nodes can explain increase resistance regard to these methods of cryptanalysis.
Index words: cryptography, block cipher, linear cryptanalysis, differential cryptanalysis, randomized replacement nodes.

Кінзерявий Василь Миколайович, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: v.kinzeryavyy@gmail.com

Кинзерявый Василий Николаевич, асистент кафедры безопасности информационных технологий Национального авиационного университета.
Kinzeryavyy Vasyl, Assistant of Academic Department of IT-Security, National Aviation University.

УДК 004.056.5(045)

АНАЛИЗ И ОЦЕНИВАНИЕ РИСКОВ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Светлана Казмирчук

Для построения систем менеджмента информационной безопасности, комплексных систем защиты информации и других систем безопасности необходимо проводить анализ и оценивание рисков. Существующие средства оценки в подавляющем большинстве основаны на статистических подходах. Во многих странах, как на уровне предприятий, так и на государственном уровне подобная статистика не ведется. Это ограничивает возможности существующих средств, например, по использованию различных типов входящих данных для оценки. Известный инструментарий не дает возможности применения для анализа и оценки рисков широкого спектра начальных параметров. На основе предложенного автором метода анализа и оценки рисков, который на основе использования модели интегрированного представления параметров риска, позволяет проводить оценивание в детерминированных условиях, с использованием десяти параметров, которые могут быть представлены, как в числовой, так и лингвистической форме, было реализовано программную систему анализа и оценки рисков потери информационных ресурсов. Для верификации разработанного программного продукта было смоделировано несколько различных ситуаций относительно защищенности информационных ресурсов, после чего проведен анализ и оценивание рисков при каждой такой ситуации. Полученные результаты исследования подтверждают адекватность реагирования программного средства на изменение значений оценочных компонент при разных условиях среды оценивания, а значение риска существенно не изменяется при изменении базиса оценочных компонент.
Ключевые слова: *риск, анализ риска, оценка риска, система анализа и оценки риска, параметры риска, безопасность информационных ресурсов.*

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.

На сегодняшний день решать такую задачу целесообразно с помощью комплексного подхода к обеспечению информационной безопасности (ИБ) ИР. Одним из этапов построения комплексной системы защиты информации (КСЗИ) является разработка модели угроз [7], методология создания которой включает в себя анализ и оценивание рисков (АОР) [6]. На данный момент существует необходимость в эффективных средствах, которые позволили бы в автоматизированном режиме осуществлять АОР. Для решения такой задачи, используя методологию синтеза систем АОР потерь ИР [2], которая основана на логико-лингвистическом подходе, известных методах [3] и модели интегрированного представления параметров риска [1], было предложено новое соответствующее структурное решение системы оценивания [4]. Для практического при-

менения разработанного метода и структуры системы, необходимо решить актуальную задачу по разработке программного средства (ПС) АОР, которое даст возможность на практике осуществлять оценивание при различных исходных величинах, а также учитывать возможности эксперта относительно четкого детерминирования оцениваемых параметров.

В связи с этим, целью данной работы является разработка соответствующего инструментария для использования при АОР.

Достижение поставленной цели осуществим на основе разработанной структуры Det-AOP системы [4]. Соответствующее ПС основывается на разработках, которое в отличие от известных [5, 6] использует в качестве входных данных различные наборы оценочных параметров, что повышает гибкость, удобство использования, интеграцию возможностей и расширяет спектр функций инструментального средства, работающего в детерминированной среде. Для такой среды, в большей степени характерна определенность и стабильность и она достаточно устойчива к влиянию разнообразных возмущений во времени.

Представленный программный продукт был реализован на основе методологии синтеза систем АОР потерь ИР [2], согласно которой на первом этапе необходимо осуществить выбор метода АОР. Далее согласно методологии, для идентификации ИР, а также действий и событий нарушения ИБ, осуществляется формирование соответствующих баз данных (БД):

– действий A_a ($a=\overline{1,n}$), составленной на основе перечня угроз из ISO / IEC 27002:2005 [8];

– информационных ресурсов IIP_h, содержащей в себе список ресурсов согласно метода CRAMM для профиля Commercial;

– оценочных компонент $ek_i^{A_a}$ (ОК).

Для удобства и последующего использования полученных результатов в ПС все данные сохраняются в проектах пользователей (ПП), которые в свою очередь собраны в БД. Отметим, что здесь в качестве входных данных выступают:

$$ИР \in \{ИР_h\}\ (h=\overline{1,20});$$

$$A \in \{A_a\}\ (a=\overline{1,60});$$

$$E \in \{E_e\}\ (e=\overline{1,7}),$$

а значение $ek_i^{A_a} : \{ek_i^A\} = \{ek_P^{A_a}, ek_F^{A_a}, ek_L^{A_a}, ek_D^{A_a}\}$, где $i=\overline{1,4}$. Идентификаторы IIP_h и A_a принимают текстовые значения соответствующие наименованиям из указанных перечней.

Для последующего оценивания степени риска (СР), отображаемого параметром *DR*, согласно методологии [2], осуществляется формирование эталонных значений СР. В предложенном ПС диапазон числовых значений для степени риска лежит в приделах от 0 до 100. В лингвистической форме *DR* может отображаться следующими значениями:

– «Незначительный риск нарушения ИБ» (*НР*);

– «СР нарушения ИБ низкая» (*РН*);

– «СР нарушения ИБ средняя» (*РС*);

– «СР нарушения ИБ высокая» (*РВ*);

– «Предельный риск нарушения ИБ» (*ПР*).

Для определения соответствия (лингвистическое распознавание) полученного числового значения СР $dr^{(A_a)}$ лингвистическому, применяется формула (1):

$$T_{DR} = \begin{cases} НР,\ при\ dr^{(A_a)} \in [\,dr_{\min};\, dr_1[\\ РН,\ при\ dr^{(A_a)} \in [\,dr_2;\, dr_3[\\ РС,\ при\ dr^{(A_a)} \in [\,dr_4;\, dr_5[\\ РВ,\ при\ dr^{(A_a)} \in [\,dr_6;\, dr_7[\\ ПР,\ при\ dr^{(A_a)} \in [dr_8;\, dr_{\max}\,] \end{cases}, \qquad (1)$$

где $[dr_{min};\ dr_1[$, $[dr_2;\ dr_3[$, $[dr_4;\ dr_5[$, $[dr_6;\ dr_7[$, $[dr_8;\ dr_{max}]$, например, будут соответствовать значения [0; 20[, [20; 40[, [40; 60[, [60; 80[, [80; 100]. Формирование эталонных значений для ОК в ПС было реализовано в следующем виде:

– *P* (принимает значение в диапазоне от 0 до 100, шаг дискретизации – 1);

– *F* (находится в диапазоне от 0 до 1, шаг дискретизации – 0,01);

– *L* (лежит в пределах от 0 до 0,5, шаг дискретизации – 0,01);

– *D* (принимает значения от 0 до 10, шаг дискретизации – 1).

На этапах формирования уровня значимости и определения текущего значения ОК в ПС для ввода данных используется интерактивный интерфейс, который представлен на рис. 1 (верхнее окно).

Классификация текущих значений и оценка СР в ПС осуществляется в автоматизированном режиме. При этом, для каждого действия (угрозы) реализуется расчет значения $dr^{(A_a)}$ по выражению

$$dr^{(A_a)} = \sum_{j=1}^{m}\left(dr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(A_a)} \right),$$

где

$$dr_j = 90\text{-}20(j\text{-}1),$$

$$\lambda_{ij}^{(A_a)} = \begin{cases} 1, \textit{ при } ek_i^{A_a} \in [\, k_{EK_i}(j-1);\, k_{EK_i} j\,[\\ 0, \textit{ при } ek_i^{A_a} \notin [\, k_{EK_i}(j-1);\, k_{EK_i} j\,[\end{cases} \quad (a = \overline{1,n}),$$

$$LS_i = \frac{2(g-i+1)}{(g-1)g} \ (i = \overline{1,g}) \text{ или } LS_i = 1/g \ \ (j = \overline{1,m}).$$

Для ИР значение $dr^{(cp)}$ вычисляется на основе выражения

$$dr^{(cp)} = (\sum_{a=1}^{m} dr^{(A_a)}) / m.$$

Полученные результаты имеют соответствующую интерпретацию, а ПС генерирует необходимый отчет.

Для тестирования основных функций и отражения принципа работы ПС АОР проводится его верификация, которая осуществляется на компьютере под управлением операционной системы Microsoft Windows 7 Home Premium x64. Разработанное приложение для своей работы не требует дополнительных библиотек и системных файлов, поскольку при компиляции проекта были указаны следующие опции: Use dynamic RTL = false; Build with runtime packages = false. Также дополнительно для функционирования БД был установлен сервер MySQL 5.1.60 x64. С помощью разработанного ПС создан тестовый проект «test24», а в качестве IIP_1 для верификации выбран «сетевой файл-сервер» из категории «Сетевые серверы». Тестирование проводилось при четко определенных исходных данных, т.е. в так называемой детерминированной среде.

Для данного ИР были установлены следующие A_a ($a = \overline{1,3}$):

A_1=«Злоупотребление средствами обработки информации» (из категории «Нецелевое использование компьютерного оборудования и сети Интернет сотрудниками организации»);

A_2=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика» (из категории «Угрозы утечки конфиденциальной информации»);

A_3=«Повреждение носителей информации» (из категории «Угрозы доступности IT-сервисов и разрушения (потери) информационных активов»).

После этого по каждой угрозе осуществляются расчеты значений $dr^{(A_a)}$, результаты которых также представлены в табл. 1, из которой видно, что значение степени риска для данного ИР по всем угрозам низкое.

Таблица 1

Результаты оценивания

A_a	P	F	L	D	$dr^{(A_a)}$	T_{DR}
A_1	42	0,67	0,05	1	35	*PH*
A_2	25	0,13	0,31	4	35	*PH*
A_3	33	0,07	0,17	3	25	*PH*

Далее производится расчет среднего значения $dr^{(cp)}$ для данного ИР, в результате чего получаем $dr^{(cp)} = 31{,}67$, что соответствует T_{DR} – *PH* (см. выражение (1)).

Дальнейшая верификация ПС выполнялась на основе моделирования для нескольких состояний среды оценивания:

1-е состояние – начальные условия с установленным количеством угроз для ИР;

2-е состояние – изменено количество угроз для ИР;

3-е состояние – блокировано одну угрозу для ИР;

4-е состояние – изменение значений оценочных компонент (уменьшение или увеличение).

1-е состояние с начальными условиями, а также результаты вычисления СР, приведены в табл.1. Рассмотрим результаты моделирования для следующих состояний.

2-е состояние

К ПП были внесены изменения, путем введения дополнительного A_4 для IIP_1=«Сетевой файл-сервер», т.е. A_4=«Нелегальное использование программного обеспечения», которое входит в категорию «Юридические угрозы».

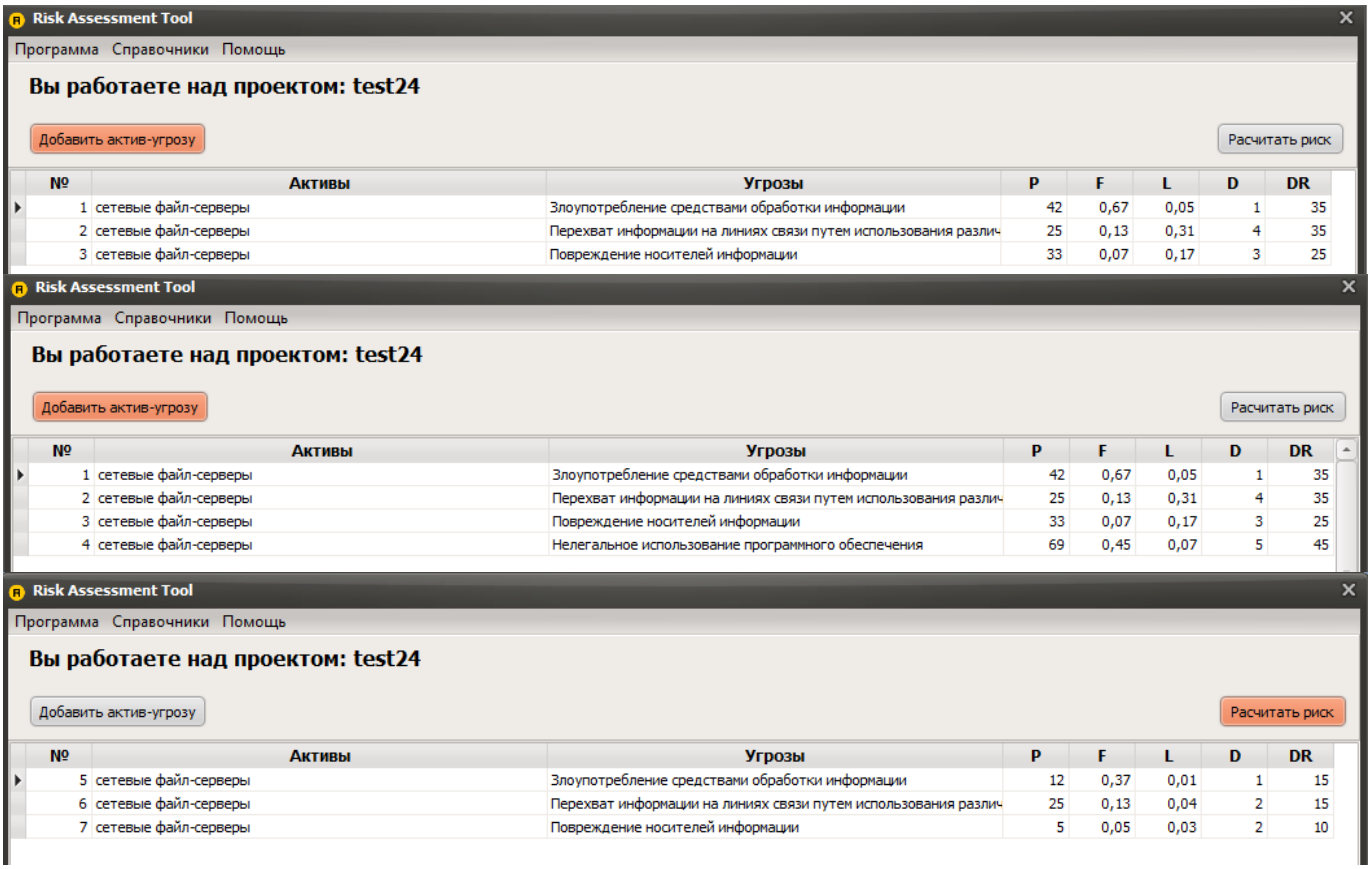


Рис. 1. Интерактивный интерфейс ПС АОР

В табл. 2 приведены значения $ek_i^{A_a}$, которые были определены по оценкам экспертов. В результате этого осуществлен расчет значения СР для A_4 т.е. $dr^{(A_a)}$=45 (см. рис. 1 центральное окно), а среднее $dr^{(cp)}$ после интегрирования с A_4 составило $dr^{(cp)}$ = 35, что соответствует значению T_{DR} – *PH*.

Таблица 2

Значение $ek_i^{A_a}$

A_a	*P*	*F*	*L*	*D*
A_1	42	0,67	0,05	1
A_2	25	0,13	0,31	4
A_3	33	0,07	0,17	3
A_4	69	0,45	0,07	5

3-е состояние

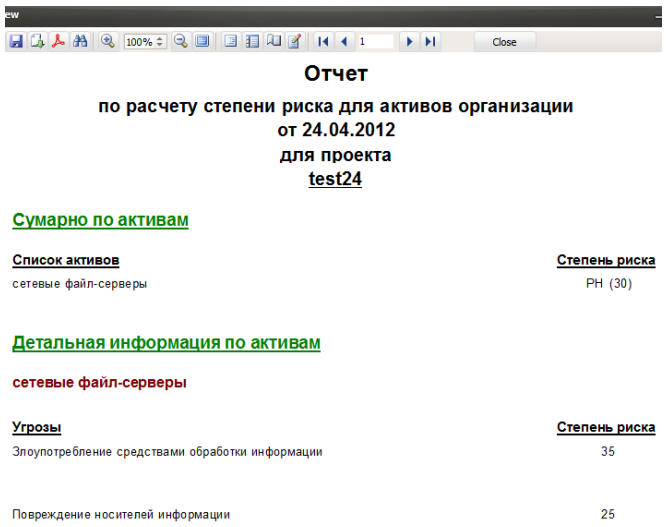
Далее было проведено моделирование в условиях, когда на оцениваемом объекте защиты проведены мероприятия по устранению A_2=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика». Здесь также выполнено повторное измерение $dr^{(A_a)}$ и $dr^{(cp)}$. Используя разработанную систему, с учетом моделируемой ситуации, полученное значение $dr^{(cp)}$ для IIP_1 уменьшилось до 30, т.е. $dr^{(cp)}$ (T_{DR})= 30 (РН). Это можно увидеть из сформированного разработанным инструментальным средством отчета, представленного на рис. 2. Здесь значение $dr^{(cp)}$ меняется при изменении количества A_a, а СР нарушения ИБ во всех случаях, определяется как низкая. Дальнейшее экспериментальное исследование показало, что при значительном увеличении или уменьшении числа A_a значение $dr^{(cp)}$ может соответственно адекватно измениться.

4-е состояние

После выполненных расчетов, согласно 1-го состояния, было проведено моделирование для двух ситуаций:

– первая (на объекте защиты учтены предыдущие результаты АОР и внедрены меры для минимизации рисков);

– вторая (на объекте защиты не учтены предыдущие результаты АОР – не приняты решения по внедрению мер для снижения рисков).



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 (30)

Детальная информация по активам

сетевые файл-серверы

Угрозы	Степень риска
Злоупотребление средствами обработки информации	35
Повреждение носителей информации	25

Рис. 2. Сгенерированный отчет ПС АОР

С учетом первой ситуации, на объекте защиты, был проведен ряд мероприятий, направленных на уменьшение уровня угроз для заданного ИР, а именно:

– внедрена система разграничения доступа, пользователям предоставлены права и привилегии в соответствии с их должностными обязанностями для минимизации A_1 = «Злоупотребление средствами обработки информации»;

– разработана система шифрования сетевого трафика для устранения A_2=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика»;

– реализованы системы мониторинга состояния жестких дисков, настроена политика регулярного создания резервных копий критической информации, внедрены технологии RAID 1 для нейтрализации A_3=«Повреждение носителей информации».

После повторной реализации АОР экспертами были установлены величины оценочных компонент, значения которых приведены в табл. 3.

Результаты проведенных изменений в проекте имеют вид, показанный на рис. 1 (нижнее окно).

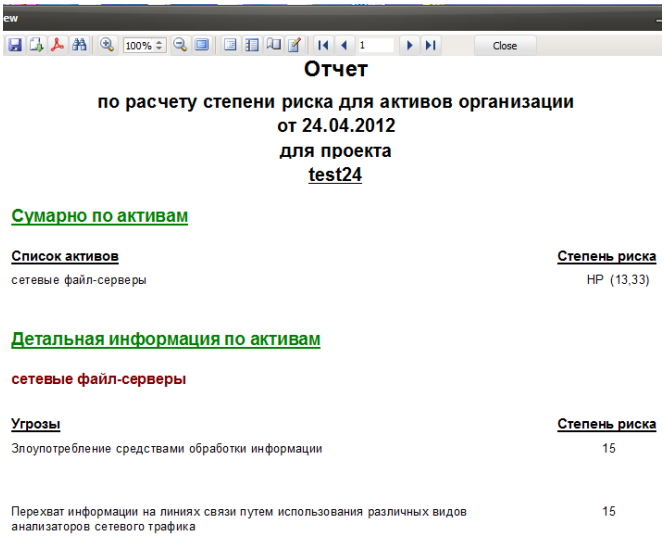
Для каждой A_a был повторно осуществлен расчет значений $dr^{(A_a)}$, результаты которого отображены в табл. 3.

Таблица 3

Значение оценочных компонент и $dr^{(A_a)}$

A_a	P	F	L	D	$dr^{(A_a)}$	T_{DR}
A_1	12	0,37	0,01	1	15	НР
A_2	25	0,13	0,04	2	15	НР
A_3	5	0,05	0,03	2	10	НР

Как видно для каждой A_a значение $dr^{(A_a)}$ интерпретируется на уровне «Незначительный риск нарушения ИБ». Очевидно, для IIP_1 величина $dr^{(cp)}$ =13,33, что соответствует ЛП – *НР* (рис. 3).



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	НР (13,33)

Детальная информация по активам

сетевые файл-серверы

Угрозы	Степень риска
Злоупотребление средствами обработки информации	15
Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика	15

Рис. 3. Результаты оценки $dr^{(A_a)}$

Из приведенного отчета (рис. 3) прослеживается существенное уменьшение значений $dr^{(A_a)}$, что позволяет, в свою очередь, сделать вывод об адекватности работы ПС АОР при изменении условий среды оценивания.

С учетом второй ситуации, осуществляется моделирование, при котором на объекте защиты не учтены предыдущие результаты АОР. После первичной реализации АОР, не приняты во внимание полученные результаты и не внедрены меры по обеспечению ИБ. В результате этого, после повторного АОР ситуация с выбранным IIP_1 ухудшилась, о чем свидетельствуют проставленные экспертами значения оценочных компонентов (табл. 4). Как видно из табл. 4, величины $dr^{(A_a)}$ по каждой A_a существенно увеличились, а для двух угроз значение «*РН*» изменилось на «*РС*» (средняя степень риска нарушения ИБ). Для IIP_1 значение $dr^{(cp)}$ =43,33, что в свою очередь соответствует, согласно выражению (1), величине T_{DR}=«*РС*». Это свидетельствует о негативных тенденциях относительно ИБ для объекта защиты (по сравнению со значением $dr^{(cp)}$ =31,67, T_{DR}=«РН» в первичном АОР).

Также с учетом первой и второй ситуации был произведен АОР для дополнительных трех ИР. В табл. 5 и на рис. 4 показаны значения $dr^{(cp)}$ для этих ИР.

Таблица 4

Результаты оценивания

A_a	P	F	L	D	$dr^{(A_a)}$	T_{DR}
A_1	52	0,81	0,05	1	40	PH
A_2	45	0,23	0,31	4	45	PC
A_3	43	0,47	0,27	3	45	PC

Сравнивая полученные результаты, можно сделать вывод, что при изменении значений оценочных компонент разработанное ПС АОР адекватно реагирует на соответствующие условия среды оценивания.

Таблица 5

Значение $dr^{(cp)}$

IIP	$dr^{(cp)}$		
	Средний уровень риска (начальные условия)	**Пониженный уровень риска**	**Повышенный уровень риска**
$ИР_1$	31,67 (PH)	13,33 (HP)	43,33 (PC)
$ИР_2$	20 (HP)	15 (HP)	26,5 (PH)
$ИР_3$	28,33 (PH)	23,33 (PH)	30 (PH)
$ИР_4$	28,33 (PH)	22,5 (PH)	31,25 (PH)

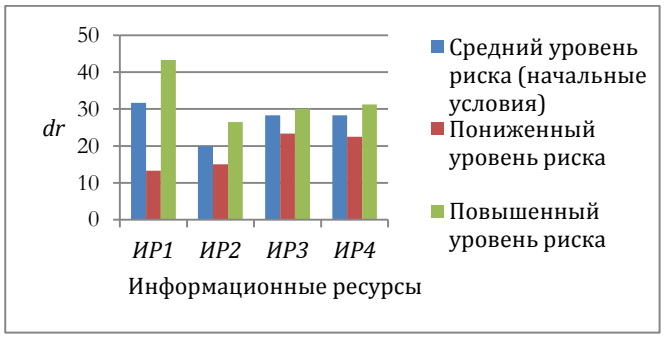


Рис. 4 Гистограмма средних значений степени риска

По аналогии с предыдущими экспериментами были проведены дополнительные исследования для других A_a, результаты которых занесены в соответствующие табл. 6-8.

В табл. 6 используются следующие сокращения, ССО – состояние среды окружения, для которой позиции 1 и 5 отображают начальные условия, 2 и 6 – изменение количества угроз заданным ИР, 3 и 8 – изменение значений оценочных компонент (3 и 7 – уменьшение значений оценочных компонент; 4 и 8 – увеличение значений оценочных компонент), а ОК – оценочные компоненты.

Приведем результаты еще нескольких экспериментов. Для подтверждения гипотезы относительно использованного базиса оценочных компонент осуществим АОР при различных наборах оценочных компонент (рис. 5).

Таблица 6

Результаты оценивания

ССО	ОК	A_1	A_2	A_3	A_4	$dr^{(cp)}$ (T_{DR})
1	**P**	30	41	12	-	-
	F	0,15	0,36	0,17	-	-
	L	0,12	0,01	0,05	-	-
	D	2	2	3	-	-
	$dr^{(A_a)}$ (T_{DR})	20 (HP)	25 (PH)	15 (HP)	-	20 (HP)
2	**P**	30	41	12	16	-
	F	0,15	0,36	0,17	0,23	-
	L	0,12	0,01	0,05	0,17	-
	D	2	2	3	5	-
	$dr^{(A_a)}$ (T_{DR})	20 (HP)	25 (PH)	15 (HP)	30 (PH)	22,5 (PH)
3	**P**	23	23	9	-	**-**
	F	0,07	0,3	0,06	-	**-**
	L	0,03	0,01	0,05	-	**-**
	D	2	1	1	-	**-**
	$dr^{(A_a)}$ (T_{DR})	15 (HP)	20 (HP)	10 (HP)	-	15 (HP)
4	**P**	36	47	23	-	-
	F	0,15	0,39	0,21	-	-
	L	0,16	0,08	0,08	-	-
	D	2	5	4	-	-
	$dr^{(A_a)}$ (T_{DR})	20 (HP)	35 (PH)	25 (PH)	-	26,67 (PH)
5	**P**	32	23	47	-	
	F	0,21	0,12	0,2	-	
	L	0,3	0,03	0,06	-	
	D	4	2	3	-	
	$dr^{(A_a)}$ (T_{DR})	40 (PH)	15 (HP)	30 (PH)	-	28,33 (PH)
6	**P**	32	23	47	41	-
	F	0,21	0,12	0,2	0,33	-
	L	0,3	0,03	0,06	0,1	-
	D	4	2	3	5	-
	$dr^{(A_a)}$ (T_{DR})	40 (PH)	15 (HP)	30 (PH)	40 (PH)	31,25 (PH)
7	**P**	26	17	22	-	-
	F	0,16	0,12	0,2	-	-
	L	0, 3	0,01	0,03	-	-
	D	3	1	3	-	-
	$dr^{(A_a)}$ (T_{DR})	35 (PH)	10 (HP)	25 (PH)	-	23,33 (PH)
8	**P**	38	31	52	-	-
	F	0,27	0,16	0,25	-	-
	L	0,33	0,04	0,12	-	-
	D	4	2	4	-	-
	$dr^{(A_a)}$ (T_{DR})	40 (PH)	15 (HP)	35 (PH)	-	30 (PH)

Полученные результаты исследования подтверждают, что ПС АОР адекватно реагирует на изменение значений оценочных компонент при различных условиях среды оценивания, а значение риска существенно не изменяется при смене базиса оценочных компонент.

Таблица 7

Значения A_3

ОК	A_3	
P	12	47
F	0,17	0,2
L	0,05	0,06
D	3	3

Таблица 8

Значения $dr^{(A_a)}$

A_a	$dr^{(A_a)}(T_{DR})$	
A_1	20 (*HP*)	40 (*PH*)
A_2	25 (*PH*)	15 (*HP*)
$dr^{(cp)}(T_{DR})$	22,5 (*PH*)	27,5 (*PH*)

Отчет

по расчету степени риска для активов организации
от 22.06.2012
для проекта
Zero_Condition

Сумарно по активам

Список активов	Степень риска
несетевые серверы общего назначения	HP - 16

Детальная информация по активам

несетевые серверы общего назначения

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.	10
Кража или повреждение компьютерного оборудования и носителей информации инсайдерами	10
Кража или повреждение компьютерного оборудования и носителей информации внешними злоумышленниками	15
Постороннее лицо может получить физический доступ к комплексу средств защиты с целью переконфигурирования либо создания возможности обхода средств защиты	20
Кража бумажных документов инсайдерами	25

Лингвистическое распознавание

Степень риска	Сокращение
Незначительный риск нарушения ИБ	НР
Степень риска нарушения ИБ низкая	РН
Степень риска нарушения ИБ средняя	РС
Степень риска нарушения ИБ высокая	РВ
Предельный риск нарушения ИБ	ПР

Рис. 5 Пример отчета ПС при выборе одного оценочного компонента

Данный подход был использован для формирования модели угроз при построении КСЗИ в Национальном авиационном университете, а также предложенное ПС было внедрено в учебный процесс кафедры безопасности информационных технологий.

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. Методология 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] Корченко А.Г. Системы анализа и оценки риска потерь государственных информационных ресурсов / Корченко А.Г., Волянская В.В., Казмирчук С.В., Охрименко А.А. // Защита информации – 2012. – №2. – С. 52-58.

[5] 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.

[6] 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.

[7] 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.

[8] ISO/IEC 27002:2005 Информационные технологии. Свод правил по управлению защитой информации с учетом Технической поправки 1, опубликованной 2007-07-01.

REFERENCES

[1] Korchenko A.G. Integrated view of risk characteristic / Korchenko A.G., Ivanchenko Ye.V., Kazmirchuk S.V. // Zahist ìnformacìï, 2011, №1 (50), pp. 96 – 101.

[2] Korchenko A.G. The synthesis methodology of analysis systems and risk assessment of information resources losses / Korchenko A.G., Kazmirchuk S.V. // Zahist ìnformacìï , 2012, №2, pp. 24 – 28.

[3] Korchenko A.G. Risk analysis and assessment methods of government information resources losses / Korchenko A.G., Sherbina V.P., Kazmirchuk S.V. // Zahist ìnformacìï, 2012, №1, pp. 126-139.

[4] Korchenko A.G. Systems analysis and risk assessment of Government Information Resources losses / Korchenko A.G., Volyanskaya V.V., Kazmirchuk S.V., Okhrimenko A.A. // Zahist ìnformacìï, 2012, №2, pp. 52-58.

[5] Lutskiy M.G. Research of information security risk & analysis assessment software / Lutskiy M.G., Korchenko A.G., Ivanchenko Ye.V., Kazmirchuk S.V. // Zahist ìnformacìï, 2011, №3, pp. 97-108.

[6] Lutskiy M.G. Modern techniques of Information Risk Management / Lutskiy M.G., Ivanchenko E.V.,

Korchenko A.G., Kazmirchuk S.V., Okhrimenko A.A. // Zahist ìnformacìï , 2011, №1, pp. 5-16.
[7] ND TZÍ 1.4-001-2000 Typical regulations on data protection agencies in the automated system.
[8] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management.

АНАЛІЗ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Для побудови систем менеджменту інформаційної безпеки, комплексних систем захисту інформації та інших систем безпеки необхідно проводити аналіз і оцінювання ризиків. Існуючі засоби оцінки в переважній своїй більшості засновані на статистичних підходах. У багатьох країнах, як на рівні підприємств, так і на державному рівні подібна статистика не ведеться. Це обмежує можливості існуючих засобів, наприклад, щодо використання різних типів вхідних даних для оцінки. Відомий інструментарій не дає можливості застосування для аналізу та оцінки ризиків широкого спектру початкових параметрів. На базі запропонованого автором методу аналізу та оцінки ризиків, який на основі використання моделі інтегрованого представлення параметрів ризику, дозволяє проводити оцінювання в детермінованих умовах, з використанням десяти параметрів, які можуть бути представлені, як в числовий, так і лінгвістичній формі, було реалізовано програмну систему аналізу та оцінки ризиків втрати інформаційних ресурсів. Для верифікації розробленого програмного продукту було змодельовано кілька різних ситуацій щодо захищеності інформаційних ресурсів. Отримані результати дослідження підтверджують адекватність реагування програмного засобу на зміну значень оціночних компонент при різних умовах середовища оцінювання, а значення ризику істотно не змінюється при зміні базису оціночних компонентів.

Ключові слова: ризик, аналіз ризику, оцінка ризику, система аналізу та оцінки ризику, параметри ризику, безпека інформаційних ресурсів.

RISK ANALYSIS AND ASSESSMENT OF INFORMATION RESOURCES

Abstract. The construction of information security management system (ISMS), complex system of information security and other security systems require carrying out the analysis and security risk assessment. The existing assessment tools in its majority are based on statistical approaches. In many countries, both at the enterprise level and at the State level such statistics is not conducted. This limits the ability of existing tools, such as the use of different input data types for assessment. A known tool gives no the administration opportunity for risks analysis and risk assessment of a wide range of initial parameters. On t he basis of the proposed risk analysis and assessment method, which based on the use of the integrated model representation of the risk parameters allow to conduct an assessment in the deterministic and fuzzy conditions using ten parameters, which can be represented as numeric and linguistic form, it was implemented the software system of risk analysis and assessment of information resources losses. To verify the developed software product there were designed various situations connected with the information security resources. The received results confirm the adequacy of software response on value changes of estimated component under different environment conditions, while the risk value does not change significantly when the basis of estimated components is changed.

Index Terms: risk, risk analysis, risk assessment, information security risk analysis and assessment method, risk management, risk parameters.

Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: sv902@mail.ru
Казмирчук Светлана Владимировна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Svitlana Kazmirchuk PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).