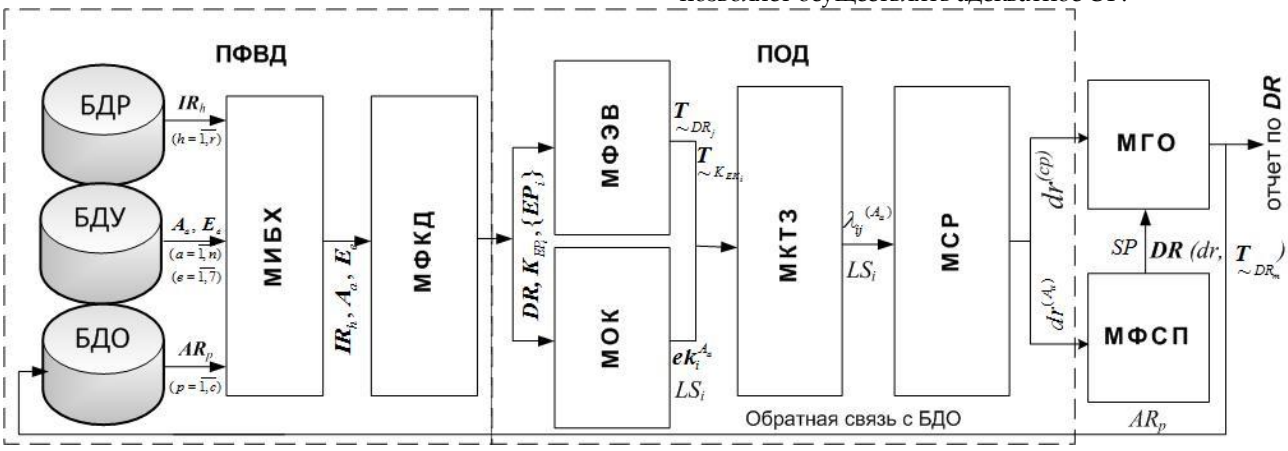

Рис. 1. Структурная схема ИАСОР

Опишем состав и функциональное назначение каждой из подсистем. Построение ПФВД осуществляется согласно разработанной модели (см. этапы 2-5 в [3]). Подсистема служит для подготовки входных данных (основанных на суждениях экспертов) в ПОД и состоит из баз данных (БД) РИС (БДР), угроз (БДУ) и результатов оценивания рисков (БДО), а также модуля инициализации базовых характеристик (МИБХ) и модуля формирования ключевых данных (МФКД). Согласно [2] БДР содержит соответствующие списки ресурсов из множества $\boldsymbol{IR} \in \{\boldsymbol{IR}_h\}\ (h = \overline{1,r})$ (где h – указатель (номер) текущего идентификатора РИС, а r – количество РИС), БДУ включает списки угроз и нарушений базовых характеристик ИБ, определенные соответственно множествами $\boldsymbol{A} \in \{\boldsymbol{A}_a\}\ (a = \overline{1,n})$ (где a – указатель (номер) текущего идентификатора угрозы [6], а n – количе-

ство угроз) и $\boldsymbol{E} \in \{\boldsymbol{E}_e\}\,(e=\overline{1,7})$ (где e – указатель (номер) текущего идентификатора нарушения базовых характеристик ИБ), а БДО содержит списки оценок риска, определенных множеством $\boldsymbol{AR} \in \{\boldsymbol{AR}_p\}$ $(p=\overline{1,c})$ (где p – указатель (номер) текущего идентификатора оценки риска, а c – их количество). Последняя предназначена для хранения в отдельных таблицах результатов, полученных от предыдущих ОР, которые используются при очередном оценивании и могут, например, иметь ориентировочную структуру, представленную на рис. 2. При формировании БДР, например, можно импортировать необходимые данные воспользовавшись классификацией ресурсов в CRAMM для профиля Commercial, а при формировании БДУ – классификацией из [2]. Модуль МИБХ предназначен для выбора из БДР и БДУ, соответственно характерные для объекта оценки *IR*, A_a и E_e. Модуль МФКД формируется согласно этапов 2 и 6 модели [3] и предназначен для получения множества параметров ОР в виде таких ЛП как «СТЕПЕНЬ РИСКА» (***DR***) и «УРОВЕНЬ ОЦЕНОЧНОГО КОМПОНЕНТА EP_i» ($\boldsymbol{K}_{EP_i}$), которые определяются соответственно кортежами <***DR***, $\underset{\sim}{\boldsymbol{T}}_{DR}$, $\underset{\sim}{\boldsymbol{X}}_{DR}$> и <$\boldsymbol{K}_{EP_i}$, $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$, $\underset{\sim}{\boldsymbol{X}}_{EP_i}$> [2], где базовые терм-множества могут задаваться m-термами $\underset{\sim}{\boldsymbol{T}}_{DR}=\bigcup_{j=1}^{m}\underset{\sim}{\boldsymbol{T}}_{DR_j}$ и $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}=\bigcup_{j=1}^{m}\underset{\sim}{\boldsymbol{T}}_{K_{EP_{ij}}}$ $(j=\overline{1,m},\ i=\overline{1,g})$. На основе этого модуля посредством синтетического кортежа $\langle \boldsymbol{AES}, \boldsymbol{CA}, \boldsymbol{D}, \boldsymbol{E}, \boldsymbol{F}, \boldsymbol{L}, \boldsymbol{P}, \boldsymbol{V}\rangle$ [7] осуществляется выбор необходимых оценочных компонент. В результате преобразований на выход ПФВД поступают {$\boldsymbol{EP}_i$}, а также ЛП ***DR*** и $\boldsymbol{K}_{EP_i}$.

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 в БДО

Далее в ПОД формируются данные для последующей оценки степени риска (СР). Она содержит: модуль оценки значений оценочных компонент (МОК), который образуется согласно этапов 8 и 9 модели [3] и используется для определения (посредством суждений экспертов) текущих значений $\boldsymbol{ep}_i^{A_a}$ (т.е. $\{\boldsymbol{ep}_i^{A_a}\} = \{ep_D^{A_a}, ep_F^{A_a}, ep_L^{A_a}, ep_P^{A_a}, ep_V^{A_a}\}$, где $\boldsymbol{A} \in \{\boldsymbol{A}_a\}, a=\overline{1,5}$) и уровня значимости оценочных компонент LS_i, $i=\overline{1,g}$; модуль формирования эталонных значений и их визуализации (МФЭВ), который предназначен для построения функций принадлежности (ФП) эталонных нечетких чисел (НЧ) на основании используемого экспертами порядка ЛП (согласно этапа 6 модели [3]); модуль классификации текущих значений (МКТЗ), в котором формируются величины $\lambda_{ij}^{(A_a)}$ $(j=\overline{1,m},\ i=\overline{1,g})$; модуль оценки значения СР (МСР), в котором непосредственно реализуется ОР. В МФЭВ на основании метода, использующего суждения экспертов определяются эталонные НЧ для ЛП ***DR*** и $\boldsymbol{K}_{EP_i}$ относительно интервалов значений, зависящих от числа используемых термов. Например, если количество интервалов m, то для ***DR*** их число 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 $\boldsymbol{K}_{EP_i}$ – [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*** и $\boldsymbol{K}_{EK_i}$. Здесь (согласно этапа 7 модели [3]) реализуются методы инкрементирования и декрементирования ЛП, т.е. посредством соответствующих функций, образуются эквивалентные ЛП, отличающиеся от исходных порядком и содержимым термов, но сохраняющие свои начальные свойства, отражающие исходные суждения экспертов. Данные методы работают с различными типами распределения НЧ по оси *dr* [4, 5]. Все исходные, преобразованные или импортированные с других БД эталоны могут визуализироваться.

Модуль МКТЗ (формируемый согласно этапа 10 модели [3]) предназначен для генерирования значений $\lambda_{ij}^{(A_a)}$ (согласно (8) в [6]) посредством полученных в МОК величин $\boldsymbol{ep}_i^{A_a}$.

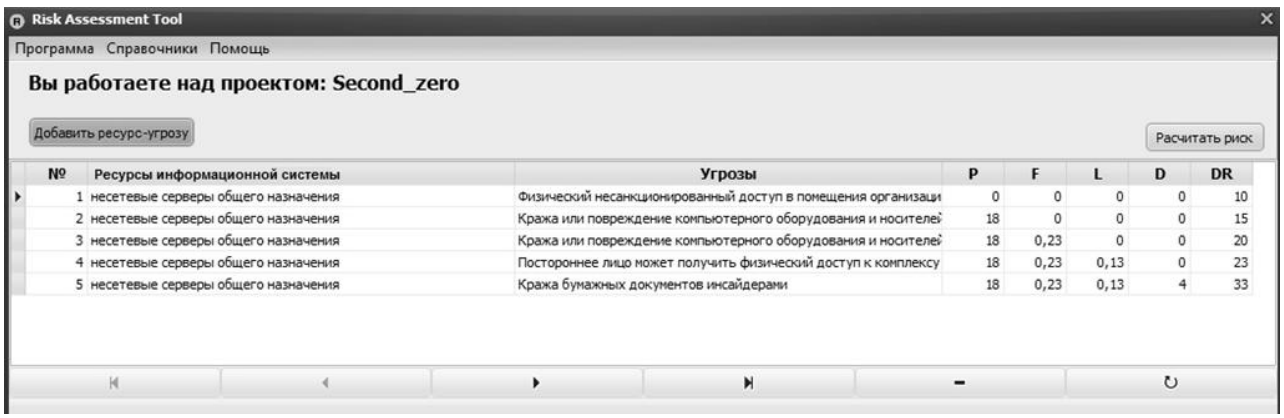

Рис. 3. Пример интерфейса МСР

В МСР (см. рис. 3) для каждой идентифицированной A_a $(a=\overline{1,n})$ осуществляется оценка СР $dr^{(A_a)}$ по формуле (9) в [6] и его среднего значения $dr^{(cp)}$ по каждому РИС (см. (11) в [6]) с учетом результатов классификации текущей вылечены оценочных компонент $\lambda_{ij}^{(A_a)}$ и соответствующего их уровня значимости LS_i. Данные из МСР поступают в МФСП, где на основании вычисленных значений $dr^{(A_a)}$, $dr^{(cp)}$ и построенных эталонов с помощью выражения (10) в [6] определяется структурированный параметр $SP^{(A_a)}$, который позволяет получить не только числовые значения СР, но и лингвистическую интерпретацию уровня уверенности эксперта (учитываемую методом формирования текущих значений оценочных компонент с дальнейшей их классификацией посредством параметра $\lambda_{ij}^{(A_a)}$).

С помощью МГО с учетом результатов работы ПФВД и ПОД генерируется отчеты по оценкам СР, которые содержат все идентифицированные $\boldsymbol{IR}_h$, $\boldsymbol{A}_a$ и $\boldsymbol{E}_e$ результаты оценки $dr^{(A_a)}$, $dr^{(cp)}$ и их лингвистические эквиваленты.

Разработанная система (см. рис. 1) в соответствие с алгоритмом (см. рис. 4) функционирует следующим образом. Согласно условия (вершина 1) определяется режим оценивания, т.е. осуществляется инициализация создания нового процесса ОР (вершины 2-3) или открытие существующего с имеющимися в БДО данными (вершины 4-5). Далее в МИБХ из БДР и БДУ поступают входные данные (ВД) $\boldsymbol{IR}_h$, $\boldsymbol{A}_a$ и $\boldsymbol{E}_e$, которые заранее определяются лицом, отвечающим за реализацию процесса ОР (вершина 6). Здесь используется три БД под управлением СУБД MySQL, первая из которых (resources) содержит РИС, вторая (threat) – перечень угроз и третья (assessment) – ОР. Далее в МФКД (вершина 7) формируются ключевые значения ЛП $\boldsymbol{DR}$, $\boldsymbol{K}_{EP_i}$ с соответствующими термами $\underset{\sim}{\boldsymbol{T}}_{DR_j}$ $(j=\overline{1,m})$, $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$ $(i=\overline{1,g})$ и оценочными интервалами. Здесь также на основе синтетического кортежа в [7] формируется подмножество $\{\boldsymbol{EP}_i\}$. Полученные $\underset{\sim}{\boldsymbol{T}}_{DR_j}$, $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$ и $\{\boldsymbol{EP}_i\}$ из МФКД поступают на МФЭВ и МОК. В МФЭВ (вершина 8) согласно потребности лица, отвечающего за процесс ОР, могут трансформироваться эталоны. Здесь также предусмотрена визуализация полученных и преобразованные эталонов.

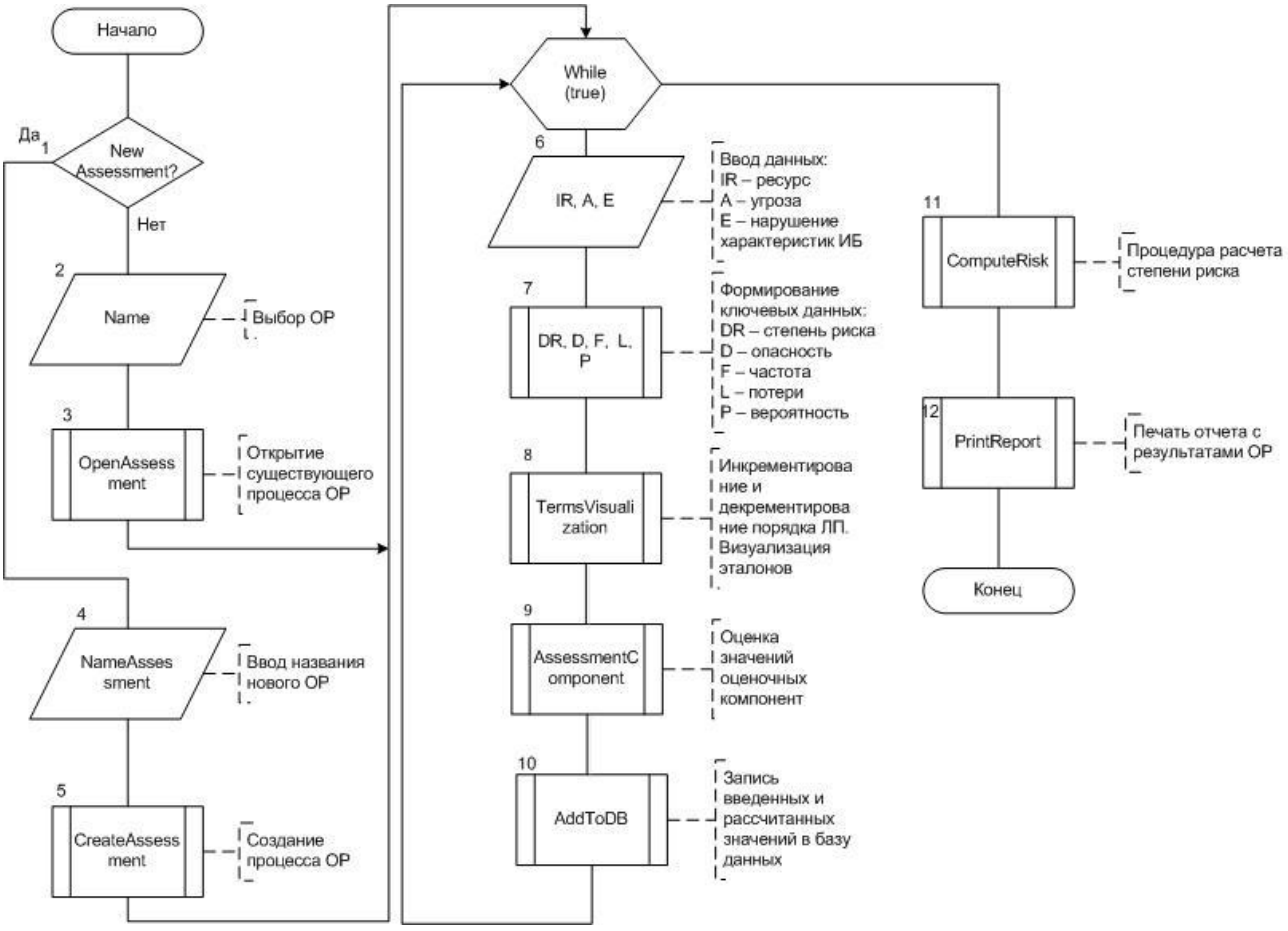

Рис. 4. Базовый алгоритм работы ИАСОР безопасности РИС

Далее полученные данные передаются в МКТЗ (вершины 9-10), где производится классификация значений $\boldsymbol{ep}_i^{A_a}$ с помощью исходящих из МФКД и МФЭВ значений. Также в МКТЗ осуществляется сравнение нечетких эталонов с текущими значениями и формируются $\lambda_{ij}^{(A_a)}$. Далее получен-

ные результаты заносятся в БДО. Из МКТЗ сформированные $\lambda_{ij}^{(A_a)}$ поступают в МСР (вершина 11), где для каждого A_a определяется $dr^{(A_a)}$ и $dr^{(cp)}$ для указанного набора IR_h, A_a и E_e. Далее ВД передаются на МФСП, где определяется $SP^{(A_a)}$. В МГО (вершина 12) формируется результирующий отчет по данным из МСР, МФСП и МИБХ с указанием всех IR_h, A_a и E_e, полученных $dr^{(A_a)}$ и $dr^{(cp)}$ в числовой и лингвистической форме, после чего все данные записываются в БДО. Пример сформированного отчета МГО ИАСОР представлен на рис. 5. Все необходимые данные (включая результаты) заносятся в соответствующую БД и для обеспечения большей надежности резервируются. Указанная БД позволяет оперативно изменять ВД без модификации программного кода и структуры системы.

На основе разработанной структурной схемы ИАСОР создано программное средство, для которого (в отличие от известных [2]) используют в качестве входных данных различные наборы оценочных параметров с возможность трансформирования порядка ЛП. Это обеспечивает высокую гибкость и интеграцию функциональных возможностей проектируемых средств ОР, функционирующих как в детерминированной, так и в нечеткой, слабоформализованной среде.

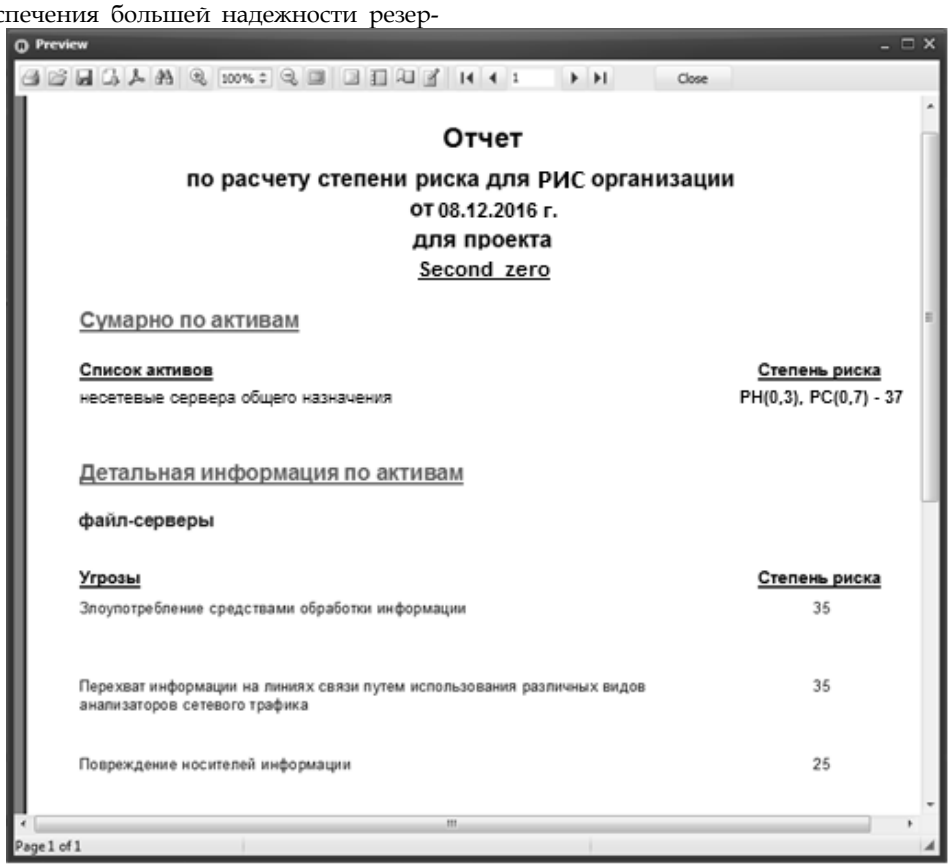

Рис. 5. Пример сгенерированного отчета

Литература

[1] Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013. – 34 p.

[2] Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук // Монография. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

[3] Казмирчук С.В. Синтез систем оценивания рисков безопасности ресурсов информационных систем / С.В. Казмирчук, А.Ю. Гололобов, А. Арджомандифард // Вісник Інженерної академії України. – 2016. – №3. – С. 78-81.

[4] Корченко А.Г. Метод n-кратного инкрементирования числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук, Б.С. Ахметов, М.Н. Жекамбаева // Безпека інформації. – 2015. – Т.21. –№2. – С. 191-200.

[5] Корченко А.Г. Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов, Н.А. Сейлова // Захист інформації. – 2014. – Т.16. – №4. – С. 284-291.

[6] Казмирчук С.В. Интегрированный метод анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Защита информации – 2014. – №3. – С. 252-261.

[7] Корченко А.Г. Бистабильная интегрированная кортежная модель характеристик риска / А.Г. Казмирчук, С.В. Казмирчук, Ю.А. Дрейс, А.Ю. Гололобов // Защита информации – 2016. – №4. – С. 314-323.

УДК 004.056.5 (045)

Казмірчук С.В., Гололобов А.Ю., Мовчан М.С., Рибалка Л.П. Інтегрована адаптивна система оцінювання ризиків безпеки ресурсів інформаційних систем

Анотація. *В основу систем менеджменту інформаційної безпеки покладена процедура управління ризиками, яка включає в себе процеси їх аналізу та оцінювання. На сьогоднішній день існує низка засобів оцінювання ризиків. В їх основу, як правило, закладено використання статистичних даних про інциденти, які пов'язані з порушенням безпеки ресурсів інформаційних систем. На підприємствах не завжди налагоджений процес збору таких даних. Існує необхідність в інтегрованих засобах, які дозволили б в автоматизованому режимі здійснювати оцінювання ризиків і реалізовувати оцінку як в чітко детермінованому, так і нечіткому, слабоформалізованому середовищі. У зв'язку з цим, на підставі моделі синтезу систем оцінювання ризиків безпеки ресурсів інформаційних систем, інтегрованого методу, а також методів інкрементування і декрементування порядку лінгвістичної змінної було запропоновано структурне рішення інтегрованої адаптованої системи аналізу та оцінювання ризиків. На його основі розроблені алгоритм і програмний засіб, який, на відміну від відомих, застосовує як вхідні дані різні множини оціночних параметрів, що забезпечує високу гнучкість і зручність використання як в детермінованому, так і в нечіткому, слабоформалізованому середовищі.*

Ключові слова*: ризик, оцінювання ризиків, система оцінювання ризиків, характеристики ризику, безпека ресурсів інформаційних систем.*

Kazmirchuk S., Gololobov A., Movchan M., Rybalka L. Integrated adaptive system of security risk assessment for information systems resources

Abstract. *The basis of the information security management systems is the procedure of risk management, which includes the processes of analysis and assessment. Nowadays, there is a number of different techniques of risk assessment. They are usually based on the use of statistical data on incidents, related to security violation of information systems resources. The process of collecting such data is not always organized at the enterprises. There is a need for integrated tools that would enable to carry out risk assessment in automatic mode and implement an assessment both in determined and in fuzzy, weakly formalized environment. In this regard, based on the model of the synthesis of the security risk assessment systems of information systems resources, integrated method, as well as the increment and decrement methods of linguistic variable it was proposed the structural solution of integrated adaptive system of analysis and risk assessment. On its basis the algorithm and software that, unlike known, uses as input the various sets of estimated parameters as entrance data that provides high flexibility and convenience of use both in determined, and in fuzzy, weakly formalized environment are developed.*

Key words: *risk, risk assessment, risk assessment system, the characteristics of risk, the security of information systems resources.*

Отримано *9 листопада 2016 року*, затверджено редколегією *21 листопада 2016 року*