УДК 681.3+681.5:007

ПРИМЕРЫ ПОСТРОЕНИЯ ПОМЕХОУСТОЙЧИВЫХ К НЕСИММЕТРИЧНЫМ НЕРЕГУЛЯРНЫМ ВИРТУАЛЬНЫМ ПОСЛЕДОВАТЕЛЬНОСТЯМ АЛГОРИТМОВ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ

АЛИПОВ Н.В., АЛИПОВ И.Н., ЛИТВИНОВА Е.И.

Строятся алгоритмы поиска точки с характерным признаком, помехоустойчивые к несимметричным нерегулярным виртуальным последовательностям, и задается функционирование дискретных автоматов с псевдослучайными переходами систем защиты информации.

В работе [1] описаны стратегии поиска, правила формирования нового интервала неопределенности и логическая схема помехоустойчивых к несимметричным нерегулярным виртуальным последовательностям алгоритмов поиска точки с характерным признаком. В предлагаемом исследовании разрабатываются примеры таких алгоритмов, синтезированных для конкретных их параметров и параметров виртуальной последовательности.

Первоначально рассмотрим случай, для которого характерно $l_1 = 1$, $l_2 = 2$, $H = 2$, $a = 4h$, $k = 1$. На основании соотношений (25), приведенных в работе [1], устанавливаем, что уменьшение исходного интервала неопределенности начинается тогда, когда для параметра алгоритма i выполняется соотношение:

$$i \geq l_2 + 1. \qquad (1)$$

Для нашего примера первое значение параметра i, которое удовлетворяет соотношению (1), будет значением $i = 3$. Для $i = 3$ алгоритм поиска достаточно прост: используется принцип “повторных сравнений”. В этом случае на основании соотношений (25) из [1] устанавливаем:

$$\varphi_{1,3}^{2,1,2,4}(3,1) = 2\ ;\ x_1^1 = h.$$

При этом если возникает исход типа а) [1], то поиск заканчивается $x \in \left[0, x_1^1\right)$; если же возникает исход типа б) [1], то повторяют эксперимент: $x_1^2 = x_1^1$.

Может также возникнуть исход типа а) либо типа б). Для исхода типа а) поиск заканчивается. В этом случае формируется такой полуоткрытый интервал неопределенности: $x \in \left[0, x_1^1\right)$.

Для исхода типа б) повторяем эксперимент: $x_1^3 = x_1^1$,

По итогам выполнения третьего шага алгоритма может быть сформирован исход типа а) либо типа б). Для исхода типа а) устанавливаем: $x \in \left[0, x_1^1\right)$.

Для исхода типа б) выделяем такой полуоткрытый интервал неопределенности: $x \in \left[x_1^1, 1\right)$.

Поскольку в распоряжении алгоритма не осталось ни одного шага, то на основании соотношений (25), определенных в работе [1], устанавливаем:

$$l\left(\left[0, x_1^1\right)\right) = h\ ;\ l\left(\left[x_1^1\right)\right) = h\ ,\ l([0,1)) = 2h\ , \qquad (2)$$

где $l\left(\left[0, x_1^1\right)\right)$ – длина полуоткрытого интервала неопределенности $\left[0, x_1^1\right)$.

Поскольку $\varphi_{1,3}^{2,1,2,4}(3,1) = l([0,1))/h$, то получаем такое равенство:

$$\varphi_{1,3}^{2,1,2,4}(3,1) = 2. \qquad (3)$$

Получаем, что в тех же случаях, когда $H = l_2$, применяется только принцип “повторных сравнений”.

Пусть $i = 4$, тогда в некоторой точке $x_1^1 \in (0,1)$ выполняем первый эксперимент. При этом, как уже установлено, может возникнуть исход типа а) и исход типа б). Для исхода типа а) на основании соотношения (1), приведенного в работе [1], устанавливаем:

$$l\left(\left[0, x_1^1\right)\right) = h\varphi_{1,3}^{2,1,2,4}(3,1) = 2h\ ;\ x_1^1 = 2h. \qquad (4)$$

Для исхода типа б) повторяем эксперимент: $x_1^2 = x_1^1$.

Если при этом возникает исход типа а), то это свидетельствует о действии виртуальной последовательности на первом шаге алгоритма. Следует заметить, что ее проявление также не будет наблюдаться и на третьем шаге алгоритма (по определению $A_{1,3}$-последовательности). Действуя на полуоткрытом интервале неопределенности $\left[0, x_1^1\right)$ классическим одношаговым алгоритмом поиска, разбиваем его на две равные части. По этой причине устанавливаем истинность соотношения

$$\varphi\left(\left[0, x_1^1\right)\right) = 2h. \qquad (5)$$

Если же на втором шаге алгоритма возникает исход типа б), то снова повторяют эксперимент: $x_1^3 = x_1^1$.

Если по итогам третьего шага формируется исход типа а), то это свидетельствует о действии виртуальной последовательности на первых двух шагах алгоритма. По определению $A_{1,3}$-последовательности на третьем и четвертом шагах проявление виртуальной последовательности не будет наблюдаться. В распоряжении алгоритма остался один

шаг (четвертый). Действуя на четвертом шаге алгоритма классическим алгоритмом поиска, разобъем полуоткрытый интервал неопределенности $\left[0, x_1^1\right)$ на две равные части, что не противоречит соотношениям (4), (5).

Если же по итогам выполнения третьего шага алгоритма будет сформирован исход типа б), то выделяем новый полуоткрытый интервал неопределенности $x \in \left[x_1^1, 1\right)$.

Поскольку в распоряжении алгоритма остался один шаг, то, как следует из соотношений (25) из [1], этот полуоткрытый интервал неопределенности не может быть уменьшен, его длина равна h.

Из проведенного анализа всевозможных исходов устанавливаем:

$$l([0,1)) = l\left(\left[0, x_1^1\right)\right) + l\left(\left[x_1^1, 1\right)\right) = 3h. \qquad (6)$$

Из (6) устанавливаем истинность соотношения

$$\varphi_{1,3}^{2,1,2,4}(4,1) = 3. \qquad (7)$$

Пусть $i = 5$ и в точке x_1^1 выполнен первый шаг алгоритма. Тогда если по итогам первого шага возникает исход типа а), то, как уже известно,

$$x \in \left[0, x_1^1\right), \; l\left(\left[0, x_1^1\right)\right) = h\varphi_{1,3}^{2,1,2,4}(4,1) = 3h. \qquad (8)$$

Если по итогам первого шага сформирован исход типа б), то повторяем эксперимент $x_1^2 = x_1^1$.

Если в результате второго шага формируется исход типа а), то на первом шаге действовала виртуальная последовательность $x \in \left[0, x_1^1\right)$ и этот полуоткрытый интервал будет разбит на $\Psi_{1,3}(5-2,1)$ равных частей. По определению рассматриваемой виртуальной последовательности она также не будет проявляться только на третьем шаге алгоритма. Поэтому устанавливаем новую длину полуоткрытого интервала $\left[0, x_1^1\right)$:

$$l\left(\left[0, x_1^1\right)\right) = 2h. \qquad (9)$$

Если в результате выполнения второго эксперимента формируется исход типа б), то эксперимент повторяется на третьем шаге алгоритма: $x_1^3 = x_1^1$.

Если возникает при этом исход типа а), то это свидетельствует о действии виртуальной последовательности на двух первых шагах алгоритма. Эта последовательность также не будет проявляться и на четвертеом шаге алгоритма. Действуя классическим алгоритмом поиска, разобъем полуоткрытый интервал неопределенности $\left[0, x_1^1\right)$ на $\Psi_{1,3}(5-3,1)$ равных частей и установим новую длину полуоткрытого интервала $\left[0, x_1^1\right)$

$$l\left(\left[0, x_1^1\right)\right) = h\Psi_{1,3}(5-3,1) = 2h. \qquad (10)$$

В том случае, когда возникает исход типа б), будут справедливы такие соотношения:

$$x \in \left[x_1^1, 1\right), \; l\left(\left[x_1^1, 1\right)\right) = h\varphi_{1,3}^{2,1,2,4}(5-3,1) = h. \qquad (11)$$

Поскольку $l([0,1)) = l\left(\left[0, x_1^1\right)\right) + l\left(\left[x_1^1, 1\right)\right)$, то на основании соотношений (8)-(11) устанавливаем:

$$\begin{aligned} &\varphi_{1,3}^{2,1,2,4}(5,1) = \\ &= \min\left\{\varphi_{1,3}^{2,1,2,4}(4,1), \Psi_{1,3}(5-2,1), \Psi_{1,3}(5-3,1)\right\} + \\ &+ \varphi_{1,3}^{2,1,2,4}(2,1) = 3. \end{aligned} \qquad (12)$$

По описанной схеме были найдены значения функции $\varphi_{1,3}^{2,1,2,4}(i,k)$ для других значений параметра i:

$$\varphi_{1,3}^{2,1,2,4}(6,1) = 4, \; \varphi_{1,3}^{2,1,2,4}(7,1) = 7. \qquad (13)$$

Показано, что для всех других значений параметра i справедливо соотношение:

$$\varphi_{1,3}^{2,1,2,4}(i,1) = \varphi_{1,3}^{2,1,2,4}(i-1,1) + \varphi_{1,3}^{2,1,2,4}(i-3,1). \qquad (14)$$

Значения функции $\varphi_{1,3}^{2,1,2,4}(i,1)$ приведены в табл.1.

Таблица 1

i	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi_{1,3}^{2,1,2,4}(i,1)$	1	1	2	3	3	4	7	10	14	21	31	45

Рассмотрим другой пример, для которого характерно $l_1 = 1$, $l_2 = 2$, $H = 2$, $a = 16h$, $k = 1$.

Следует заметить, что для значений параметра i, принадлежащих диапазону $[1,8]$, значения функций $\varphi_{1,3}^{2,1,2,16}(i,1)$ и $\varphi_{1,3}^{2,1,2,4}(i,1)$ совпадают.

Пусть $i = 9$ и в некоторой точке выполнен первый эксперимент. При этом для исхода типа а), как уже известно, будем иметь

$$l\left(\left[0, x_1^1\right)\right) = h\varphi_{1,3}^{2,1,2,16}(8,1) = 10h. \qquad (15)$$

Для исхода типа б) повторяем эксперимент. Рассмотрим наихудший случай: исход типа б) возникает на втором шаге, на третьем шаге повторяем эксперимент, по итогам этого эксперимента может появиться исход типа а) либо типа б).

Для исхода типа а) характерно действие виртуальной последовательности на первых двух шагах алгоритма, на третьем шаге алгоритма это проявление было обнаружено (ее действие прекратилось и это привело к противоречию). На этом основании устанавливаем $x \in \left[0, x_1^1\right)$, виртуальная последовательность не будет проявляться на четвертом, седьмом, восьмом шагах алгоритма. Действуя на

этих шагах классическим алгоритмом поиска точки x с характерным признаком, разобъем полуоткрытый интервал $\left[0, x_1^1\right)$ на восемь равных частей. На этом основании устанавливаем:

$$l\left(\left[0, x_1^1\right)\right) = h\Psi_{1,3}(9-3,1) = 8h\,. \qquad (16)$$

Если на третьем шаге алгоритма формируется исход типа б), то, как было показано ранее, будут справедливы такие соотношения:

$$x \in \left[x_1^1, 1\right),\ l\left(\left[x_1^1, 1\right)\right) = h\varphi_{1,3}^{2,1,2,16}(9-3,1) = 4h\,. \qquad (17)$$

Поскольку $l([0,1)) = l\left(\left[0, x_1^1\right)\right) + l\left(\left[x_1^1, 1\right)\right)$, то с учетом соотношений (15)-(17) будет справедливо выражение

$$\begin{aligned}&\varphi_{1,3}^{2,1,2,16}(9,1) = \\ &= \min\left\{\varphi_{1,3}^{2,1,2,16}(8,1), \Psi_{1,3}(9-3,1)\right\} + \\ &+ \varphi_{1,3}^{2,1,2,16}(9-3,1) = 12.\end{aligned} \qquad (18)$$

Показано, что для $i = 10$ будут иметь место такие соотношения:

$$\begin{aligned}&l\left(\left[0, x_1^1\right)\right) = h\varphi_{1,3}^{2,1,2,16}(10-1,1) = 12\,; \\ &l\left(\left[0, x_1^1\right)\right) = h\Psi_{1,3}(10-3,1) = 8\,; \\ &l\left(\left[x_1^1, 1\right)\right) = h\varphi_{1,3}^{2,1,2,16}(10-3,1) = 7\,,\end{aligned} \qquad (19)$$

на основании которых устанавливаем:

$$\varphi_{1,3}^{2,1,2,16}(10,1) = \Psi_{1,3}(10-3,1) + \varphi_{1,3}^{2,1,2,16}(10-3,1) = 15\,.$$

При всех других значениях параметра i для функции $\varphi_{1,3}^{2,1,2,16}(i,1)$ справедливо выражение

$$\varphi_{1,3}^{2,1,2,16}(i,1) = \varphi_{1,3}^{2,1,2,16}(i-1,1) + \varphi_{1,3}^{2,1,2,16}(i-3,1). \qquad (20)$$

Значения этой функции приведены в табл.2.

Таблица 2

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi_{1,3}^{2,1,2,4}(i,1)$	1	1	2	3	3	4	7	10	12	15	25	37	52

В том случае, когда параметры алгоритма принимают значения $l_1 = 1$, $l_2 = 2$, $H = 2$, $a = \infty$, $k = 1$, для функции $\varphi_{1,3}^{2,1,2,\infty}(i,1)$ справедлив такой ряд ее значений (табл.3).

Таблица 3

i	1	2	3	4	5	6	7	8	9
$\varphi_{1,3}^{2,1,2,4}(i,1)$	1	1	2	3	3	4	7	10	12
i	10	11	12	13	14	15			
$\varphi_{1,3}^{2,1,2,4}(i,1)$	15	25	37	47	57	94			

Показано, что для этой функции имеет место такое соотношение:

$$\begin{aligned}&\varphi_{1,3}^{2,1,2,1\infty}(i,1) = \\ &= \min\left\{\varphi_{1,3}^{2,1,2,\infty}(i-1,1), \Psi_{1,3}(i-3,1)\right\} + \\ &+ \varphi_{1,3}^{2,1,2,\infty}(i-3,1)\ .\end{aligned} \qquad (21)$$

Рассмотрим еще один пример построения алгоритма поиска точки с характерным признаком, для которого $l_1 = 1$, $l_2 = 2$, $H = 3$, $a = 4h$, $k = 1$. При таком сочетании параметров алгоритма поиска целесообразно применить для исхода а) оптимистическую стратегию поиска, для исхода б) – пессимистическую стратегию [1].

Показано, что для $i = 1, 2, 3, 4, 5$ значения функций $\varphi_{1,3}^{3,1,2,4}(i,1)$ и $\varphi_{1,3}^{2,1,2,4}(i,1)$ совпадают.

Предположим, что $i = 6$ и в некоторой точке x_1^1 совершен первый шаг алгоритма. Тогда, если возникает исход типа а), то, как известно,

$$l\left(\left[0, x_1^1\right)\right) = h\varphi_{1,3}^{3,1,2,4}(i-1,1) = 3h\,. \qquad (22)$$

В том случае, когда возникает исход типа б), принимаем на этом шаге оптимистическую стратегию $x_1^2 \in \left[x_1^1, 1\right)$.

Если на втором шаге алгоритма возникает исход типа а), то на третьем шаге принимаем пессимистическую стратегию $x_1^3 = x_1^1$.

При этом если на третьем шаге алгоритма формируется исход типа а), то это свидетельствует о действии виртуальной последовательности на первом шаге алгоритма, следующее ее применение возможно только на пятом и шестом шагах алгоритма. Классическим алгоритмом поиска разобъем полуоткрытый интервал $\left[0, x_1^1\right)$ на $\Psi_{1,3}(i-3,1) = 2$ равных частей, следовательно,

$$l\left(\left[0, x_1^1\right)\right) = 2h\,. \qquad (23)$$

Если на этом шаге алгоритма возникает исход типа б), то устанавливаем $x \in \left[x_1^1, x_1^2\right)$, и на этом полуоткрытом интервале неопределенности будет действовать помехоустойчивый алгоритм поиска, который, по предположению, разобьет его на $\varphi_{1,3}^{3,1,2,4}(6-3,1)$ равные части. Следовательно,

$$l\left(\left[x_1^1, x_1^2\right)\right) = 2h\,. \qquad (24)$$

В том случае, когда $x_1^2 \in \left[x_1^1, 1\right)$ и на втором шаге алгоритма возникает исход типа б), то на третьем шаге снова применяем оптимистическую стратегию $x_1^3 \in \left[x_1^2, 1\right)$. Если при такой комбинации оптимистических стратегий на третьем шаге возникает исход типа а), то на четвертом шаге алгоритма

применяем пессимистическую стратегию $x_1^4 = x_1^1$. При этом если возникает исход типа а), то это свидетельствует о действии виртуальной последовательности на первых двух шагах алгоритма. По определению виртуальной $A_{1,3}$-последовательности при таких исходах эта последовательность будет отсутствовать на третьем, четвертом, пятом шагах алгоритма ($H = 3$). Поэтому применим на пятом шаге алгоритма классический алгоритм поиска: разобьем полуоткрытый интервал неопределенности на две равные части, что не противоречит соотношению (23).

Если же на четвертом шаге алгоритма возникнет исход типа б), то на пятом шаге снова применим пессимистическую стратегию $x_1^5 = x_1^2$. Если при этом возникнет исход типа а), то это будет свидетельствовать о том, что $x \in \left[x_1^1, x_1^2\right)$ и виртуальная $A_{1,3}$-последовательность действовала на втором шаге алгоритма. Если возникает исход типа б), то это свидетельствует о том, что виртуальная последовательность не проявлялась на третьем, четвертом и пятом шагах алгоритма, на шестом шаге алгоритма ее проявление возобновится. Поэтому, хотя проявление виртуальной последовательности и обнаружено, уменьшить длину выделенного полуоткрытого интервала не удается (на шестом шаге в обязательном порядке будет действовать виртуальная последовательность). На этом основании устанавливаем истинность соотношений:

$$\Psi_{1,3}(6-5,1) = 1,\ \ l\left(\left[x_1^1, x_1^2\right)\right) = h, \qquad (25)$$

которые противоречат (24).

Если же при использовании пессимистической стратегии вида $x_1^5 = x_1^2$ возникает исход типа б), то

$$x \in \left[x_1^2, x_1^3\right),\ \ l\left(\left[x_1^2, x_1^3\right)\right) = h. \qquad (26)$$

В том случае, когда $x_1^3 \in \left[x_1^2, 1\right)$ и на третьем шаге возникает исход типа б), то устанавливаем, что $x \in \left[x_1^1, 1\right)$ (исход типа б) возник $(l_2 + 1) - h$ раз; это и есть подтверждением того, что исход типа б), возникший на первом шаге алгоритма, был истинным). На четвертом шаге алгоритма снова применяем оптимистическую стратегию поиска $x_1^4 \in \left[x_1^3, 1\right)$.

Как известно, если в распоряжении алгоритма остается l_2 шагов, то независимо от типа исхода применяют принцип повторных сравнений (для исхода типа а) он применяется в точках x_1^2, x_1^3, для исхода типа б) – в точках x_1^3, x_1^4).

Для исхода типа а) такой эксперимент выполняем в точке $x_1^5 = x_1^2$. При этом если возникает исход типа а), то это свидетельствует о том, что $x \in \left[x_1^1, x_1^2\right)$ и действии виртуальной последовательности на втором и третьем шагах алгоритма.

По определению виртуальной $A_{1,3}$-последовательности в такой ситуации ее проявление не будет наблюдаться на четвертом, пятом и шестом шагах алгоритма. Действуя классическим алгоритмом поиска точки x с характерным признаком, разобъем некоторый интервал неопределенности на $\Psi_{1,3}(6-5,1) = 2$ равные части. На этом основании устанавливается истинность соотношения

$$l\left(\left[x_1^1, x_1^2\right)\right) = h, \qquad (27)$$

которое противоречит соотношению (25).

Если при размещении пятого эксперимента в точке x_1^2 возникает исход типа б), то последний шестой эксперимент выполняется в точке x_1^3. В этом случае устанавливается истинность следующих соотношений: для исхода типа а)

$$l\left(\left[x_1^2, x_1^3\right)\right) = h;\ \ l\left(\left[x_1^2, x_1^3\right)\right) = h. \qquad (28)$$

Если при размещении четвертого эксперимента в одной из точек интервала $\left[x_1^3, 1\right)$ возникает исход типа б), то $x \in \left[x_1^2, 1\right)$ и принцип "повторных сравнений" на каждом шаге алгоритма первоначально применяют в точке x_1^3 и подтверждают истинность соотношения:

$$l\left(\left[x_1^2, x_1^3\right)\right) = h\Psi_{1,3}(6-5,1) = 2h. \qquad (29)$$

Затем в случае возникновения исхода типа б) на шестом шаге в точке x_1^4 устанавливают истинность таких выражений:

$$l\left(\left[x_1^3, x_1^4\right)\right) = h\Psi_{1,3}(6-6,1) = h;$$

$$l\left(\left[x_1^4, 1\right)\right) = h\varphi_{1,3}^{3,1,2,4}(6-6,1) = h. \qquad (30)$$

Поскольку

$$l([0,1]) = l\left(\left[0, x_1^1\right)\right) + l\left(\left[x_1^1, x_1^2\right)\right) + l\left(\left[x_1^2, x_1^3\right)\right) + l\left(\left[x_1^3, x_1^4\right)\right) + l\left(\left[x_1^4, 1\right)\right), \qquad (31)$$

то на основании минимаксного критерия оптимальности и соотношений (22), (23), (25), (31) устанавливаем

$$\varphi_{1,3}^{H,1,2,4}(6,1) = \Psi_{1,3}(6-3,1) + \Psi_{1,3}(6-5,1) + \varphi_{1,3}^{H,1,2,4}(6-4,1) + \Psi_{1,3}(6-6,1) + \varphi_{1,3}^{H,1,2,4}(6-6,1) = 6. \qquad (32)$$

Показано, что для $i = 7$ целесообразно применить на первых трех шагах алгоритма принцип "повтор-

ных сравнений". В этом случае устанавливаем истинность такого соотношения:

$$\varphi_{1,3}^{3,1,2,4}(7,2) = 8 \ . \qquad (33)$$

Для других значений параметра i построение алгоритма поиска точки с характерным признаком приведем без детального пояснения. На первом шаге алгоритма некоторым образом выберем точку первого эксперимента $x_1^1 \in [0,1)$.

Для исхода типа а) имеем:

$$x \in \left[0, x_1^1\right), \ l\left(\left[0, x_1^1\right)\right) = h\varphi_{1,3}^{3,1,2,4}(7,1) = 8h \ . \qquad (34)$$

Для исхода типа б) второй эксперимент совершаем в точке $x_1^2 \in \left[x_1^1, 1\right)$, относительно точки x формируем полуоткрытый интервал неопределенности $\left[x_1^{1,1}, 1\right)$, где

$$x_1^{1,1} = \begin{cases} x_1^1 - 4h, x_1^1 - 4h \ge 0; \\ 0 \ \text{в противном случае.} \end{cases} \qquad (35)$$

Если в этом случае возникает исход типа а), то $x_1^3 = x_1^1$. Если при таких условиях формируется исход типа а), то $x \in \left[x_1^{1,1}, x_1^1\right)$ и этот отрезок будет разбит на $\Psi_{1,3}(8-3,1)$ равных частей. Поэтому устанавливаем:

$$l\left(\left[x_1^{1,1}, x_1^1\right)\right) = h\Psi_{1,3}(8-3,1) = 4h \ ,$$

что не противоречит соотношению (35).

Если в этом случае возникает исход типа б), то $x \in \left[x_1^1, x_1^2\right)$ и

$$l\left(\left[x_1^1, x_1^2\right)\right) = h\varphi_{1,3}^{3,1,2,4}(8-3,1) = 3h \ . \qquad (36)$$

Второй шаг: $x_1^2 \in \left[x_1^2, 1\right)$, возникает исход типа б) $x_1^3 \in \left[x_1^2, 1\right)$, $x \in \left[x_1^{2,1}, 1\right)$,

$$x_1^{2,1} = \begin{cases} x_1^2 - 4h \ge x_1^{1,1}; \\ x_1^{1,1} \ \text{в противном случае.} \end{cases}$$

Третий шаг: $x_1^3 \in \left[x_1^2, 1\right)$, возникает исход типа а): $x_1^4 = x_1^1$.

Четвертый шаг: $x_1^4 = x_1^1$, возникает исход типа а):

$$x \in \left[0, x_1^1\right), \ l\left(\left[x_1^{1,1}, x_1^1\right)\right) = 4h \ ; \qquad (37)$$

возникает исход типа б): $x_1^5 = x_1^2$.

Пятый шаг: возникает исход типа а): виртуальная последовательность действовала на втором шаге и на этом основании устанавливаем: $x \in \left[x_1^1, x_1^2\right)$ и

$$l\left(\left[x_1^1, x_1^2\right)\right) = h\Psi_{1,3}(8-3,1) = 4h \ ; \qquad (38)$$

возникает исход типа б): $x \in \left[x_1^2, x_1^3\right)$,

$$l\left(\left[x_1^2, x_1^3\right)\right) = h\varphi_{1,3}^{3,1,2,4}(8-3,1) = 2h \ . \qquad (39)$$

Четвертый шаг: $x_1^3 \in \left[x_1^2, 1\right)$ и на третьем шаге возникает исход типа б): $x \in \left[x_1^1, 1\right)$, $x_1^4 \in \left[x_1^3, 1\right)$; если при этом возникает исход типа а), то $x_1^5 = x_1^2$.

Пятый шаг: если для $x_1^5 = x_1^2$ возникает исход типа а), то $x \in \left[x_1^1, x_1^4\right)$ и на втором и третьем шагах алгоритма действовала помеха; на этом основании устанавливаем:

$$x \in \left[x_1^1, x_1^2\right), \ l\left(\left[x_1^1, x_1^2\right)\right) = h\Psi_{1,3}(8-5,1) = 2h \ , \qquad (40)$$

если при этом возник исход типа б), то $x_1^6 = x_1^3$.

Шестой шаг: возникает исход типа а):

$$x \in \left[x_1^2, x_1^3\right), \ l\left(\left[x_1^2, x_1^3\right)\right) = h\Psi_{1,3}(8-6,1) = h \ ; \qquad (41)$$

возникает исход типа б):

$$x \in \left[x_1^3, x_1^4\right), \ l\left(\left[x_1^3, x_1^4\right)\right) = h\varphi_{1,3}^{3,1,2,4}(8-6,1) = h \ . \qquad (42)$$

Четвертый шаг: если $x_1^4 \in \left[x_1^3, 1\right)$ и возникает при этом исход типа б), то $x \in \left[x_1^2, 1\right)$, $x_1^5 \in \left[x_1^4, 1\right)$.

Пятый шаг: возникает исход типа а): $x_1^6 = x_1^3$.

Шестой шаг: возникает исход типа а):

$$x \in \left[x_1^2, x_1^3\right), \ l\left(\left[x_1^2, x_1^3\right)\right) = h\Psi_{1,3}(8-5,1) = 2h \ ; \qquad (43)$$

возникает исход типа б): $x_1^7 = x_1^4$.

Седьмой шаг: возникает исход типа а):

$$x \in \left[x_1^3, x_1^4\right), \ l\left(\left[x_1^3, x_1^4\right)\right) = h\Psi_{1,3}(8-7,1) = h \ ; \qquad (44)$$

возникает исход типа б):

$$x \in \left[x_1^4, x_1^5\right), \ l\left(\left[x_1^4, x_1^5\right)\right) = h\varphi_{1,3}^{3,1,2,4}(8-7,1) = h \ . \qquad (45)$$

Пятый шаг: $x_1^5 \in \left[x_1^4, 1\right)$ и возникает исход типа б): $x \in \left[x_1^3, 1\right)$, $x_1^6 \in \left[x_1^5, 1\right)$.

Шестой шаг: если возникает исход типа а), то $x_1^7 = x_1^4$.

Седьмой шаг: возникает исход типа а):

$$x \in \left[x_1^3, x_1^4\right), \ l\left(\left[x_1^3, x_1^4\right)\right) = h\Psi_{1,3}(8-7,1) = h \ ; \qquad (46)$$

возникает исход типа б): $x_1^7 = x_1^4$.

Восьмой шаг: возникает исход типа а):

$$x \in \left[x_1^4, x_1^5\right), l\left(\left[x_1^4, x_1^5\right)\right) = h\Psi_{1,3}(8-8,1) = h; \quad (47)$$

возникает исход типа б):

$$x \in \left[x_1^5, x_1^6\right), \; l\left(\left[x_1^5, x_1^6\right)\right) = h\varphi_{1,3}^{3,1,2,4}(8-8,1) = h. \quad (48)$$

Шестой шаг: $x_1^6 \in \left[x_1^5, 1\right)$ и возникает исход типа б): $x \in \left[x_1^4, 1\right), \; x_1^7 = x_1^5$.

Седьмой шаг: возникает исход типа а):

$$x \in \left[x_1^4, x_1^5\right), \; l\left(\left[x_1^4, x_1^5\right)\right) = h\Psi_{1,3}(8-7,1) = 2h; \quad (49)$$

возникает исход типа б): $x_1^8 = x_1^6$.

Восьмой шаг: возникает исход типа а):

$$x \in \left[x_1^5, x_1^6\right), \; l\left(\left[x_1^5, x_1^6\right)\right) = h\Psi_{1,3}(8-8,1) = h; \quad (50)$$

возникает исход типа б):

$$x \in \left[x_1^6, 1\right), \; l\left(\left[x_1^6, 1\right)\right) = h\varphi_{1,3}^{3,1,2,4}(8-8,1) = h. \quad (51)$$

Поскольку

$$\begin{aligned} l([0,1]) = {} & l\left(\left[0, x_1^1\right)\right) + l\left(\left[x_1^1, x_1^2\right)\right) + \\ & + l\left(\left[x_1^2, x_1^3\right)\right) + l\left(\left[x_1^3, x_1^4\right)\right) + l\left(\left[x_1^4, x_1^5\right)\right) + \\ & + l\left(\left[x_1^5, x_1^6\right)\right) + l\left(\left[x_1^6, 1\right)\right), \end{aligned} \quad (52)$$

то с учетом соотношений (34)–(51) устанавливаем:

$$\varphi_{1,3}^{3,1,2,4}(8,1) = 8+2+1+1+1+1+1 = 15. \quad (53)$$

Проведя детальный анализ исходов, возникающих для $i = 9$, получаем такое соотношение:

$$\varphi_{1,3}^{3,1,2,4}(9,1) = 26. \quad (54)$$

Значения функции $\varphi_{1,3}^{3,1,2,4}(i,1)$ сведены в табл.4.

Таблица 4

i	1	2	3	4	5	6	7	8	9
$\varphi_{1,3}^{3,1,2,4}(i,1)$	1	1	2	3	3	6	8	15	26

По описанной схеме может быть построен помехоустойчивый алгоритм для любых его параметров и параметров несимметричной нерегулярной виртуальной последовательности.

Литература: 1. *Алипов Н.В., Алипов И.Н., Беляев С.А., Ребезюк Л.Н.* Методы защиты информации в дискретном канале на основе помехоустойчивых к несимметричным нерегулярным виртуальным помехам алгоритмов поиска точки с характерным признаком // Радиоэлектроника и информатика. 2000. № 2. С. 104-111.

Поступила в редколлегию 21.06.2000

Рецензент: д-р техн. наук, проф. Руденко О.Г.

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры проектирования и эксплуатации электронных аппаратов ХТУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств, защита информации. Адрес: Украина, 61089, Харьков, ул. Иртышская, 8, тел. 40-94-94.

Алипов Илья Николаевич, канд. техн. наук, Научные интересы: защита информации. Адрес: Украина, 61089, Харьков, ул. Иртышская,8.

Литвинова Евгения Ивановна, канд. техн. наук, доцент кафедры проектирования и эксплуатации электронных аппаратов ХТУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 61018, Харьков, ул. Деревянко, 48, кв.43., тел. 40-94-94.