Раздел III. Защита объектов информатизации

УДК 621.311

О.А. Финько, Е.П. Соколовский

АЛГОРИТМ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА И.А. РЯБИНИНА

Оценка рисков безопасности структурно-сложных систем, в том числе систем защиты информации, с использованием логико-вероятностного метода И.А. Рябинина основана на исследовании сценариев перехода систем в опасное состояние, реализованных монотонными булевыми функциями. Развитие путей практического использования логико-вероятностного метода затруднено сложностью автоматизации процесса получения арифметического полинома вероятностной функции перехода системы в опасное состояние, имеющей в сценарии перехода группы совместных и несовместных событий. В статье предложен алгоритм построения и реализации арифметического полинома вероятностной функции для сценария перехода системы защиты информации в опасное состояние с группами совместных и несовместных событий, основанный на фундаментальных положениях алгебры логики, а именно методов построения и реализации числовых нормальных форм представления булевых функций и теории вероятностей. Применение известных положений позволяет получить преимущества при автоматизации процессов оценки рисков информационной безопасности в ходе решения задач построения и вычисления арифметических полиномов вероятностных функций перехода систем защиты информации в опасное состояние.

Логико-вероятностный метод; оценка риска, оценка систем защиты информации; числовая нормальная форма; реализация логических вычислений арифметическими полиномами.

O.A. Finko, E.P. Sokolovsky

RISK ASSESSMENT INFORMATION SECURITY ALGORITHM IS BASED ON THE I. RYABININ LOGICAL-PROBABILISTIC METHOD

Assessment of risks of safety of structural and difficult systems, including information security systems, with logiko-probabilistic method use. I.A. Ryabinin it is based on research of scenarios of transition of systems in the dangerous condition, realized by monotonous Boolean functions. Development of ways of practical use of a logiko-probabilistic method is complicated by complexity of automation of process of receiving an arithmetic polynom of probabilistic function of transition of system in the dangerous condition, having in the scenario of transition of group of joint and not joint events. In article the algorithm of construction and realization of an arithmetic polynom of probabilistic function for the scenario of transition of system of information security in a dangerous condition with groups of the joint and not joint events, based on fundamental provisions of algebra of logic, namely methods of construction and realization of numerical normal forms of representation of Boolean functions and probability theory is offered. Application of known provisions allows to get advantages at automation of processes of an assessment of risks of information security during the solution of problems of construction and calculation of arithmetic polynoms of probabilistic functions of transition of systems of information security in a dangerous condition.

Logiko-probabilistic method; risk assessment, assessment of systems of information security; numerical normal form; realization of logical calculations by arithmetic polynoms.

Согласно [1] булеву функцию, связывающую состояние элементов с состоянием системы, будем называть *функцией опасного состояния системы* (ФОС). Под *вероятностной функцией* (ВФ) будем понимать вероятность истинности булевой функции:

$$P\{\, f\,(\vec{\mathbf{z}})=1\},$$

где здесь и далее $f(\vec{\mathbf{z}}): \vec{\mathbf{z}}=\begin{bmatrix} z_1 & \dots & z_n \end{bmatrix},\ z_1,\dots,z_n \in \{0,1\}$.

В общем виде *алгоритм 1* оценки риска заключается в следующем [1]:

Шаг 1. Экспертным путем строится сценарий перехода некоторой системы в опасное состояние, описываемый *монотонной* булевой функцией.

Шаг 2. *По правилам перехода* из ФОС осуществляется получение арифметического полинома ВФ опасного состояния.

Шаг 3. На основании полученного арифметического полинома ВФ опасного состояния производится оценка риска для системы (безопасности системы).

В монографии [1] приведены основные приемы получения арифметического полинома ВФ перехода исследуемой системы в опасное состояние. В частности, один из алгоритмов основан на использовании *теоремы сложения вероятностей совместных событий*. В качестве событий рассматриваются *кратчайшие пути опасного функционирования системы*.

Кратчайший путь опасного функционирования (КПОФ) представляет собой такую конъюнкцию инициирующих условий (ИУ) z_i, ни одну из компонент которой нельзя изъять, не нарушив опасного функционирования системы [1]. Такую конъюнкцию можно записать в виде функции:

$$F_l = \bigwedge_{i\subset K_{F_l}} z_i\,, \qquad (1)$$

где K_{F_l} – множество номеров инициирующих условий, соответствующих данному l-му КПОФ; $\bigwedge$ – символ многоместной конъюнкции.

Очевидно, что КПОФ описывает один из возможных самостоятельных вариантов попадания исследуемой системы в опасное состояние с помощью минимального набора ИУ абсолютно необходимых для его осуществления. Тогда арифметический полином ВФ перехода исследуемой системы в опасное состояние можно получить по формуле [1]:

$$\begin{aligned} P\{\, f\,(\vec{\mathbf{z}})=1\} = Q_c = P\left\{\bigvee_{l=1}^{d} F_l\right\} = \sum_i P(F_i) - \sum_i\sum_j P(F_i\wedge F_j\,)+ \\ +\sum_i\sum_j\sum_k P(F_i\wedge F_j\wedge F_k) - \ldots + (-1)^{d-1}P(F_i\wedge\ldots\wedge F_d), \end{aligned} \qquad (2)$$

где F_l – кратчайшие пути опасного функционирования; d – количество КПОФ.

В качестве примера рассмотрим сценарий перехода некоторой системы защиты информации (СЗИ) в опасное состояние (рис. 1).

В соответствии с рис. 1 сценарий перехода в опасное состояние описывается ФОС:

$$\begin{aligned} f(\vec{\mathbf{z}}) &= ((z_1\vee z_2)\wedge(z_2\vee z_3))\vee z_3 z_4 = \\ &= z_1z_2\vee z_1z_3\vee z_2\vee z_2z_3\vee z_3z_4, \end{aligned} \qquad (3)$$

где здесь и далее z_i – булева переменная, обозначающая i-е ИУ и принимающая значения:

$z_i = 0$ – при нахождении ИУ в безопасном состоянии,

$z_i = 1$ – в случае перехода ИУ в опасное состояние.

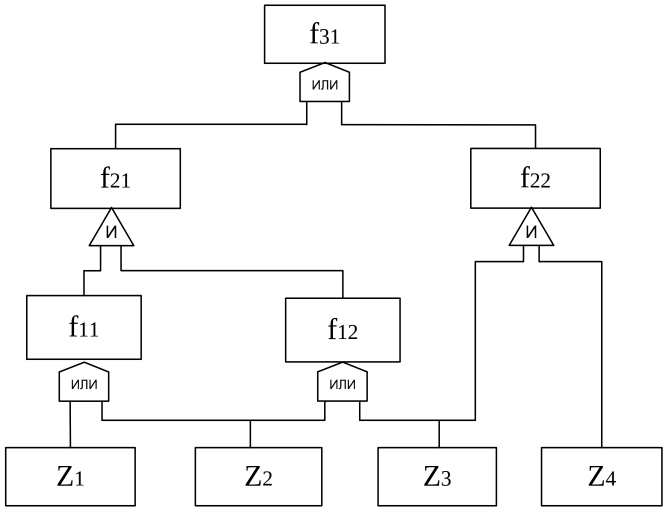

Рис. 1. Сценарий перехода СЗИ в опасное состояние

Запишем в соответствии с (1) КПОФ для сценария (рис. 1):

$$F_1 = z_2, \quad F_2 = z_1 z_3, \quad F_3 = z_3 z_4. \tag{4}$$

Подставляя (4) в (2) получим арифметический полином ВФ перехода СЗИ (рис. 1) в опасное состояние:

$$P\{ f(\vec{\mathbf{z}}) = 1\} = Q_c = P\left\{ \bigvee_{l=1}^{d} K_{F_l} \right\} = Q_2 + Q_1Q_3 + Q_3Q_4 - Q_1Q_2Q_3 - Q_1Q_3Q_4 - \tag{5}$$
$$-Q_2Q_3Q_4 + Q_1Q_2Q_3Q_4,$$

где здесь и далее Q_i – значение вероятности перехода *i*-го элемента СЗИ (ИУ) в опасное состояние.

Известны фундаментальные положения алгебры логики, согласно которым произвольная булева функция может быть однозначно представлена в:

- ♦ алгебраической нормальной форме (полиномом Жегалкина) [2]:

$$f(\vec{\mathbf{z}}) = \bigoplus_{i=0}^{2^n-1} g_i \wedge (z_1^{i_1} \wedge z_2^{i_2} \wedge \ldots \wedge z_n^{i_n}),\ g_i \in \{0,1\};$$

- ♦ числовой нормальной форме (ЧНФ) (арифметическим полиномом) [3]:

$$P(\vec{\mathbf{z}}) = \sum_{i=0}^{2^n-1} c_i\, z_1^{i_1} z_2^{i_2} \ldots z_n^{i_n},$$

$$z_u^{i_u} = \begin{cases} z_u, & i_u = 1, \\ 1, & i_u = 0 \end{cases}, \ c_i \text{ – целое.}$$

Представление булевой функции в указанных взаимосвязанных формах можно получить из обычной таблицы истинности (табл. 1).

Таблица 1

Обычная таблица истинности булевой функции

№ набора	$z_1,..., z_n$	$f(\vec{\mathbf{z}})$
0	000…0	$Y^{(0)}$
1	000…1	$Y^{(1)}$
⋮	⋮	⋮
2^n-1	111…1	$Y^{(2^n-1)}$

В качестве примера построим таблицу истинности ФОС (3) (табл. 2).

Таблица 2

Таблица истинности ФОС (3)

№ набора	$z_1,..., z_4$	$f(\vec{\mathbf{z}})$	№ набора	$z_1,..., z_4$	$f(\vec{\mathbf{z}})$
0	0000	0	8	1000	0
1	0001	0	9	1001	0
2	0010	0	10	1010	1
3	0011	1	11	1011	1
4	0100	1	12	1100	1
5	0101	1	13	1101	1
6	0110	1	14	1110	1
7	0111	1	15	1111	1

Совершенная дизъюнктивная нормальная форма (3) на основании табл. 2 представляется в виде:

$$\begin{aligned} f(\vec{\mathbf{z}}) = {} & \bar{z}_1\bar{z}_2z_3z_4 \vee \bar{z}_1z_2\bar{z}_3\bar{z}_4 \vee \bar{z}_1z_2\bar{z}_3z_4 \vee \bar{z}_1z_2z_3\bar{z}_4 \vee \\ & \vee\bar{z}_1z_2z_3z_4 \vee z_1\bar{z}_2z_3\bar{z}_4 \vee z_1\bar{z}_2z_3z_4 \vee z_1z_2\bar{z}_3\bar{z}_4 \vee \\ & \vee z_1z_2\bar{z}_3z_4 \vee z_1z_2z_3\bar{z}_4 \vee z_1z_2z_3z_4. \end{aligned} \tag{6}$$

При помощи эквивалентного преобразования [2] $\bar{z} = 1 \oplus z$ из (6) получим:

$$\begin{aligned} f(\vec{\mathbf{z}}) = {} & z_2 \oplus z_1z_3 \oplus z_3z_4 \oplus z_1z_2z_3 \oplus z_1z_3z_4 \oplus \\ & \oplus z_2z_3z_4 \oplus z_1z_2z_3z_4. \end{aligned} \tag{7}$$

Используя соотношения перехода от булевых функций к их представлению в ЧНФ [4, 5]:

$$x_1 \wedge x_2 = x_1x_2, \quad x_1 \vee x_2 = x_1 + x_2 - x_1x_2, \quad x_1 \oplus x_2 = x_1 + x_2 - 2x_1x_2, \quad \bar{x} = 1 - x$$

из (7) получим представление ФОС (3) арифметическим полиномом ВФ:

$$P(\vec{\mathbf{z}}) = Q_2 + Q_1Q_3 + Q_3Q_4 - Q_1Q_2Q_3 - Q_1Q_3Q_4 - Q_2Q_3Q_4 + Q_1Q_2Q_3Q_4,$$

который совпадает с ранее полученным арифметическим полиномом (5).

Известен [4, 5] *матричный способ* получения арифметического спектра коэффициентов ЧНФ с помощью прямого и обратного логического дискретного преобразования Фурье (ЛДПФ):

$$\begin{aligned} \vec{\mathbf{C}} &= \mathbf{A}_{2^n}\vec{\mathbf{Y}}, \\ \vec{\mathbf{Y}} &= \mathbf{A}_{2^n}^{-1}\vec{\mathbf{C}}, \end{aligned} \tag{8}$$

где $\mathbf{A}_{2^n}$ – матрица прямого арифметического преобразования размерности $2^n \times 2^n$ (базис преобразования); $\vec{\mathbf{Y}}$ – вектор истинности булевой функции $f(\vec{\mathbf{z}})$ такой, что

$$\vec{\mathbf{Y}} = \begin{pmatrix} Y^{(0)} & Y^{(1)} & \dots & Y^{(2^n-1)} \end{pmatrix}^T,$$

где T – символ транспонирования; $Y^{(i)}$ – числовое значение, принимаемое булевой функцией $f(\vec{\mathbf{z}})$ на i-м наборе булевых аргументов обычной таблицы истинности (табл. 1); $\vec{\mathbf{C}} = \begin{pmatrix} c_0 & c_1 & \dots & c_{2^n-1} \end{pmatrix}^T$ – арифметический спектр ЧНФ.

Матрица

$$\mathbf{A}_{2^n} = \left[\begin{array}{c|c} \mathbf{A}_{2^{n-1}} & 0 \\ \hline -\mathbf{A}_{2^{n-1}} & \mathbf{A}_{2^{n-1}} \end{array} \right], \tag{9}$$

является n-кронекеровской степенью

$$\mathbf{A}_{2^n} = \bigotimes_{j=1}^{n} \mathbf{A}_1, \tag{10}$$

где $\mathbf{A}_1 = \left[\begin{array}{c|c} 1 & 0 \\ \hline -1 & 1 \end{array} \right]$.

В соответствии с таблицей истинности (табл. 2):

$$\vec{\mathbf{Y}} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}^T,$$

матрица $\mathbf{A}_{2^4}$ согласно (9), (10) примет вид:

$$\mathbf{A}_{2^4} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 \\
-1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1
\end{pmatrix}$$

Выполняя прямое ЛДПФ (8), получим арифметический спектр арифметического полинома ФОС (3):

$$\vec{\mathbf{C}} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 0 & 0 & -1 & 1 \end{bmatrix}. \tag{11}$$

Тогда ЧНФ примет вид (совпадает с (5)):

$$P(\vec{\mathbf{z}}) = Q_2 + Q_1 Q_3 + Q_3 Q_4 - Q_1 Q_2 Q_3 - Q_1 Q_3 Q_4 - Q_2 Q_3 Q_4 + Q_1 Q_2 Q_3 Q_4.$$

При преобладании нулевых коэффициентов ЧНФ спектр $\vec{\mathbf{C}}$ удобно представлять в виде [6]:

$$\vec{\mathbf{C}} = \left[\left\{ c_{i_0}, i_0 \right\} \;\; \left\{ c_{i_1}, i_1 \right\} \;\; \ldots \;\; \left\{ c_{i_j}, i_j \right\} \right], \quad j < 2^n - 1, \tag{12}$$

где $c_{i_0}, c_{i_1}, \ldots, c_{i\,j} \neq 0$.

С учетом (12) спектр (11) можно представить в виде:

$$\vec{\mathbf{C}} = \left[\{1, 3\} \;\; \{1, 4\} \;\; \{-1, 7\} \;\; \{1, 10\} \;\; \{-1, 11\} \;\; \{-1, 14\} \;\; \{1, 15\} \right].$$

Применение способов построения и реализации ЧНФ в логико-вероятностном методе И.А. Рябинина (ЛВМ) позволяет получить преимущества при автоматизации процессов построения и реализации арифметических полиномов ВФ перехода исследуемой СЗИ в опасное состояние.

Согласно [7] булева функция n переменных $f(v)$ называется *полностью определенной*, если ее значения $f(v_i) = a_i = 0$ или 1 заданы во всех 2^n точках v_i области определения, $v_i = (z_1, \ldots, z_i)$. Если же значения функции не задано хотя бы в одной точке v_i, то она называется *неполностью определенной*.

В качестве примера рассмотрим сценарий перехода некоторой СЗИ в опасное состояние (рис. 2).

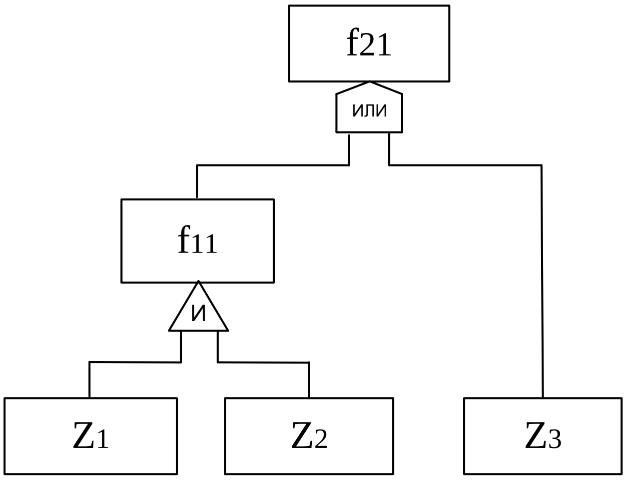

Рис. 2. Сценарий перехода СЗИ в опасное состояние

Логическая ФОС для сценария (рис. 2) примет вид:

$$f(z_1, z_2, z_3) = z_1 \wedge z_2 \vee z_3. \tag{13}$$

Когда в сценарии (рис. 2) ИУ z_i *совместны* – ФОС (13) будет полностью определенной и вероятность перехода СЗИ в опасное состояние определяется в соответствии с *алгоритмом 1*.

Если в сценарии перехода СЗИ в опасное состояние (рис. 2) ИУ, например, z_1 и z_3 – *несовместны,* то значения ФОС (13) будут заданы не на всех наборах обычной таблицы истинности (табл. 3).

Таблица 3

Таблица истинности ФОС (13) при несовместных ИУ z_1 и z_3

№ набора	z_1	z_2	z_3	$f(z_1, z_2, z_3)$
0	0	0	0	0
1	0	0	1	1
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	Ф
6	1	1	0	1
7	1	1	1	Ф

Очевидно, на пятом и седьмом наборах (табл. 3), когда аргументы $z_1 = 1$ и $z_3 = 1$ ФОС (13) имеет *неопределенное* значение, что в теории вероятностей известно как *несовместное событие* [8].

В подобных случаях использование положения алгебры логики о возможности *произвольного доопределения* с целью получения *полностью определенной* булевой функции [7] противоречит правилам теории вероятностей и ЛВМ.

Оценка безопасности функционирования системы, имеющей в сценарии перехода в опасное состояние элементы, которые могут находиться в трех состояниях, а также группы несовместных событий, рассматривалась в работах [1, 9, 10].

В соответствии с [9, 10] определение вероятности перехода системы, имеющей в своем составе *несовместные* события, в опасное состояние возможно при соблюдении ограничений:

- рассматриваются однородные объекты риска;
- справедливы следующие тождества:

$$z_1 \wedge z_2 = 0, \quad \overline{z}_1 \vee \overline{z}_2 = 1, \quad \overline{z}_1 \wedge z_2 = z_2, \quad z_1 \vee \overline{z}_2 = \overline{z}_2; \tag{14}$$

- для замещения несовместных событий их вероятностями используются правила:

$$\begin{cases} P\{z_1 \wedge z_2\} = 0, \quad P\{z_1 \vee z_2\} = P(z_1) + P(z_2) = 1, \\ P\{\overline{z}_1 \vee \overline{z}_2\} = 1, \quad P\{\overline{z}_1 \wedge \overline{z}_2\} = 1 - \{P(z_1) + P(z_2)\}. \end{cases} \tag{15}$$

Учитывая (14) и (15), а также правила ЛВМ получения арифметического полинома ВФ, для СЗИ, имеющей в сценарии перехода в опасное состояние несовместные ИУ, вероятность перехода в опасное состояние можно вычислить с использованием *алгоритма 2*:

Шаг 1. В сценарии перехода СЗИ в опасное состояние определяем:

- *группы совместных событий* (*ГСС*) (рис. 4). На рис. 4 обозначены: Z_{k-1}, Z_{k+1} – несовместные ИУ, ГСС – группа совместных событий, $P_{ОС\ ГСС\ 1}$ – вероятность перехода в опасное состояние ГСС 1, $P_{ОС\ ГСС}\ n$ – вероятность перехода в опасное состояние n-й ГСС, $P_{ОС\ Z^k}$ – вероятность перехода в опасное состояние Z_k ИУ, $P_{ОС\ ССС\ ГНС}$ – вероятность перехода в опасное состояние системы с несовместными ИУ;
- *несовместные* ИУ, которые не входят ни в одну из ГСС.

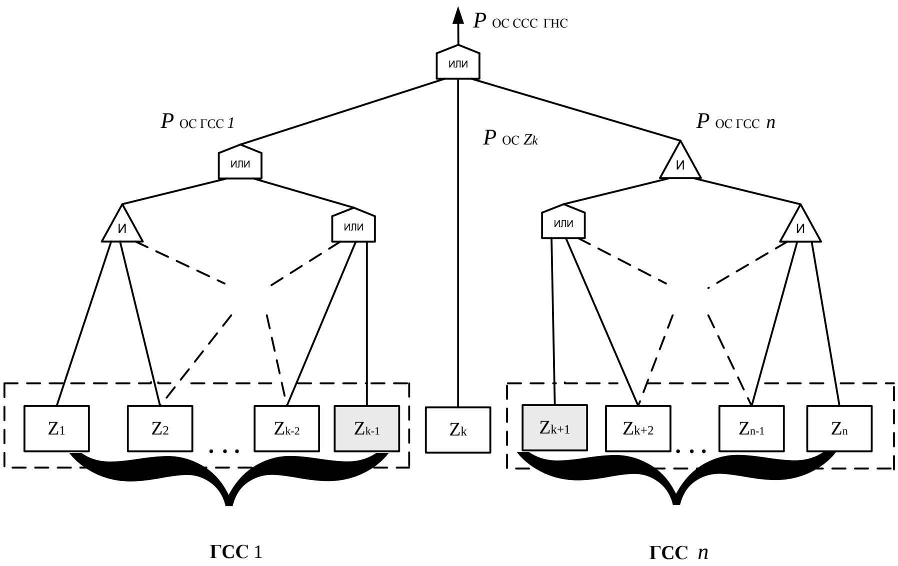

Рис. 4. Порядок определения ГСС для неполностью определенной ФОС

Шаг 2. Булеву функцию, описывающую взаимосвязь ИУ в соответствующей ГСС представляем:

- в ЧНФ (с использованием прямого ЛДПФ (8));
- арифметическим полиномом, используя известные соотношения [5]:

$$z_1 \wedge z_2 = z_1 z_2, \quad z_1 \vee z_2 = z_1 + z_2 - z_1 z_2 . \tag{16}$$

Шаг 3. С учетом тождеств (14), (15) и выражений (16) получаем арифметический полином ВФ перехода СЗИ в опасное состояние, описываемой неполностью определенной ФОС.

В соответствии с *алгоритмом 2* представим неполностью определенную ФОС с несовместными ИУ z_1 и z_3 (14) (табл. 3) арифметическим полиномом ВФ:

Шаг 1. Очевидно, что ИУ z_1 и z_2 – составляют ГСС, а ИУ z_3 в данную ГСС не входит.

Шаг 2. В соответствии с (16) построим арифметический полином ВФ перехода в опасное состояние ГСС:

$$P\left\{ f(z_1 \wedge z_2) = 1 \right\} = Q_1 Q_2 ,$$

где Q_i – вероятность перехода в опасное состояние i-го ИУ.

Шаг 3. В соответствии с (15) получаем арифметический полином ВФ перехода в опасное состояние системы с несовместными ИУ z_1 и z_3 (рис. 3):

$$P\left\{ f(z_1, z_2, z_3) = 1 \right\} = Q_3 + Q_1 Q_2 , \tag{18}$$

где Q_i – вероятность перехода в опасное состояние i-го ИУ.

Ясно, что с учетом несовместности z_1 и z_3 для (18) должно выполняться условие $Q_1 + Q_3 \le 1$ [8].

Использование фундаментальных положений алгебры логики, теории вероятностей, а также известных работ [1, 9, 10], делает удобным *алгоритм 2* для вычисления вероятности перехода в опасное состояние систем, описываемых как полностью определенными, так и неполностью определенными ФОС. Применение способов реализации ЧНФ позволяет получить преимущества при автоматизации процессов вычисления вероятности перехода исследуемых СЗИ в опасное состояние.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем: Монография. – СПб.: Политехника, 2000. – 248 с.
2. *Яблонский, С.В.* Введение в дискретную математику: Учеб. пособие для вузов. – 2-е изд., перераб. и доп.: Монография. – М.: Наука. гл. ред. физ.-мат. лит., 1986. – 348 с.
3. *Логачёв О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.
4. *Малюгин В.Д.* Применение алгебры кортежей логических функций // X Всесоюзное совещание по проблемам управления: Тез. докл. Кн. 1. – М.: Ин-т проблем управления, 1986.
5. *Финько О.А.* Модулярная арифметика параллельных логических вычислений: Монография / Под ред. В.Д. Малюгина. – М.: ИПУ РАН, 2003. – 224 с.
6. *Соколовский Е.П., Малашихин А.К., Финько О.А.* Применение числовой нормальной формы представления булевых функций в логико-вероятностном методе И.А. Рябинина // Материалы XIII Международной научно-практической конференции «Информационная безопасность», г. Таганрог, 9-13 июля 2013 г. Ч. II. – С. 113-118.
7. *Пухальский Г.И., Новосельцева Т.Я.* Цифровые устройства: Учебное пособие для втузов. – СПб.: Политехника, 1996. – 885 с.
8. *Вентцель, Е.С.* Теория вероятностей: Монография. – М., 1969. – 576 с.
9. *Черкесов, Г.Н., Можаев А.С.* Логико-вероятностные методы расчета надежности структурно-сложных систем. Качество и надежность изделий. – М.: Знание, 1991. – 340 с.
10. *Соложенцев, Е.Д.* Сценарное логико-вероятностное управление риском в бизнесе и технике: Монография. – СПб.: Изд. дом «Бизнес-пресса», 2004. – 432 с.

Статью рекомендовал к опубликованию д.т.н. В.Н. Марков.

Финько Олег Анатольевич – Филиал Военной академии связи (г. Краснодар). e-mail: ofinko@yandex.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79615874848; профессор.

Соколовский Евгений Петрович – e-mail: Biryza_08@mail.ru; тел.: +79181744325; адъюнкт.

Finko Oleg Anatolievich – Branch of the Military Academy of Communications (Krasnodar); e-mail: ofinko@yandex.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79615874848; professor.

Sokolovsky Evgeniy Petrovich – e-mail: Biryza_08 @mail.ru; phone: +79181744325; adjunct.

УДК 004.42

Е.Н. Тищенко, Е.Ю. Шкаранда

АЛГОРИТМИЗАЦИЯ ПРОЦЕССА ФОРМИРОВАНИЯ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются подходы к алгоритмизации процесса формирования частной модели угроз безопасности персональных данных организаций и предприятий. Предложены решения для определения состава угроз, уязвимостей и последствий реализации угроз. Для этого использованы экспертные, вероятностные методы и формализованные процедуры анализа предметной области. Рассмотрены основные блоки алгоритма формирования модели угроз, описаны особенности каждого из блоков. Показано, что предложенные подходы и методы решают проблему формализации решаемой задачи, позволяют унифицировать и автоматизировать