[3]. M.A. Ivanov, I.V. Chugunkov The the theory application and evaluation a generator for pseudo sequences. M.: Cudits-Obraz, 2003, 240 p.
[4]. F.R. Gantmaher Matrix Theory., M.: Fizmathlit, 2004, 560 p.
[5]. A.Ja. Beletsky, A.A. Beletsky, E.A. Beletsky. Transformations Gray. Monography in 2 vols. V. Fundamentals of the theory - Kiev: Book publisher NAU, 2007, 412 p.
[6]. A.Ja. Beletsky, A.A. Beletsky. Synthesis of primitive matrices of finite Galois fields and their application. Information technology in education, Kherson: KSU, 2012, pp. 23-43.
[7]. A.Ja. Beletsky. Primitive matrices over prime Galois fields. // The information processing system. – Khar-kov. HUVS, 2012, № 3, pp. 218-219.

КРИПТОГРАФІЧНІ ЗАСТОСУВАННЯ УЗАГАЛЬНЕНИХ МАТРИЦЬ ГАЛУА І ФІБОНАЧЧІ

Формування псевдовипадкових послідовностей двійкових чисел становить актуальну проблему, яка вирішується в криптографії. Найбільш поширений метод генерації ПСП заснований на лінійних регістрах зсуву максимального порядку з лінійними зворотними зв'язками, однозначно описуваних класичними матрицями Галуа і Фібоначчі. У роботі розглянуті питання синтезу узагальнених примітивних матриць Галуа і Фібоначчі (а також їх сполучених варіантів) довільного порядку *n* над простим полем Галуа характеристики *p*. Синтез матриць базується на використанні незвідних поліномів *fn* ступеня *n* характеристики *p* і примітивних елементів розширеного поля Галуа, породжуваного поліномом *fn*. Обговорюється перспектива застосування таких матриць при побудові узагальнених генераторів псевдовипадкових послідовностей *p*-ічних чисел. Розроблено оператори перетворення будь-який з узагальнених матриць в усі інші. Запропоновано стилізоване подання зворотних зв'язків у ЛРС-генераторах псевдовипадкових послідовностей.
Ключові слова: незвідні поліноми, примітивні матриці, примітивні елементи поля Галуа.

CRIPTOGRAFY APPLICATIONS OF PRIMITIVE MATRICES GALOIS AND FIBONACCI

Formation of pseudo-random sequences of binary numbers is the actual problem being solved in cryptography. The most common method of generating pseudo-random sequences is based on linear shift registers of maximal order linear feedback is uniquely described by the classical Galois and Fibonacci matrices. The paper deals with the synthesis of generalized primitive matrices Galois and Fibonacci (and their dual versions) of any order n over Galois prime field of characteristic p. Synthesis of matrices based on the use of irreducible polynomials of degree n fn characteristic p and primitive elements of the extended Galois field generated by the polynomial fn. We discuss the prospects of using such matrices in the construction of pseudorandom sequence of generalized p-ary numbers. Developed conversion operators of any generalized matrix of all the others. Proposed stylized representation of feedbacks in the LSR-generators of pseudo-random sequences.
Keywords: irreducible polynomials, primitive ma-trices, primitive elements of the field Galois.

Білецький Олександр Анатолійович, молодший науковий співробітник кафедри електроніки, Національний авіаційний університет.
E-mail: alexander.beletsky@gmail.com
Белецкий Александр Анатольевич, младший научный сотрудник кафедры электроники, Национальный авиационный университет.
Beletsky Alexsander, Junior Research Fellow Department of Electronics, National Aviation University.

УДК 004.056.5(045)

АНАЛИЗ И ОЦЕНИВАНИЕ РИСКОВ ИНФОРМАЦИОННЫХ РЕСУРСОВ В НЕЧЕТКИХ УСЛОВИЯХ

Светлана Казмирчук

Для построения систем управления информационной безопасности необходимо проводить анализ и оценивание рисков, которые часто характеризуются высокой неопределенностью. Существующие средства оценки не дают возможности применения для анализа и оценивания рисков широкого спектра начальных параметров. На основе предложенного автором метода анализа и оценивания рисков потери информационных ресурсов, было реализовано соответствующую программную систему. Она позволяет проводить оценивание в нечетких условиях с использованием установленного базиса оценочных компонент, которые отображаются моделью интегрированного представления параметров риска и могут быть представлены, как в числовой, так и лингвистической форме. Для верификации разработанного програ-

ммного продукта было осуществлено моделирование при нескольких различных условиях среды оценивания относительно защищенности информационных ресурсов. Полученные результаты исследования под-тверждают то, что программное средство адекватно реагирует на изменения условий среды оценивания, которая отображается значениями оценочных компонент. Исследования показали, что значение риска существенно не изменяется при изменении базиса оценочных компонент.

***Ключевые слова**: риск, анализ риска, оценка риска, система анализа и оценки риска, параметры риска, метод.*

Для построения систем управления информационной безопасности (ИБ) необходимо проводить анализ и оценивания рисков (АОР), которые часто характеризуются высокой неопределенностью.

Для решения этой проблемы, на основании методологии синтеза систем АОР потерь информационных ресурсов (ИР) [2], которая основана на логико-лингвистическом подходе, известных методах [3] и модели интегрированного представления параметров риска (ИППР) [1] было предложено новое структурное решение системы АОР [4]. Для применения на практике разработанного метода и структурной схемы, была решена актуальная задача по разработке соответствующего программного обеспечения (ПО), которое позволило проводить оценивание при различном базисе исходных величинах с учетом неуверенности эксперта в своих суждениях.

В связи с этим, целью работы было создание и верификация средства оценивания, которое даст возможность проводить АОР на основе выбранного базиса параметров в нечеткой, слабоформализованной среде. Она характеризуется большой степенью неопределенности, случайности, нестабильности, влиянием разнообразных возмущений во времени и т.п., а для формализации ее процессов используется математический аппарат теории нечетких множеств.

Для достижения поставленной цели было разработано ПО, которое основывалось на предложенном в [4] структурном решении Fuz-АОР системы. Представленное ПО, в отличие от известных [5, 6], использует в качестве входных данных различные базисы (наборы) оценочных параметров, отражаемые моделью ИППР [1], что повышает гибкость, удобство использования и расширяет возможности спроектированного средства АОР, позволяющего функционировать в зоне неуверенности, т.е. когда эксперт сомневается в однозначности своих приоритетов.

За основу разработки ПО АОР была взята методология синтеза [2], согласно которой на первом этапе необходимо осуществить выбор метода АОР. Далее, для идентификации ИР, 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 $ИР_h$, содержащей в себе список ресурсов согласно метода CRAMM для профиля Commercial; оценочных компонент $ek_i^{A_a}$ (ОК).

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 $ИР_h$ и A_a принимают текстовые значения соответствующие наименованиям из указанных перечней.

Для последующей оценки степени риска (СР), согласно методологии [2] осуществляется определение лингвистической переменной (ЛП) «СТЕПЕНЬ РИСКА» (*DR*), соответствующей кортежу [2] <*DR*, T_{DR}, X_{DR}>, для чего задается ее базовое терм-множество $T_{DR} = \bigcup_{j=1}^{m} T_{DR_j}$ $(j=\overline{1,m}$, где m – количество термов), если для *DR* их m, то количество интервалов будет G=2m-1, с общим видом $[b_{11}; b_{21}[$, $[b_{21}; b_{12}[$, $[b_{12}; b_{22}[$, …, $[b_{2j-1}; b_{1j}[$, $[b_{1j}; b_{2j}[$, …, $[b_{2m-1}; b_{1m}[$, $[b_{1m}; b_{2m}]$ $(j=\overline{1,m})$ и функциями принадлежности (ФП) μj(dr). T_{DR1},…, T_{DRj},…, T_{DRm} представляются трапециевидными нечеткими числами (НЧ) с ФП соответственно $\mu_1(dr)$, …, $\mu_j(dr)$, …, $\mu_m(dr)$, которые вычисляются по выражению (1) [3]:

$$\mu_j(dr)=\begin{cases} L\left(\dfrac{b_{1j}-dr}{b_{1j}-a_j}\right), & dr\in[a_j,b_{1j}]; \\ 1, & dr\in[b_{1j},b_{2j}]; \\ R\left(\dfrac{dr-b_{2j}}{c_j-b_{2j}}\right), & dr\in[b_{2j},c_j], \end{cases} \qquad (1)$$

где $a_j < b_{1j} \le b_{2j} < c_j$, при $j=\overline{1,m}$, $\{a_1 \ldots c_m\}=\{\varnothing\}$, а *L(dr)*, *R(dr)* – функции (невозрастающие на множестве не положительных чисел), которые удовлетворяют свойствам: *L(-dr)=L(dr)*, *R(-dr) = R(dr)*, *L(0) = R(0)* = 1. Например, при m=5 –

$\bigcup_{j=1}^{5} T_{DR_j}$ = {«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*)}, тогда G=9, а интервалам

$$[b_{11};\ b_{21}[,\ [b_{21};\ b_{12}[,\ [b_{12};\ b_{22}[,\ [b_{22};\ b_{13}[,\ [b_{13};\ b_{23}[,\ [b_{23};\ b_{14}[,\ [b_{14};\ b_{24}[,\ [b_{24};\ b_{15}[,\ [b_{15};\ b_{25}]$$

с учетом (1), соответствуют

$$[b_{11};\ b_{21}[,\ [a_2,\ c_1[,\ [b_{12};\ b_{22}[,\ [a_3;\ c_2[,\ [b_{13};\ b_{23}[,\ [a_4;\ c_3[,\ [b_{14};\ b_{24}[,\ [a_5;\ c_4[,\ [b_{15};\ b_{25}],$$

а конкретные данные (интервалы значений и ФП заданных термов), для примера, занесены в табл. 1.

Таблица 1

Пример значений интервалов и $\mu_i(dr)$

Интервалы	**Термы**	$\mu_i(dr)$
$[b_{11};\ b_{21}[$=[0; 10[	T_{DR1}	1
$[b_{21};\ b_{12}[$=[10; 20[	T_{DR1}	$\mu_1(dr)$=(20-dr)/10
	T_{DR2}	$\mu_2(dr)$=1-$\mu_1(dr)$
$[b_{12};\ b_{22}[$=[20; 30[	T_{DR2}	1
$[b_{22};\ b_{13}[$=[30; 40[	T_{DR2}	$\mu_2(dr)$=(40-dr)/10
	T_{DR3}	$\mu_3(dr)$=1-$\mu_2(dr)$
$[b_{13};\ b_{23}[$=[40; 50[	T_{DR3}	1
$[b_{23};\ b_{14}[$=[50; 60[	T_{DR3}	$\mu_3(dr)$=(60-dr)/10
	T_{DR4}	$\mu_4(dr)$=1-$\mu_3(dr)$
$[b_{14};\ b_{24}[$=[60; 70[	T_{DR4}	1
$[b_{24};\ b_{15}[$=[70; 80[	T_{DR4}	$\mu_4(dr)$=(80-dr)/10
	T_{DR5}	$\mu_5(dr)$=1-$\mu_4(dr)$
$[b_{15};\ b_{25}]$=[80; 100]	T_{DR5}	1

Для лингвистического распознавания полученного числового значения СР $dr^{(A_a)}$ применяется формула (2) формирования структурированного параметра СР SP:

$$SP^{(A_a)} = \begin{cases} (dr^{(A_a)}; T_{DR_j})\ при\ \mu_j(dr) = 1, \\ (dr^{(A_a)}; T_{DR_j}(\mu_j(dr)); T_{DR_{j+1}}(\mu_{j+1}(dr))) \\ \qquad при\ \mu_j(dr), \mu_{j+1}(dr) \neq 1, \end{cases} \quad (2)$$

где $(dr^{(A_a)}; T_{DR_j})$ словесно интерпретируется, как – степень риска T_{DR_j} с числовым эквивалентом $dr^{(A_a)}$, а $(dr^{(A_a)};\ T_{DR_j}(\mu_j(dr)); T_{DR_{j+1}}(\mu_{j+1}(dr)))$, как – СР с числовым эквивалентом $dr^{(A_a)}$ граничит между T_{DR_j} и $T_{DR_{j+1}}$ с уверенностью эксперта по границе T_{DR_j} – $\mu_j(dr)$ и $T_{DR_{j+1}}$ – $\mu_{j+1}(dr)$.

На этапе формирование эталонных значений ОК в ПО формируется ЛП «УРОВЕНЬ ОЦЕНОЧНОГО КОМПОНЕНТА (УОК) EK_i» (K_{EK_i}), которая определяется кортежем [2] $< K_{EK_i},\ T_{K_{EK_i}},\ X_{EK_i} >$, где базовые терм-множества задаются m термами $T_{K_{EK_i}} = \bigcup_{j=1}^{m} T_{K_{EK_ij}}$, например, при m=5 (интервалы значений и ФП заданных термов) занесены в табл. 2.

Классификация текущих значений и оценка СР в ПО осуществляется в автоматизированном режиме. Для каждого действия (угрозы) рассчитывается 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

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

$$\lambda_{i1}^{(A_a)} = \begin{cases} 1\ при\ ek_i^{A_a} \in [bi_{11}, bi_{12}[\\ 0\ при\ ek_i^{A_a} \notin [bi_{11}, ci_1[\\ \mu_1(ek_i^{A_a})\ при\ ek_i^{A_a} \in [bi_{12}, ci_1[\end{cases},$$

$$\lambda_{im}^{(A_a)} = \begin{cases} \mu_m(ek_i^{A_a})\ при\ ek_i^{A_a} \in [ai_m, bi_{1m}[\\ 1\ при\ ek_i^{A_a} \in [bi_{1m}, bi_{2m}[\\ 0\ при\ ek_i^{A_a} \notin [ai_m, bi_{2m}[\end{cases},$$

$$\lambda_{ij}^{(A_a)} = \begin{cases} \mu_j(ek_i^{A_a})\ при\ ek_i^{A_a} \in [ai_j, bi_{1j}[\\ 1\ при\ ek_i^{A_a} \in [bi_{1j}, bi_{2j}[\\ \mu_j(ek_i^{A_a})\ при\ ek_i^{A_a} \in [bi_{2j}, ci_j[\\ 0\ при\ ek_i^{A_a} \notin [ai_j, ci_j[\end{cases},$$

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

Для ИР значение $dr^{(cp)}$ вычисляется на основе выражения $dr^{(cp)} = (\sum_{a=1}^{m} dr^{(A_a)})/m$.

Таблица 2

Пример значений интервалов и $\mu_j(ek_i^{A_a})$ ($i=\overline{1,4}$, $j=\overline{1,5}$)

Интервалы для EK_i				**Термы**	$\mu_j(ek_i^{A_a})$			
P	***F***	***L***	***D***	$T_{K\,EK_i j}$	$\mu_j(ek_1^{A_a})$	$\mu_j(ek_2^{A_a})$	$\mu_j(ek_3^{A_a})$	$\mu_j(ek_4^{A_a})$
[0;10[	[0;0,1[	[0;0,1[	[0;1[	$T_{K\,EK_i 1}$	$\mu_1(ek_1^{A_a})=1$	$\mu_1(ek_2^{A_a})=1$	$\mu_1(ek_3^{A_a})=1$	$\mu_1(ek_4^{A_a})=1$
[10;20[	[0,1;0,2[	[0,1;0,15[	[1;2[	$T_{K\,EK_i 1}$	$\mu_1(ek_1^{A_a})=(20-ek_1^{A_a})/10$	$\mu_1(ek_2^{A_a})=(0,2-ek_2^{A_a})*10$	$\mu_1(ek_3^{A_a})=(0,15-ek_3^{A_a})*20$	$\mu_1(ek_4^{A_a})=(2-ek_4^{A_a})$
				$T_{K\,EK_i 2}$	$\mu_2(ek_1^{A_a})=1-\mu_1(ek_1^{A_a})$	$\mu_2(ek_2^{A_a})=1-\mu_1(ek_2^{A_a})$	$\mu_2(ek_3^{A_a})=1-\mu_1(ek_3^{A_a})$	$\mu_2(ek_4^{A_a})=1-\mu_1(ek_4^{A_a})$
[20;30[	[0,2;0,3[	[0,15;0,2[	[2;3[	$T_{K\,EK_i 2}$	$\mu_2(ek_1^{A_a})=1$	$\mu_2(ek_2^{A_a})=1$	$\mu_2(ek_3^{A_a})=1$	$\mu_2(ek_4^{A_a})=1$
[30;40[	[0,3;0,4[	[0,2;0,25[	[3;4[	$T_{K\,EK_i 2}$	$\mu_2(ek_1^{A_a})=(40-ek_1^{A_a})/10$	$\mu_2(ek_2^{A_a})=(0,4-ek_2^{A_a})*10$	$\mu_2(ek_3^{A_a})=(0,25-ek_3^{A_a})*20$	$\mu_2(ek_4^{A_a})=(4-ek_4^{A_a})$
				$T_{K\,EK_i 3}$	$\mu_3(ek_1^{A_a})=1-\mu_2(ek_1^{A_a})$	$\mu_3(ek_2^{A_a})=1-\mu_2(ek_2^{A_a})$	$\mu_3(ek_3^{A_a})=1-\mu_2(ek_3^{A_a})$	$\mu_3(ek_4^{A_a})=1-\mu_2(ek_4^{A_a})$
[40;50[	[0,4;0,5[	[0,25;0,3[	[4;5[	$T_{K\,EK_i 3}$	$\mu_3(ek_1^{A_a})=1$	$\mu_3(ek_2^{A_a})=1$	$\mu_3(ek_3^{A_a})=1$	$\mu_3(ek_4^{A_a})=1$
[50;60[	[0,5;0,6[	[0,3;0,35[	[5;6[	$T_{K\,EK_i 3}$	$\mu_3(ek_1^{A_a})=(60-ek_1^{A_a})/10$	$\mu_3(ek_2^{A_a})=(0,6-ek_2^{A_a})*10$	$\mu_3(ek_3^{A_a})=(0,35-ek_3^{A_a})*20$	$\mu_3(ek_4^{A_a})=(6-ek_4^{A_a})$
				$T_{K\,EK_i 4}$	$\mu_4(ek_1^{A_a})=1-\mu_3(ek_1^{A_a})$	$\mu_4(ek_2^{A_a})=1-\mu_3(ek_2^{A_a})$	$\mu_4(ek_3^{A_a})=1-\mu_3(ek_3^{A_a})$	$\mu_4(ek_4^{A_a})=1-\mu_3(ek_4^{A_a})$
[60;70[	[0,6;0,7[	[0,35;0,4[	[6;7[	$T_{K\,EK_i 4}$	$\mu_4(ek_1^{A_a})=1$	$\mu_4(ek_2^{A_a})=1$	$\mu_4(ek_3^{A_a})=1$	$\mu_4(ek_4^{A_a})=1$
[70;80[	[0,7;0,8[	[0,4;0,45[	[7;8[	$T_{K\,EK_i 4}$	$\mu_4(ek_1^{A_a})=(80-ek_1^{A_a})/10$	$\mu_4(ek_2^{A_a})=(0,8-ek_2^{A_a})*10$	$\mu_4(ek_3^{A_a})=(0,45-ek_3^{A_a})*20$	$\mu_4(ek_4^{A_a})=(8-ek_4^{A_a})$
				$T_{K\,EK_i 5}$	$\mu_5(ek_1^{A_a})=1-\mu_4(ek_1^{A_a})$	$\mu_5(ek_2^{A_a})=1-\mu_4(ek_2^{A_a})$	$\mu_5(ek_3^{A_a})=1-\mu_4(ek_3^{A_a})$	$\mu_5(ek_4^{A_a})=1-\mu_4(ek_4^{A_a})$
[80;100]	[0,8;1[	[0,45;0,5[	[8;10[	$T_{K\,EK_i 5}$	$\mu_5(ek_1^{A_a})=1$	$\mu_5(ek_2^{A_a})=1$	$\mu_5(ek_3^{A_a})=1$	$\mu_5(ek_4^{A_a})=1$

Полученные результаты обрабатываются, интерпретируются и представляются в виде отчета.

Для проверки основных функций и отражения принципа работы ПО АОР проведена его верификация. В качестве $ИР_1$ был выбран «сетевой файл-сервер» из категории «Сетевые серверы». Тестирование проводилось для конкретных исходных данных заданных в лингвистической форме. Для данного ИР были установлены следующие A_a ($a=\overline{1,3}$): A_1=«Злоупотребление средствами обработки информации»; A_2=«Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика»; A_3=«Повреждение носителей информации».

Далее по каждой угрозе осуществлялся расчет значений $dr^{(A_a)}$, результаты которого занесены в табл. 3, из которой видно, что значение СР для данного ИР по всем угрозам низкое.

Таблица 3

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

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	37,5	PH
A_3	33	0,07	0,17	3	30	PH

После этого осуществлялся расчет среднего значения $dr^{(cp)}$=34,17 для $ИР_1$, что по выражению (2) соответствует лингвистической интерпретации: СР с числовым эквивалентом 34,17 граничит между низким и средним риском с уверенностью эксперта по границе РН – 0,58 и РС – 0,42.

Дальнейшая проверка ПО проводилась на основе моделирования 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 – изменено значения оценочных компонент (уменьшение или увеличение).

1-е состояние с начальными условиями, а также результаты вычисления СР, приведены в табл. 3. Рассмотрим результаты моделирования для следующих состояний.

2-е состояние

На объекте оценивания изменились условия среды окружения, а именно после повторного анализа $ИР_1$ была дополнительно идентифицирована угроза A_4, т.е. A_4= «Нелегальное использование программного обеспечения». В результате этого осуществлен расчет значения СР для A_4 т.е. $dr^{(A_a)}$=32,5, а значение $dr^{(cp)}$ после введения A_4 составило $dr^{(cp)}$= 33,75 (РН (0,625), РС (0,375)), что граничит между низким (с уверенностью эксперта 0,625) и средним (с уверенностью эксперта 0,375) значением риска (рис. 2).

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 повторный расчёт $dr^{(A_a)}$ и $dr^{(cp)}$. Используя разработанную систему, с учетом моделируемой ситуации, полученное значение $dr^{(cp)}$ для $ИР_1$ уменьшилось до 32,5 (РН (0,75), РС (0,25)), т.е. $dr^{(cp)}$, граничит между низким (с уверенностью эксперта 0,75) и средним (с уверенностью эксперта 0,25) значением риска. Здесь значение $dr^{(cp)}$ меняется при изменении количества A_a. Дальнейшее экспериментальное исследование показало, что при значительном увеличении или уменьшении числа A_a значение $dr^{(cp)}$ может соответственно адекватно измениться.

Отчет

по расчету степени риска для активов организации
от 23.05.2012
для проекта
fuzzymethod

Сумарно по активам

Список активов	Степень риска
сетевые файл-серверы	РН (0,625), РС (0,375) - 33,75

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	37,5
Повреждение носителей информации	30
Нелегальное использование программного обеспечения	32,5

Рис. 2. Окно с отчетом значений СР

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).

На объекте оценивания были внедрены мероприятия для минимизации уровня угроз A_1, A_2, A_3.

После повторной реализации АОР экспертами были установлены величины оценочных компонент, значения которых приведены в табл. 4.

Таблица 4

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	23,5	РН
A_2	25	0,13	0,04	2	21,5	РН
A_3	5	0,05	0,03	2	15	НР

Для каждой A_a был повторно произведен расчет $dr^{(A_a)}$ (см. табл. 4). Величина $dr^{(cp)}$ для $ИР_1$ $dr^{(cp)}$=20, что соответствует значению T_{DR} = «РН» (уверенность эксперта – 1). Из сгенерированного ПО отчета видно, что степень риска существенно уменьшилась, следовательно, внедренные меры по обеспечению ИБ являются эффективными, а система АОР отреагировала адекватно изменению условий среды оценивания.

С учетом второй ситуации, осуществляется моделирование, при котором на объекте оценивания не учтены предыдущие результаты АОР. После первичной реализации АОР, не приняты во внимание полученные результаты и не внедрены меры по обеспечению ИБ.

После повторных АОР ситуация с выбранным ИР ухудшилась, о чем свидетельствуют определенные экспертами значения оценочных компонент (табл. 5). Из табл. 5 видно, что $dr^{(A_a)}$ существенно увеличились, а для двух угроз значение «РН» изменилось на «РС» (средняя степень риска нарушения ИБ).

Таблица 5

Результаты оценивания

A_a	P	F	L	D	$dr^{(A_a)}$	T_{DR}
A_1	52	0,81	0,05	1	45	РН
A_2	45	0,23	0,31	4	46	РС
A_3	43	0,47	0,27	3	45	РС

Величина $dr^{(cp)}$ для $ИР_1$ $dr^{(cp)}$=45,33, что соответствует значению T_{DR} = «РС» (уверенность эксперта – 1).

Также с учетом первой и второй ситуации был произведен АОР для дополнительных трех ИР. В табл. 6 и на рис. 3 показаны значения $dr^{(cp)}$ для этих ИР.

По аналогии с предыдущим экспериментом, проведены дополнительные исследования для других A_a, результаты которых занесены в табл. 7.

Таблица 6

Значение $dr^{(cp)}$

ИР	$dr^{(cp)}$		
	Средний уровень риска (начальные условия)	**Пониженный уровень риска**	**Повышенный уровень риска**
$ИР_1$	34,17 (РН (0,58), РС (0,42))	20 (РН)	45,33 (РС)
$ИР_2$	2,7 (РН)	16,7 (НР (0,33), РН (0,67))	29,83 (РН)
$ИР_3$	32 (РН (0,8), РС (0,2))	24,67 (РН)	39,33 (РН (0,07), РС (0,93))
$ИР_4$	25,75 (РН)	30,13 (РН (0,99), РС (0,01))	33 (РН (0,70), РС (0,30))

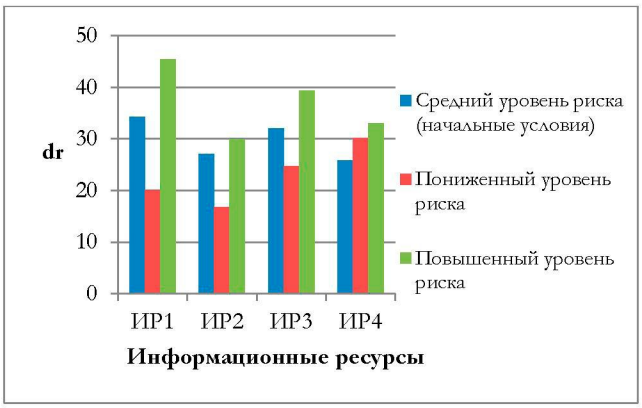

Рис. 3 Гистограмма средних значений СР

Полученные данные исследования подтверждают то, что ПО АОР адекватно реагирует на изменение значений выбранного базиса оценочных компонент при различных условиях среды оценивания, а значение риска существенно не изменяется при смене соответствующего базиса.

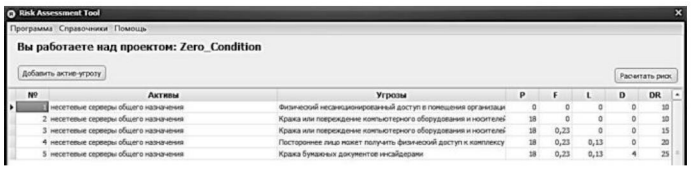

Рис. 4 Окно системы для выбора различных базисов оценочных компонент

Таблица 7

Результаты оценивания

ССО	ОК	A_1	A_2	A_3	A_4	$dr^{(ср)}$ (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})	24,5 (РН)	33 (РН)	23,5 (РН)	-	27 (РН)
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})	24,5 (РН)	33 (РН)	23,5 (РН)	22,5 (РН)	25,88 (РН)
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})	20 (*НР*)	20 (*НР*)	10 (*НР*)	-	16,67 – НР (0,33), РН (0,67)
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})	32,5 (РН)	27 (РН)	30 (РН)	-	29,83 (РН)
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})	45 (РС)	21 (РН)	30 (РН)	-	32 – РН (0,8), РС (0,2)
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})	45 (РС)	21 (РН)	30 (*РН*)	24,5 (РН)	30,13 – РН (0,99), РС (0,01)
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})	33 (*РН*)	16 (*НР*)	25 (*РН*)	-	24,67 (РН)
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})	48 (РС)	28 (РН)	42 (РС)	-	39,33 – РН (0,07), РС (0,93)

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	НР - 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
Посторонее 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 системы АОР

Данное ПО было использовано в учебном процессе кафедры безопасности информационных технологий Национального авиационного университета (г. Киев).

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., Ivanchenko Ye.V., Kazmirchuk S.V. Integrated view of risk characteristic, Zahist informacii, 2011, №1 (50), pp. 96-101.
[2]. Korchenko A.G., Kazmirchuk S.V. The synthesis methodology of analysis systems and risk assessment of information resources losses, Zahist informacii, 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 informacii, 2012, №1, pp. 126-139.
[4]. Korchenko A.G., Volyanskaya V.V., Kazmirchuk S.V., Okhrimenko A.A.Systems analysis and risk assessment of Government Information Resources losses, Zahist informacii, 2012, №2, pp. 52-58.
[5]. Lutskiy M.G., Korchenko A.G., Ivanchenko Ye.V., Kazmirchuk S.V. Research of information security risk & analysis assessment software, Zahist informacii, 2011, №3, pp. 97-108.
[6]. Lutskiy M.G., Ivanchenko E.V., Korchenko A.G., Kazmirchuk S.V., Okhrimenko A.A. Modern techniques of Information Risk Management, Zahist informacii, 2011, №1, pp. 5-16.
[7]. ND TZI 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 У НЕЧІТКИХ УМОВАХ

Для побудови систем управління інформаційної безпеки необхідно проводити аналіз і оцінювання ризиків, які часто характеризуються високою невизначеністю. Існуючі засоби оцінки не дають можливості застосування для аналізу та оцінювання ризиків широкого спектру початкових параметрів. На основі запропонованого автором методу аналізу та оцінювання ризиків втрати інформаційних ресурсів, було реалізовано відповідну програмну систему. Вона дозволяє проводити оцінювання в нечітких умовах з використанням встановленого базису оціночних компонент, які відображаються моделлю інтегрованого представлення параметрів ризику і можуть бути відображені, як в числовій, так і лінгвістичної формі. Для верифікації розробленого програмного продукту було здійснено моделювання при декількох різних умовах середовища оцінювання щодо захищеності інформаційних ресурсів. Отримані результати дослідження підтверджують те, що програмний засіб адекватно реагує на зміну умови середовища оцінювання, яка відображається значеннями оціночних компонент. Дослідження показали, що значення ризику істотно не змінюється при зміні базису оціночних компонент.

Ключові слова: ризик, аналіз ризику, оцінка ризику, система аналізу та оцінки ризику, параметри ризику, метод.

RISK ANALYSIS AND ASSESSMENT OF INFORMATION RESOURCES IN FUZZY CONDITIONS

The construction of information security management system requires providing the analysis and security risk assessment that are often characterized by high fuzzy conditions. The existing assessment tools do not provide opportunities for risk analysis and risk assessment of a wide range of initial parameters. On the basis of the proposed risk analysis and assessment method it was implemented an appropriate software system. It allows making assessment in fuzzy conditions using the established assessment components, which are displayed by the model of the integrated concept of risk parameters and can be represented in both numerical and linguistic forms. To verify the developed software product it was implemented the modeling under a number of different environmental conditions. 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, system of risk analysis and assessment, risk parameters, method.

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).