УДК 681.3+681.5:007

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ДИСКРЕТНОМ КАНАЛЕ НА ОСНОВЕ УСТОЙЧИВЫХ К СИММЕТРИЧНЫМ НЕРЕГУЛЯРНЫМ ВИРТУАЛЬНЫМ ПОМЕХАМ АЛГОРИТМОВ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ

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

Строятся помехоустойчивые к симметричным нерегулярным виртуальным последовательностям алгоритмы поиска точки с характерным признаком. Такие алгоритмы задают функционирование дискретных автоматов в системах защиты информации.

Известно [1], что виртуальных нерегулярных симметричных последовательностей может быть восемь. Каждая такая последовательность описывается [2] длительностью (l) выброса, интервалом между двумя соседними выбросами (H) и амплитудой импульса (a). В работе рассматриваются так называемые $A_{2,3}$ – последовательности, характерной особенностью которых является то, что параметр l считается случайной величиной, принадлежащей диапазону $[l_1, l_2]$, где l_1, l_2 – соответственно минимальное и максимальное значение этого параметра.

Для решения задачи синтеза подобных алгоритмов воспользуемся подходами, описанными в работах [2–4]. Первоначально приведем решение этой задачи синтеза для случая, когда $l_1 = 1$, $l_2 = 2$, $H > 3$, $k = 1$. Предположим, что i – шаговый алгоритм поиска позволяет разбить первоначальный интервал неопределенности $(0,1)$ на $\varphi_{2,3}^{H,l_1,l_2,a}(i,1)$ равных частей, а $(i-1)$ – шаговый алгоритм – на $\varphi_{2,3}^{H,l_1,l_2,a}(i-1,1)$ равных частей и т.д.

Пусть некоторым образом выбрана точка x_1^1 первого эксперимента. Тогда по итогам первого шага могут быть сформированы исходы типа а) и типа б):

а) $(x+\zeta(t)) \in [0, x_1^1)$; б) $(x+\zeta(t)) \in [x_1^1, 1)$.

На втором шаге алгоритма независимо от исхода применяем стратегию принципа "повторных сравнений" $(x_1^2 = x_1^1)$ (смешанная стратегия принимается тогда, когда $k > 1$). Для исхода типа а) будем иметь:

$a_1)\ (x+\zeta(t)) \in [0, x_1^1)$; $a_2)\ (x+\zeta(t)) \in [x_1^1, 1)$.

Для исхода типа $a_1)$ на третьем шаге снова используем принцип "повторных сравнений": $x_1^3 = x_1^1$. По итогам третьего шага алгоритма могут возникнуть исходы:

$a_{11})\ (x+\zeta(t)) \in [0, x_1^1)$; $a_{12})\ (x+\zeta(t)) \in [x_1^1, 1)$.

Для исхода типа $a_{11})$ характерно то, что эксперимент повторялся три раза и его результаты совпали. Поскольку максимальная длительность импульса помехи равна $2\Delta t$ $(l_2 = 2)$, то однозначно можно утверждать, что $x \in [0, x_1^1)$ и на этом полуоткрытом интервале действует $(i-3)$ – шаговый помехоустойчивый алгоритм, который разобъет его на $\varphi_{2,3}^{3,1,2,a}(i-3,1)$ равных частей. Этим самым устанавливаем истинность соотношения

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

Для исхода типа $a_{12})$ возникшее противоречие свидетельствует только о действии помехи на первом, втором либо третьем шагах алгоритма. На этом основании четвертый эксперимент планируем в точке $x_1^4 = x_1^1$.

При этом по итогам выполнения четвертого шага алгоритма может возникнуть один из исходов:

$a_{121})\ (x+\zeta(t)) \in [0, x_1^1)$; $a_{122})\ (x+\zeta(t)) \in [x_1^1, 1)$.

Для исхода типа $a_{121})$ характерно действие виртуальной помехи на третьем шаге алгоритма. Поскольку действие помехи обнаружено, то на основании принципа "пересечения" устанавливаем:

$x \in [x_1^{1,1}, x_1^1)$, где $x_1^{1,1} = \begin{cases} x_1^1 - ah, & x_1^1 - ah \geq 0; \\ 0 & \text{в противном случае.} \end{cases}$

Поскольку проявление виртуальной помехи обнаружено, то на последующих шагах алгоритма применяется классический алгоритм поиска, особенностью которого является пропуск тех шагов, на которых проявляется виртуальная последовательность (помеха). Полуоткрытый интервал неопределенности $[x_1^{1,1}, x_1^1)$ будет разбит на $\Psi_{2,3}(i-4,1)$ равных частей. Если по итогам выполнения четвертого шага алгоритма возникает исход типа $a_{122})$, то это будет свидетельствовать о действии виртуальной последовательности на первом, втором либо на третьем, четвертом шагах алгоритма. Для устранения этой неоднозначности выполним пятый эксперимент в точке $x_1^5 = x_1^1$.

При этом может возникнуть один из исходов:

$a_{1221})\ (x+\zeta(t)) \in [0, x_1^1)$; $a_{1222})\ (x+\zeta(t)) \in [x_1^1, 1)$.

Исход типа $a_{1221})$ свидетельствует о том, что виртуальная последовательность действовала на третьем и четвертом шагах алгоритма и $x \in [x_1^{1,1}, x_1^1)$.

За оставшиеся $(i-5)$ шагов алгоритма выделенный интервал неопределенности видоизмененным классическим алгоритмом поиска будет разбит на $\Psi_{2,3}(i-5,1)$ равных частей. Для исхода типа a_{1222}) характерно действие помехи на двух первых шагах алгоритма. На этом устанавливаем:

$$x \in \left[x_1^1, x_1^{1,2}\right), \text{ где } x_1^{1,2} = \begin{cases} x_1^1 + ah, x_1^1 + ah \le 1; \\ 1 \text{ в противном случае.} \end{cases}$$

Поскольку действие помехи обнаружено, то выделенный интервал неопределенности за оставшиеся $(i-5)$ шагов будет разбит видоизмененным классическим алгоритмом поиска на $\Psi'_{2,3}(i-5,1)$ равных частей.

Для исхода типа a_{1221}) характерно то, что действие виртуальной последовательности закончилось на четвертом шаге алгоритма. На пятом, шестом и седьмом шагах проявление виртуальной последовательности не будет наблюдаться, затем на восьмом шаге алгоритма она снова проявится (этот шаг пропускают), на девятом шаге ее проявление либо будет наблюдаться, либо не будет. Для устранения этой неоднозначности на девятом шаге следует применить принцип "повторных сравнений". Если при этом возникает противоречие, то действие виртуальной последовательности окончилось, и на последующих $(H-1)$ шагах алгоритма снова применяют классический принцип поиска и т.д.

Поэтому в самом благоприятном случае (длительность импульса виртуальной последовательности в процессе дальнейшего поиска не изменяется и равна $l_1\Delta t$) для функции $\Psi'_{2,3}(i-5,1)$ справедливо соотношение:

$$\Psi'_{2,3}(i-2l_2-1,1) = (k+1)^{(H-1)\alpha_1} * (k+1)^{\alpha_2}, \quad (2)$$

$$\text{где } \alpha_1 = \begin{cases} \dfrac{i-2l_2-1}{H+l_1}, \ (i-2l_2-1)\bmod(H+l_1) = 0; \\ \left]\dfrac{i-2l_2-1}{H+l_1}\right[, \ (i-2l_2-1)\bmod(H+l_1) \ne 0; \end{cases}$$

$$\alpha_2 = \begin{cases} 0, \ (i-2l_2-1)\bmod(H+l_1) = 0 \text{ либо} \\ (i-2l_2-1)\bmod(H+l_1), \ (i-2l_2-1)\bmod(H+l_1) \le l_1; \\ ((i-2l_2-1)\bmod(H+l_1)-l_1), \ (i-2l_2-1)\bmod(H+l_1) > l_1. \end{cases}$$

В самом неблагоприятном случае (длительность импульса виртуальной последовательности в процессе дальнейшего поиска всегда равна $l_2\Delta t$) для функции $\Psi'_{2,3}(i-5,1)$ справедливо соотношение

$$\Psi'_{2,3}(i-2l_2-1,1) = (k+1)^{(H-1)} * (k+1)^{H\bar{\alpha}_1} * (k+1)^{\bar{\alpha}_2}, \quad (3)$$

$$\text{где } \bar{\alpha}_1 = \begin{cases} \dfrac{i-2l_2-H}{H+l_2}, \ (i-2l_2-H)\bmod(H+l_2) = 0; \\ \left]\dfrac{i-2l_2-H}{H+l_2}\right[, \ (i-2l_2-H)\bmod(H+l_2) \ne 0; \end{cases}$$

$$\alpha_2 = \begin{cases} 0, \ (i-2l_2-H)\bmod(H+l_2) = 0 \text{ либо} \\ (i-2l_2-H)\bmod(H+l_2) \le l_2; \\ ((i-2l_2-H)\bmod(H+l_2)-l_2), \\ \qquad (i-2l_2-H)\bmod(H+l_2) > l_2. \end{cases}$$

Аналогично показано, что для функции $\Psi_{2,3}(i-5,1)$ справедливы такие соотношения:

$$\Psi_{2,3}(i-2l_2-1,1) = (k+1)^{H-l_2-1} * (k+1)^{(H-1)\alpha_3} * (k+1)^{\alpha_4}, \quad (4)$$

$$\Psi_{2,3}(i-2l_2-1,1) = (k+1)^{H-l_2-1} * (k+1)^{H\bar{\alpha}_3} * (k+1)^{\bar{\alpha}_4}, \quad (5)$$

$$\text{где } \alpha_3 = \begin{cases} \dfrac{i-l_2-H}{H+l_1}, \ (i-l_2-H)\bmod(H+l_1) = 0; \\ \left]\dfrac{i-l_2-H}{H+l_1}\right[, \ (i-l_2-H)\bmod(H+l_1) \ne 0; \end{cases}$$

$$\alpha_4 = \begin{cases} 0, \ (i-l_2-H)\bmod(H+l_1) = 0 \text{ либо} \\ (i-l_2-H)\bmod(H+l_1) \le l_1; \\ ((i-l_2-H)\bmod(H+l_1)-l_1), \\ \qquad (i-l_2-H)\bmod(H+l_1) > l_1; \end{cases}$$

$$\bar{\alpha}_3 = \begin{cases} \dfrac{i-l_2-H}{H+l_2}, \ (i-l_2-H)\bmod(H+l_2) = 0; \\ \left]\dfrac{i-l_2-H}{H+l_2}\right[, \ (i-l_2-H)\bmod(H+l_2) \ne 0; \end{cases}$$

$$\bar{\alpha}_4 = \begin{cases} 0, \ (i-l_2-H)\bmod(H+l_2) = 0 \text{ либо} \\ (i-l_2-H)\bmod(H+l_2) \le l_2; \\ ((i-l_2-H)\bmod(H+l_2)-l_2), \\ \qquad (i-l_2-H)\bmod(H+l_2) > l_2. \end{cases}$$

В том случае, когда на втором шаге алгоритма возникает исход типа a_2) , это свидетельствует о действии виртуальной последовательности на первом либо втором шаге. По этой причине на третьем шаге применяют принцип "повторных сравнений": $x_1^3 = x_1^1$.

По итогам третьего шага алгоритма может возникнуть один из исходов:

a_{21}) $(x+\zeta(t)) \in \left[0, x_1^1\right)$; a_{22}) $(x+\zeta(t)) \in \left[x_1^1, 1\right)$.

Появление исхода типа a_{21}) свидетельствует о действии виртуальной последовательности на втором шаге алгоритма. На этом основании формируют новый полуоткрытый интервал неопределенности $x \in \left[x_1^{1,1}, x_1^1\right)$, который будет разбит на $\Psi_{2,3}(i-3,1)$ равных частей.

Для исхода a_{22}) нельзя однозначно установить: на каких шагах виртуальная последовательность действовала. По этой причине на четвертом шаге применяем принцип "повторных сравнений": $x_1^4 = x_1^1$.

В результате выполнения четвертого шага алгоритма может появиться один из исходов:

$а_{221})\ (x+\zeta(t))\in\left[0, x_1^1\right);\ а_{222})\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Для исхода типа $а_{221})$ характерно действие виртуальной последовательности на втором и третьем шагах алгоритма, для исхода типа $а_{222})$ – на первом шаге алгоритма. На этом основании соответственно устанавливаем истинность соотношений : $x\in\left[x_1^{1,1}, x_1^1\right);\ x\in\left[x_1^1, x_1^{1,2}\right).$

Каждый из этих полуоткрытых интервалов неопределенности будет соответственно разбит на $\Psi_{2,3}(i-4,1)$ и $\Psi'_{2,3}(i-4,1)$ равных частей.

Поскольку оценкой алгоритма является количество равных частей, на которые в наихудшем случае разбивается вновь сформированный полуоткрытый интервал неопределенности, то для полуоткрытого интервала неопределенности $\left[x_1^{1,1}, x_1^1\right)$ будем иметь:

$$\min\left\{\Psi_{2,3}(i-3,1), \Psi_{2,3}(i-4,1), \Psi_{2,3}(i-5,1)\right\} = \Psi_{2,3}(i-5,1). \quad (6)$$

Для полуоткрытого интервала неопределенности $\left[x_1^1, x_1^{1,2}\right)$ будет справедлива такая оценка:

$$\min\left\{\Psi'_{2,3}(i-4,1), \Psi'_{2,3}(i-5,1)\right\} = \Psi'_{2,3}(i-5,1). \quad (7)$$

По этой причине нецелесообразно синтезировать выражения для функции $\Psi_{2,3}(i-3,1)$, $\Psi_{2,3}(i-4,1)$, $\Psi'_{2,3}(i-4,1)$.

В том случае, когда на первом шаге алгоритма поиска возникает исход типа б), на втором шаге алгоритма применяют принцип "повторных сравнений": $x_1^2 = x_1^1$.

По итогам выполнения второго шага алгоритма может сформироваться один из исходов:

$б_1)\ (x+\zeta(t))\in\left[0, x_1^1\right);\ б_2)\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Исход типа $б_1)$ свидетельствует о действии виртуальной последовательности на первом либо на втором шаге алгоритма. Для устранения неоднозначности на третьем шаге повторяем эксперимент $\left(x_1^3 = x_1^1\right)$. При этом может быть сформирован один из исходов:

$б_{11})\ (x+\zeta(t))\in\left[0, x_1^1\right);\ б_{12})\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Для исхода типа $б_{11})$ повторяют эксперимент $\left(x_1^4 = x_1^1\right)$ и получают один из исходов:

$б_{111})\ (x+\zeta(t))\in\left[0, x_1^1\right);\ б_{112})\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Для исхода типа $б_{111})$ характерно действие виртуальной последовательности на первом шаге алгоритма. На этом основании подтверждается истинность соотношения $x\in\left[x_1^{1,1}, x_1^1\right)$.

Этот полуоткрытый интервал неопределенности будет разбит на $\Psi'_{2,3}(i-4,1)$ равных частей. Для исхода $б_{112})$ характерно действие виртуальной последовательности на втором и третьем шагах алгоритма. Это устанавливает истинность соотношения $x\in\left[x_1^1, x_1^{1,2}\right)$.

Вновь сформированный полуоткрытый интервал неопределенности за оставшиеся $(i-4)$ шага видоизмененным классическим алгоритмом поиска будет разбит на $\Psi_{2,3}(i-4,1)$ равных частей.

Для исхода типа $б_{1,2})$ характерно действие виртуальной последовательности на втором шаге алгоритма, что подтверждает истинность соотношения $x\in\left[x_1^1, x_1^{1,2}\right)$. Этот полуоткрытый интервал за оставшиеся $(i-4)$ шагов апгоритма будет разбит на $\Psi_{2,3}(i-4,1)$ равных частей.

Если в процессе поиска возникнет исход типа $б_2)$, то вновь повторяют эксперимент $\left(x_1^3 = x_1^1\right)$.

При этом формируется один из исходов:

$б_{21})\ (x+\zeta(t))\in\left[0, x_1^1\right),\ б_{22})\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Для исхода типа $б_{21})$ характерно действие виртуальной последовательности на первом, втором либо третьем шагах алгоритма. В этом случае повторяем эксперимент $\left(x_1^4 = x_1^1\right)$.

По итогам выполнения четвертого шага алгоритма может возникнуть один из исходов:

$б_{211})\ (x+\zeta(t))\in\left[0, x_1^1\right),\ б_{212})\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Для исхода типа $б_{211})$ повторяем эксперимент $\left(x_1^5 = x_1^1\right)$, в результате которого может быть сформирован один из исходов:

$б_{2111})\ (x+\zeta(t))\in\left[0, x_1^1\right),\ б_{2112})\ (x+\zeta(t))\in\left[x_1^1, 1\right).$

Для исхода типа $б_{2111})$ характерно действие виртуальной последовательности на первом и втором шагах алгоритма. По этой причине устанавливаем истинность соотношения: $x\in\left[x_1^{1,1}, x_1^1\right)$.

Этот полуоткрытый интервал неопределенности будет разбит на $\Psi_{2,3}(i-5,1)$ равных частей.

Для исхода типа $б_{2112})$ характерно действие виртуальной последовательности на третьем и четвертом шагах алгоритма. Это устанавливает истинность соотношения: $x\in\left[x_1^1, x_1^{1,2}\right)$.

Если возникает исход типа $б_{212})$, то это свидетельствует о действии виртуальной последовательности на третьем шаге алгоритма и истинности выражения $x\in\left[x_1^1, x_1^{1,2}\right)$.

Этот полуоткрытый интервал неопределенности за оставшиеся $(i-4)$ шага алгоритма будет разбит на $\Psi_{2,3}(i-4,1)$ равных частей.

Для исхода типа $б_{22}$) характерно то, что результаты трех экспериментов совпадают и это свидетельствует о том, что виртуальная последовательность на первых трех шагах не наблюдалась и $x \in \left[x_1^1, 1\right]$.

Этот отрезок за оставшиеся $(i-3)$ шага алгоритма помехоустойчивым алгоритмом будет разбит на $\varphi_{2,3}^{3,1,2,a}(i-3,1)$ равных частей, следовательно,

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

Соотношения (1), (8) устанавливают, что, с одной стороны, полуоткрытые интервалы $\left[0, x_1^1\right), \left[x_1^1, 1\right)$ будут разбиты на $\varphi_{2,3}^{3,1,2,a}(i-3,1)$ равные части, каждая из которых имеет длину h, где $h = x_1^1 / \varphi_{2,3}^{3,1,2,a}(i-3,1)$. С другой стороны, полуоткрытые интервалы неопределенности $\left[x_1^{1,1}, x_1^1\right)$, $\left[x_1^1, x_1^{1,2}\right)$, принадлежащие соответственно полуоткрытым интервалам $\left[0, x_1^1\right)$, $\left[x_1^1, 1\right)$, будут разбиты на $\Psi_{2,3}(i-5,1)$ либо на $\Psi'_{2,3}(i-5,1)$ равные части, каждая из которых будет иметь длину h^1, h^2, где $h^1 = \left(x_1^1 - x_1^{1,1}\right) / \Psi_{2,3}(i-5,1)$; $h^2 = \left(x_1^{1,2} - x_1^1\right) / \Psi'_{2,3}(i-5,1)$.

Поскольку оценкой алгоритма выступает количество равных частей, на которые разбивается вновь выделенный полуоткрытый интервал неопределенности, либо длина каждого такого интервала, полученного на последнем шаге алгоритма, то, исходя из наихудшего случая, следует истинность соотношения:

$$\varphi_{2,3}^{3,1,2,a}(i,1) = 2\overline{\varphi}_{2,3}^{3,1,2,a}(\alpha,1), \qquad (9)$$

где $\overline{\varphi}_{2,3}^{3,1,2,a}(\alpha,1) = \begin{cases} \varphi_{2,3}^{3,1,2,a}(i-3,1), h \ge h_1, h_1 \ge h_2; \\ \Psi_{2,3}(i-5,1), h < h_1, h_1 \ge h_2; \\ \Psi'_{2,3}(i-5,1), h < h_1, h_1 < h_2. \end{cases}$

Соотношение (9) для произвольных значений параметров l_1, l_2, H запишется в таком виде:

$$\varphi_{2,3}^{H,l_1,l_2,a}(i,1) = 2\overline{\varphi}_{2,3}^{H,l_1,l_2,a}(\alpha,1), \qquad (10)$$

где

$$\overline{\varphi}_{2,3}^{H,l_1,l_2,a}(\alpha,1) = \begin{cases} \varphi_{2,3}^{H,l_1,l_2,a}(i-l_2-1,1), h \ge h_1, h_1 \ge h_2; \\ \Psi_{2,3}(i-2l_2-1,1), h < h_1, h_1 \ge h_2; \\ \Psi'_{2,3}(i-2l_2-1,1), h < h_1, h_1 < h_2. \end{cases}$$

Анализ всевозможных исходов, возникающих в процессе поиска точки с характерным признаком, позволяет методом индукции по i синтезировать алгоритм поиска в условиях воздействия нерегулярной симметричной виртуальной последовательности для случая, когда $k = 1$.

Рассмотрим более общий случай, для которого характерно, что $l_1 < l_2$, $k = 3$, $H > l_2$, амплитуда помехи – некоторое положительное число «a».

Пусть некоторым образом выбраны точки первого эксперимента x_1^1, x_2^1, x_3^1. Тогда по итогам выполнения первого шага алгоритма может возникнуть один из исходов:

a_0) $(x + \zeta(t)) \in \left[0, x_1^1\right)$;

a_1) $(x + \zeta(t)) \in \left[x_{q_1}^1, x_{q_1+1}^1\right)$, $q_1 = 1,2$;

a_2) $(x + \zeta(t)) \in \left[x_3^1, 1\right]$.

Рассмотрим первоначально решение исхода типа a_1). Для него a_1) при $q_1 = 1$ на втором шаге следует применить смешанную стратегию:

$x_1^2 = x_{q_1}^1$; $x_3^2 = x_{q_1+1}^1$; $x_2^2 \in \left(x_{q_1}^1, x_{q_1+1}^1\right)$.

В результате выполнения второго шага алгоритма может появиться один из исходов:

$в_1$) $(x + \zeta(t)) < x_1^1$;

$в_2$) $(x + \zeta(t)) \in \left[x_{q_2}^2, x_{q_2+1}^2\right)$, $q_2 = 1,2$;

$в_3$) $(x + \zeta(t)) > x_3^1$.

Для исхода типа $в_1$) характерно то, что виртуальная последовательность могла действовать либо на первом шаге алгоритма, либо на втором. В такой ситуации однозначно можно утверждать, что $x \in \left[x_1^{1,1}, x_1^{1,2}\right)$ и стратегия поиска будет заключаться в том, что на последующих $(l_1 - 1)$ шагах алгоритма в полуоткрытом интервале неопределенности $\left[x_1^{1,1}, x_1^1\right)$ применяется классический алгоритм поиска, а начиная с $(l_1 + 2)$-го шага – смешанная стратегия: первые $(k-1)$ точек эксперимента размещаются во вновь выделенном полуоткрытом интервале, а последняя точка выбирается на основании соотношения $x_k^{l_1+2} = x_1^1$.

При этом если $(x + \zeta(t)) < x_1^1$, то по такой же схеме выполняется $(l_1 + 3)$-й шаг алгоритма и т.д. Если же $(x + \zeta(t)) > x_1^1$, то это будет свидетельствовать о том, что виртуальная последовательность начала проявляться на втором шаге и ее действие закончилось на предыдущем шаге. Поскольку проявление помехи обнаружено, то устанавливаем: $x \in \left[\begin{matrix} =1,2 \\ x_1^1, x_1 \end{matrix}\right)$,

где $\begin{matrix} =1,2 \\ x_1 \end{matrix} = \begin{cases} x_1^1 + ah, \; x_1^1 + ah \le x_2^1; \\ x_2^1, \; x_1^1 + ah > x_2^1. \end{cases}$

Выделенный полуоткрытый интервал неопределенности будет разбит видоизмененным классическим алгоритмом поиска на $\Psi'_{2,3}(i-j,k)$ равных частей (j – номер шага, на котором соотношение $(x + \zeta(t)) > x_1^1$ стало истинным).

Если же соотношение $(x+\zeta(t)) < x_1^1$ выполняется на $(l_1+3),(l_1+4),\ldots(l_2+2)$-х шагах алгоритма, то это свидетельствует о действии виртуальной последовательности на первом шаге алгоритма и эта последовательность на последующих $(H-l_2-1)$ шагах алгоритма еще не будет проявляться, затем снова проявится и т.д. В этом случае выделенный на (l_2+2)-м шаге алгоритма полуоткрытый интервал неопределенности видоизмененным классическим алгоритмом поиска будет разбит на $\Psi_{2,3}(i-l_2-2,k)$ равных частей.

Для исхода типа $в_3$) характерно то, что и для исхода типа $в_1$) : виртуальная последовательность могла действовать либо на первом шаге алгоритма, либо на втором. В нашей ситуации однозначно можно утверждать, что $x \in \left[x_2^{1,1}, x_2^{1,2}\right)$.

Стратегия поиска в этом случае аналогична стратегии поиска для исхода типа $в_1$) : на последующих (l_1-1) шагах алгоритма в полуоткрытом интервале неопределенности $\left[x_2^1, x_2^{1,2}\right)$ принимается классический алгоритм поиска, начиная с (l_1+2)-го шага алгоритма предпринимают смешанную стратегию, отличающуюся от ранее рассмотренной для исхода типа $в_1$) тем, что первая точка эксперимента выбирается согласно соотношению $x_1^{l_1+2} = x_2^2$, а остальные – в выделенном на (l_2+1)-м шаге алгоритма полуоткрытом интервале неопределенности.

По итогам (l_1+2)-го шага алгоритма могут быть сформированы исходы:

$д_1$) $(x+\zeta(t)) \geq x_2^2$;

$д_2$) $(x+\zeta(t)) \leq x_2^2$.

Если возникает исход типа $д_1$), то точки эксперимента на $(l_1+3),(l_1+4),\ldots$ шагах выделяются описанным образом. Если же возникает исход типа $д_2$), то это будет свидетельствовать о том, что виртуальная последовательность действовала, начиная со второго шага и кончая предыдущим шагом. На этом основании устанавливаем:

$$x \in \left[\begin{matrix}=2,1\\ x_2\end{matrix}, x_2^2\right), \text{ где } \begin{matrix}=2,1\\ x_2\end{matrix} = \begin{cases} x_2^2 - ah, & x_2^2 - ah \leq x_1^2; \\ x_1^2 & \text{в противном случае}. \end{cases}$$

Выделенный полуоткрытый интервал неопределенности будет за оставшиеся $(i-j)$ шагов алгоритма (j – номер шага алгоритма, на котором был сформирован в первый раз исход типа $д_2$)) разбит видоизмененным классическим алгоритмом поиска на $\Psi'_{2,3}(i-j,3)$ равные части.

Если исход типа $д_1$) появляется на $(l_1+3),(l_1+4),\ldots(l_2+2)$-х шагах алгоритма, то это будет свидетельствовать о том, что виртуальная последовательность действовала на первом шаге алгоритма, а на последующих $(H-l_2-2)$ шагах алгоритма она также не будет проявляться, затем снова проявится на последующих l_3-х шагах алгоритма $(l_3 \in [l_1, l_2])$.

Выделенный на (l_2+2)-м шаге полуоткрытый интервал неопределенности за оставшиеся $(i-l_2-2)$ шагов алгоритма будет разбит на $\Psi_{2,3}(i-l_2-2,3)$ равные части.

В том случае, когда по итогам выполнения второго шага формируется исход типа $в_2$), то на основании принципа пересечения устанавливают:

$$x \in \left[x_{q_2}^{2,1}, x_{q_2+1}^{2,2}\right), \; q_2 = 1,2, \qquad (11)$$

где $$x_{q_2}^{2,1} = \begin{cases} x_{q_2}^2 - ah, & x_{q_2}^2 - ah \leq x_{q_1}^{1,1}; \\ x_{q_1}^{1,1} & \text{в противном случае}; \end{cases}$$

$$x_{q_2+1}^{2,2} = \begin{cases} x_{q_2+1}^2 + ah, & x_{q_2+1}^2 + ah \leq x_{q_1+1}^{1,2}; \\ x_{q_1+1}^{1,2} & \text{в противном случае}; \end{cases}$$

и применяют известным способом смешанную стратегию:

$$x_1^3 = x_{q_2}^2; \; x_{q_3}^3 \in \left(x_{q_2}^2, x_{q_2+1}^2\right); \; q_3 = 2; \; x_3^3 = x_{q_2+1}^2.$$

Пусть исход типа $в_2$) формировался на первых j-х шагах алгоритма. Тогда при $j < (l_2+1)$ к вновь выделенному полуоткрытому интервалу неопределенности применяют смешанную стратегию поиска и процесс поиска повторяется. В том случае, когда $j = (l_2+1)$, для исхода типа $в_2$) устанавливаем истинность соотношения: $x \in \left[x_{q(j-1)}^j, x_{q(j-1)+1}^j\right)$.

И на этом полуоткрытом интервале действует $(i-j)$-шаговый помехоустойчивый алгоритм поиска, который разобъет интервал на $\varphi_{2,3}^{H,l_1,l_2,a}(i-j,3)$ равные части. Полуоткрытый интервал неопределенности, сформированный на первом шаге алгоритма для исхода типа a_1), будет разбит на $\varphi^*_{2,3}(i-1,3)$ равные части, причем для функции $\varphi^*_{2,3}(i-1,3)$ справедливо соотношение

$$\varphi^*_{2,3}(i-1,3) = (k-1)^{j-1} \varphi_{2,3}^{H,l_1,l_2,a}(i-j,3). \qquad (12)$$

В том случае, когда величина амплитуды выброса виртуальной последовательности ah равна либо больше длины исходного интервала неопределенности, соотношение (12) можно записать в другой форме. Действительно, в этом случае появление исхода типа $в_2$) на j-м шаге алгоритма ($j = l_2+1$)

будет означать, что поиск точки с характерным признаком осуществлялся в интервале времени, совпавшем с паузой между двумя соседними выбросами виртуальной $A_{2,3}$ – последовательности. По этой причине на последующих шагах алгоритма применяется смешанная стратегия классического алгоритма поиска.

При этом появление исходов типа $в_1)$, $в_3)$ будет означать начало действия следующего выброса виртуальной последовательности. В этой ситуации последующие $(l_1 - 1)$ шагов алгоритма пропускаются, а на следующих $(l_2 - l_1)$ шагах алгоритма применяется смешанная стратегия:

для исхода типа $в_1)$

$$x_1^{j+z} = x_{q_{j+z-1}}^{j+z-1};\ x_{q_{j+z}}^{j+z} \in \left(x_{q_{j+z-1}}^{j+z-1}, x_{q_{j+z-1}+1}^{j+z-1} \right); \quad (13)$$

$$q_{j+z} = \overline{2,k};$$

для исхода типа $в_3)$

$$x_k^{j+z} = x_{q_j+1}^{j};\ x_{\rho_{j+z}}^{j+z} \in \left(x_{\rho_{j+z-1}}^{j+z-1}, x_{\rho_{j+z-1}+1}^{j+z-1} \right);$$

$$\rho_{j+z} = \overline{1,k-1},$$

где $\left[x_{\rho_{j+z-1}}^{j+z-1}, x_{\rho_{j+z-1}+1}^{j+z-1} \right)$ – полуоткрытый интервал неопределенности, выделенный на $(j+z-1)$-м шаге алгоритма поиска.

Такие стратегии принимаются до тех пор, пока не станет истинным одно из соотношений:

для исхода $в_1)$: $x + \zeta(t) > x_{q_{j+z-1}}^{j+z-1}$;

для исхода $в_3)$: $x + \zeta(t) < x_{q_{j+z-1}+1}^{j+z-1}$.

Истинность этих соотношений будет означать, что проявление очередного выброса виртуальной последовательности окончилось на z-м шаге и на последующих $(H-1)$-х шагах следует применить стратегию классического алгоритма поиска, необходимо пропустить l_1 шагов, затем на последующих $(l_2 - l_1)$ шагах алгоритма применить стратегию поиска, задаваемую соотношением (13).

В том случае, когда по итогам выполнения $(j+1)$-го шага алгоритма формируется исход типа $в_2)$, то и на последующих шагах снова применяется смешанная стратегия классического алгоритма поиска. Пусть исход типа $в_2)$ возникает $(j+z)$ раз и при этом $j+z=H$. Тогда, как это следует из определения виртуальной последовательности, на следующем шаге алгоритма начнется проявление очередного выброса виртуальной последовательности. На этом и последующих шагах алгоритма применяется видоизмененная стратегия классического алгоритма поиска (стратегия с пропусками тех шагов, на которых виртуальная последовательность проявляется).

Такой алгоритм поиска точки с характерным признаком разобьет полуоткрытый интервал неопределенности, выделенный на j-м шаге алгоритма, для исходов $в_1)$, $в_3)$ на $\overline{\Psi}_{2,3}(i-j,k)$, а для исхода $в_2)$ – $\overline{\overline{\Psi}}_{2,3}(i-j,k)$ равных частей.

Для функции $\overline{\Psi}_{2,3}(i-j,k)$ в наихудшем случае будет справедливым такое соотношение:

$$\overline{\Psi}_{2,3}(i-j,k) = (k-1)^{z-1} * (k+1)^{\gamma H} * (k+1)^{\gamma 1},$$

где

$$\gamma = \begin{cases} \dfrac{i-j-z-l_2+1}{l_2+H}, (i-j-z-l_2+1) \bmod (l_2+H) = 0; \\ \left] \dfrac{i-j-z-l_2+1}{l_2+H} \right[, (i-j-z-l_2+1) \bmod (l_2+H) \neq 0; \end{cases}$$

$$\gamma_1 = \begin{cases} 0, (i-j-z-l_2+1) \bmod (l_2+H) = 0; \\ (i-j-z-l_2+1) \bmod (l_2+H), \\ \qquad (i-j-z-l_2+1) \bmod (l_2+H) \le H; \\ H, (i-j-z-l_2+1) \bmod (l_2+H) > H. \end{cases}$$

Полуоткрытый интервал неопределенности, сформированный на первом шаге алгоритма для исхода типа $a_1)$, в этом случае будет разбит на $\varphi_{2,3}^{**}(i-1,k)$ равных частей.

Для этой функции будет истинным такое соотношение:

$$\varphi_{2,3}^{**}(i-1,k) = (k-1)^{j-1} \overline{\Psi}_{2,3}(i-j,k). \quad (14)$$

Для функции $\overline{\overline{\Psi}}_{2,3}(i-j,k)$ в наихудшем случае справедливо такое соотношение:

$$\overline{\overline{\Psi}}_{2,3}(i-j,k) = (k-1)^{z} (k+1)^{\gamma_2 H} (k+1)^{\gamma_3},$$

где $\gamma_2 = \begin{cases} \dfrac{i-j-z}{l_2+H}, (i-j-z) \bmod (l_2+H) = 0; \\ \left] \dfrac{i-j-z}{l_2+H} \right[, (i-j-z) \bmod (l_2+H) \neq 0; \end{cases}$

$$\gamma_3 = \begin{cases} 0, (i-j-z) \bmod (l_2+H) = 0 \text{ либо} \\ (i-j-z) \bmod (l_2+H) \le l_2; \\ (i-j-z) \bmod (l_2+H) - l_2, \\ \qquad (i-j-z) \bmod (l_2+H) > l_2. \end{cases}$$

Полуоткрытый интервал неопределенности, сформированный на первом шаге алгоритма для исхода типа $a_1)$, будет разбит на $\varphi_{2,3}^{***}(i-1,k)$ равных частей.

Для этой функции справедливым будет такое соотношение:

$$\varphi_{2,3}^{***}(i-1,k) = (k-1)^{j-1} \overline{\overline{\Psi}}_{2,3}(i-j,k). \quad (15)$$

Итак, если для $j=(l_2+1)$ продолжать поиск точки с характерным признаком в полуоткрытом интер-

вале неопределенности, выделенном на j-м шаге алгоритма, то его можно разбить на $\overline{\Psi}_{2,3}(i-j,k)$ либо на $\overline{\overline{\Psi}}_{2,3}(i-j,k)$ равных частей.

На основании минимаксной стратегии поиска устанавливаем:

$$\varphi^{*}_{2,3}(i-j,k)=\min\left\{\overline{\Psi}_{2,3}(i-j,k),\overline{\overline{\Psi}}_{2,3}(i-j,k)\right\}. \quad (16)$$

Таким образом, в самом наихудшем случае, продолжая процесс поиска, полуоткрытый интервал неопределенности, выделенный на j-м шаге алгоритма, будет разбит на $\varphi^{*}_{2,3}(i-j,k)$ равных частей.

Очевидно, чтобы принять решение о продолжении поиска, необходимо, чтобы выполнялось условие

$$\varphi^{**}_{2,3}(i-j,k)>\varphi^{H,l_1,l_2,a}_{2,3}(i-j,k). \quad (17)$$

С учетом соотношений (12), (16), (17) можно утверждать, что полуоткрытый интервал неопределенности, выделенный на первом шаге для исхода типа a_1), будет разбит на $\overline{\overline{\Psi}}_{2,3}(i-1,k)$ равных частей. Для этой функции справедливо такое выражение:

$$\overline{\overline{\Psi}}_{2,3}(i-1,3)=(k-1)^{j-1}\max\left\{\varphi^{H,l_1,l_2,a}_{2,3}(i-j,k),\min\left\{\overline{\Psi}_{2,3}(i-j,k),\overline{\overline{\Psi}}_{2,3}(i-j,k)\right\}\right\} \quad (18)$$

Нетрудно заметить, что соотношение (18) имеет смысл только для значений $k\ge 2$.

Пусть $j<(l_2+1)$ и на этом шаге возникает исход типа $в_1$). Тогда на основании принципа "пересечения" устанавливаем: $x\ge x^{j-1,1}_{q_{j-1}}$, где

$$x^{j-1,1}_{q_{j-1}}=\begin{cases}x^{j-1}_{q_{j-1}}-ah,\ x^{j-1}_{q_{j-1}}-ah\ge x^{j-2,1}_{q_{j-2}};\\ x^{j-2,1}_{q_{j-2}}\ \text{в противном случае,}\end{cases}$$

$\left[x^{j-1}_{q_{j-1}},x^{j-1}_{q_{j-1}+1}\right)$ – интервал неопределенности относительно точки $(x+\zeta(t))$, выделенной на $(j-1)$-м шаге алгоритма. В полуоткрытом интервале $\left[x^{j-1,1}_{q_{j-1}},x^{j-1}_{q_{j-1}}\right)$ применяем разработанную для исхода типа $в_1$) стратегию поиска: на последующих (l_1-1) шагах алгоритма в полуоткрытом интервале $\left[x^{j-1,1}_{q_{j-1}},x^{j-1}_{q_{j-1}}\right)$ применяется классический апгоритм поиска, начиная с $(j+l_1)$ шага алгоритма применяется смешанная стратегия: первые $(k-1)$ точек эксперимента размещаются во вновь выделенном полуоткрытом интервале, последняя точка выбирается исходя из соотношения

$$x^{j+l_1}_{k}=x^{j-1}_{q_{j-1}}. \quad (19)$$

При этом если выполняется соотношение

$$x+\zeta(t)\le x^{j-1}_{q_{j-1}}, \quad (20)$$

то и на последующих шагах алгоритма $(j+l_1+1)$, $(j+l_1+1),\dots,(j+l_2-1)$ точки эксперимента выбираются по описанной схеме ($(k-1)$ точка размещается во вновь выделенном полуоткрытом интервале неопределенности, а последняя – в точке $x^{j-1}_{q_{j-1}}$).

Самым наихудшим случаем будет тот, для которого на всех последующих шагах алгоритма вплоть до $(j+l_2-1)$-го шага будет выполняться соотношение (20). В этой ситуации следующий $(j+l_2)$-й шаг снова выполняют по схеме ($(k-1)$, точку размещают во вновь выделенном полуоткрытом интервале, а последнюю – в точке $x^{j-1}_{q_{j-1}}$).

Если по итогам выполнения последнего шага алгоритма устанавливается ложность соотношения (20), то это будет свидетельствовать о действии виртуальной последовательности на j-м, $(j+1)$, ..., $(j+l_2-1)$ шагах алгоритма; начиная с $(j+l_2)$-го шага виртуальная последовательность не будет проявляться на последующих H шагах алгоритма, затем снова проявится на следующих l_3-х шагах алгоритма ($l_3\in[l_1,l_2]$) и т.д. На основании принципа "пересечения" устанавливаем $x\in\left[x^{j-1}_{q_{j-1}},x^{=j-1}_{q_{j-1}}\right)$,

где $x^{=j-1}_{q_{j-1}}=\begin{cases}x^{j-1}_{q_{j-1}}-ah,\ x^{j-1}_{q_{j-1}}-ah\le x^{j-1}_{q_{j-1}+1};\\ x^{j-1}_{q_{j-1}+1}\ \text{в противном случае.}\end{cases}$

Этот полуоткрытый интервал неопределенности будет разбит на $\Psi'_{2,3}(i-j-l_2,k)$ равных частей.

В самом наихудшем случае для функции $\Psi'_{2,3}(i-j-l_2,k)$ справедливо соотношение:

$$\Psi'_{2,3}(i-j-l_2,k)=(k+1)^{H-1}(k+1)^{H\alpha_5}(k+1)^{\overline{\alpha}_5}, \quad (21)$$

где

$$\alpha_5=\begin{cases}\dfrac{i-j-l_2-H+1}{l_2+H},\ (i-j-l_2-H+1)\bmod(l_2+H)=0;\\ \left]\dfrac{i-j-l_2-H+1}{l_2+H}\right[,\ (i-j-l_2-H+1)\bmod(l_2+H)\ne 0;\end{cases}$$

$$\overline{\alpha}_5=\begin{cases}0,\ (i-j-l_2-H+1)\bmod(l_2+H)=0\ \text{либо}\\ (i-j-l_2-H+1)\bmod(l_2+H)\le l_2;\\ ((i-j-l_2-H+1)\bmod(l_2+H)-l_2),\\ \qquad (i-j-l_2-H+1)\bmod(l_2+H)>l_2.\end{cases}$$

Проведенный анализ возможных исходов, возникающих в процессе поиска, позволяет заключить, что полуоткрытый интервал неопределенности $\left[x^1_1,x^1_2\right)$ за $(j-1)$ первых шагов в результате применения смешанной стратегии будет разбит на $(k-1)^{j-2}$ равных частей; в свою очередь каждый из полуоткрытых интервалов на $(j-1)$-м шаге алгоритма

будет в наихудшем случае разбит на $\Psi'_{2,3}(i-j-l_2,k)$ равных частей. Поэтому на основании соотношения (21) устанавливаем справедливость выражения

$$l\left(\left[x_1^1, x_2^1\right)\right) = h(k-1)^{j-2}\,\Psi'_{2,3}(i-j-l_2,k). \qquad (22)$$

Если по итогам выполнения $(j+l_2)$-го шага алгоритма будет установлена истинность соотношения (20), то это будет свидетельствовать о проявлении виртуальной последовательности на первых $(j-1)$ шагах алгоритма и на этом основании устанавливаем истинность соотношения $x \in \left[x_{q_{j-1}}^{j-1,1}, x_{q_{j-1}}^{j-1}\right)$.

На последующих шагах алгоритма в полуоткрытом интервале, выделенном на $(j+l_2)$-м шаге алгоритма, применяем видоизмененный классический алгоритм поиска: на последующих $(H-l_2-1)$ шагах алгоритма применяем классический алгоритм поиска, затем пропускаем l_3 шагов алгоритма и т.д. Этот полуоткрытый интервал неопределенности будет разбит на $\Psi_{2,3}(i-j-l_2,k)$ равных частей.

Для этой функции в самом наихудшем случае будет иметь место такое соотношение:

$$\Psi_{2,3}(i-j-l_2,k) = (k+1)^{H-l_2-1}(k+1)^{H\alpha_6}(k+1)^{\overline{\alpha}_6}, \qquad (23)$$

где $\alpha_6 = \begin{cases} \dfrac{i-j-H+1}{l_2+H}, (i-j-H+1)\bmod(l_2+H)=0; \\ \left]\dfrac{i-j-H+1}{l_2+H}\right[, (i-j-H+1)\bmod(l_2+H)\neq 0; \end{cases}$

$$\overline{\alpha}_6 = \begin{cases} 0, (i-j-H+1)\bmod(l_2+H)=0 \text{ либо} \\ (i-j-H+1)\bmod(l_2+H)\le l_2; \\ ((i-j-H+1)\bmod(l_2+H)-l_2), \\ \qquad (i-j-H+1)\bmod(l_2+H)>l_2. \end{cases}$$

Как уже известно, при возникновении на j-м шаге алгоритма исхода типа $в_1$) на последующих (l_1-1) шагах применяется классический алгоритм поиска, затем, начиная с $(j+l_1)$-го шага и кончая $(j+l_2)$-м шагом алгоритма, применяется смешанная стратегия. В результате такой комбинации стратегий поиска полуоткрытый интервал неопределенности $\left[x_{q_{j-1}}^{j-1,1}, x_{q_{j-1}}^{j-1}\right)$ будет разбит на $(k+1)^{(l_1-1)}k^{(l_2-l_1+1)}$ равных частей.

С учетом соотношения (23) устанавливаем справедливость выражения:

$$l\left(\left[x_{q_{j-1}}^{j-1,1}, x_{q_{j-1}}^{j-1}\right)\right) = h_1(k+1)^{(l_1-1)}k^{(l_2-l_1+1)}\Psi_{2,3}(i-j-l_2,k). \qquad (24)$$

Пусть $j<(l_2+1)$ и по итогам выполнения j-го шага возникает исход типа $в_3$). Тогда на основании принципа "пересечения" устанавливаем: $x \le x_{q_{j-1}+1}^{j-1,2}$,

где $x_{q_{j-1}+1}^{j-1,2} = \begin{cases} x_{q_{j-1}+1}^{j-1}+ah,\ x_{q_{j-1}+1}^{j-1}+ah \le x_{q_{j-2}}^{j-2,2}; \\ x_{q_{j-2}}^{j-2,2} \text{ в противном случае.} \end{cases}$

В полуоткрытом интервале $\left[x_{q_{j-1}+1}^{j-1}, x_{q_{j-1}+1}^{j-1,2}\right)$ применяем известную стратегию поиска: на последующих (l_1-1)-м шагах алгоритма используется стратегия классического алгоритма поиска, затем, начиная с $(j+l_1)$-го шага – смешанная стратегия поиска, для которой характерно то, что первой точкой эксперимента является точка $x_{q_{j-1}+1}^{j-1}$ и остальные $(k-1)$ точки эксперимента размещаются во вновь сформированном на $(j-l_1+1)$ шаге алгоритма полуоткрытом интервале неопределенности.

При этом могут возникать такие исходы:

c_1) $x+\zeta(t) > x_{q_{j-1}+1}^{j-1}$; c_2) $x+\zeta(t) < x_{q_{j-1}+1}^{j-1}$.

Самым наихудшим случаем окажется тот, для которого на всех последующих шагах алгоритма вплоть до $(j+l_2-1)$-го шага будет появляться исход типа c_1). В такой ситуации и на $(j+l_2)$-м шаге алгоритма снова применяют смешанную стратегию.

При этом если по итогам выполнения $(j+l_2)$-го шага алгоритма будет сформирован исход типа c_2), то это будет свидетельствовать о действии виртуальной последовательности на j-м, $(j+1)$, ..., $(j+l_2-1)$ шагах алгоритма. Поэтому если действие виртуальной последовательности было обнаружено на $(j+l_2)$-м шаге алгоритма, то по определению эта последовательность не будет проявляться еще на $(H-1)$ шаге, затем снова проявится и т.д.

По этой причине на последующих шагах алгоритма применяется видоизмененный классический алгоритм поиска. В такой ситуации на основании принципа "пересечения" формируем полуоткрытый интервал неопределенности относительно точки с характерным признаком: $x \in \left[x_{q_{j-1}+1}^{=j-1}, x_{q_{j-1}+1}^{j-1}\right)$,

где $x_{q_{j-1}+1}^{=j-1} = \begin{cases} x_{q_{j-1}+1}^{j-1}-ah,\ x_{q_{j-1}+1}^{j-1}-ah \le x_{q_{j-1}}^{j-1}; \\ x_{q_{j-1}}^{j-1} \text{ в противном случае.} \end{cases}$

Этот полуоткрытый интервал неопределенности за оставшиеся $(i-j-l_2)$ шагов алгоритма будет разбит на $\Psi'_{2,3}(i-j-l_2,k)$ равных частей. Для функции $\Psi'_{2,3}(i-j-l_2,k)$ справедливо соотношение (21).

Если по итогам выполнения $(j+l_2)$-го шага алгоритма сформируется исход типа c_1), то это будет свидетельствовать о проявлении виртуальной последовательности на первых $(j-1)$ шагах алгоритма. На основании принципа "пересечения" устанавливаем: $x \in \left[x_{q_{j-1}+1}^{j-1}, x_{q_{j-1}+1}^{j-1,2}\right)$.

На последующих шагах алгоритма в выделенном на $(j+l_2)$-м шаге применяют видоизмененный классический алгоритм поиска, который разобъет его на $\Psi_{2,3}(i-j-l_2,k)$ равных частей. Для функции $\Psi_{2,3}(i-j-l_2,k)$ справедливо соотношение (23).

На основании соотношений (23), (24) устанавливаем:

$$l\left(\left[x^{j-1}_{q_{j-1}+1}, x^{j-1,2}_{q_{j-1}+1}\right)\right) = \\ = h_1(k+1)^{(l_1-1)}k^{(l_2-l_1+1)}\Psi_{2,3}(i-j-l_2,k). \quad (25)$$

Нетрудно убедиться в том, что для других значений параметра q_l исхода типа a_1) справедливо соотношение

$$l\left(\left[x^1_2, x^1_3\right)\right) = h(k-1)^{j-2}\Psi'_{2,3}(i-j-l_2,k), \quad (26)$$

а также выражения (24), (25).

Рассмотрим особенности решения исходов типа a_0) и a_2), возникающих по итогам выполнения первого шага алгоритма. Для них также, как и для исхода типа a_1), на втором шаге применяют смешанную стратегию:

исход типа a_0): $x^2_1 = 0$; $x^2_2 \in (0, x^1_1)$; $x^2_3 = x^1_1$;

исход типа a_2): $x^2_1 = x^1_3$; $x^2_2 \in (x^1_3, 1)$; $x^2_3 = 1$.

При этом если для исхода типа a_0) на втором шаге формируется исход типа $в_1$), то это будет свидетельствовать о действии виртуальной последовательности на втором и последующих шагах алгоритма (такие шаги пропускаются); если для исхода типа a_2) на втором шаге алгоритма формируется исход типа $в_3$), то это будет свидетельствовать о действии виртуальной последовательности на втором и последующих шагах алгоритма (такие шаги пропускаются). Для всех других исходов, возникающих в процессе поиска, используется рассмотренная для исхода типа a_1) стратегия поиска. На этом основании устанавливаем истинность соотношения

$$l\left(\left[0, x^1_1\right)\right) = l\left(\left[x^1_3, 1\right)\right) = h(k-1)^{j-2}\Psi'_{2,3}(i-j-l_2,k). \quad (27)$$

На основе анализа выражений (12), (22), (24) устанавливаем такую закономерность:

$$\varphi^{H,l_1,l_2,a}_{2,3}(i,k) = (k+1)\overline{\varphi}^{H,l_1,l_2,a}_{2,3}(\alpha,k), \quad (28)$$

где

$$\overline{\varphi}^{H,l_1,l_2,a}_{2,3}(\alpha,k) = \begin{cases} (k-1)^{j-1}\max\left\{\varphi^{H,l_1,l_2,a}_{2,3}(i-j,k), \right. \\ \left. \min\left\{\underline{\Psi}_{2,3}(i-j,k), \overline{\Psi}_{2,3}(i-j,k)\right\}\right\}, \\ h_0 \ge h, h_0 \ge h_1; \\ (k-1)^{j-2}\Psi'_{2,3}(i-j-l_2,k), h \ge h_0, \\ h \ge h_1; \\ (k+1)^{l_1-1}k^{(l_2-l_1+1)}\Psi_{2,3}(i-j-l_2,k), \\ h_1 \ge h_0, h_1 \ge h; \end{cases}$$

$$h_0 = \left(x^1_{q1+1} - x^1_{q1}\right) \Big/ (k-1)^{j-1}\varphi^{H,l_1,l_2,a}_{2,3}(i-j,k); q_1 = \overline{0,k}.$$

Для случая, когда амплитуда выброса виртуальной последовательности равна или больше длины исходного интервала неопределенности, на основании соотношений (18), (22), (24) устанавливаем:

$$\varphi^{H,l_1,l_2,a}_{2,3}(i,k) = (k+1)\overline{\varphi}^{=H,l_1,l_2,a}_{2,3}(\alpha,k), \quad (29)$$

где

$$\overline{\varphi}^{=H,l_1,l_2,a}_{2,3}(\alpha,k) = \begin{cases} (k-1)^{j-1}\max\left\{\varphi^{H,l_1,l_2,a}_{2,3}(i-j,k), \right. \\ \left. \min\left\{\underline{\Psi}_{2,3}(i-j,k), \overline{\Psi}_{2,3}(i-j,k)\right\}\right\}, \\ h_0 \ge h, h^1_0 \ge h_1; \\ (k-1)^{j-2}\Psi'_{2,3}(i-j-l_2,k), h \ge h^1_0, \\ h \ge h_1; \\ (k+1)^{l_1-1}k^{(l_2-l_1+1)}\Psi_{2,3}(i-j-l_2,k), \\ h_1 \ge h^1_0, h_1 \ge h; \end{cases}$$

$$h^1_0 = \left(x^1_{q1+1} - x^1_{q1}\right) \Big/ (k-1)^{j-1}\max\left\{\varphi^{H,l_1,l_2,a}_{2,3}(i-j,k), \right. \\ \left. \min\left\{\underline{\Psi}_{2,3}(i-j,k), \overline{\Psi}_{2,3}(i-j,k)\right\}\right\}$$

Следует заметить, что если выполняется соотношение $i = 2l_2 + 1$, то применяется на всех шагах алгоритма принцип "повторных сравнений". На этом основании устанавливаем:

$$\varphi^{H,l_1,l_2,a}_{2,3}(1,k) = \varphi^{H,l_1,l_2,a}_{2,3}(2,k) = ... = \\ = \varphi^{H,l_1,l_2,a}_{2,3}(2l_2,k) = 1; \\ \varphi^{H,l_1,l_2,a}_{2,3}(2l_2+1,k) = (k+1). \quad (30)$$

Проведенный анализ всевозможных исходов, возникающих в процессе поиска точки с характерным признаком, позволяет методом индукции по i синтезировать алгоритм поиска для любых его параметров: i, k, a, l_1, l_2, H.

Описанные стратегии поиска (закономерности распределения точек экспериментов), правила формирования нового интервала неопределенности и логические схемы алгоритмов поиска позволяют методом индукции построить алгоритм для любых его параметров и любых параметров $A_{2,3}$-последовательности и, тем самым, разработать оригинальные методы защиты информации.

Литература: 1 *Алипов Н. В., Алипов И.Н., Булах Е.В., Охапкин А. А., Ребезюк Л.Н.* Датчики виртуальной помехи, используемые для организации функционирования дискретных автоматов в системах защиты информации // Радиотехника. Вып. 111.С.33-39. 2 *Алипов Н.В.* Разработка теории и методов решения задач помехоустойчивого поиска и преобразования информации // Автореф. дис. на соискание учёной степени д-ра техн. наук. Харьков:ХИРЭ, 1986, 50 с. 3 *Альсведе Р., Вегенер М.* Задачи поиска. М: Мир, 1982. 365с. 4 *Алипов Н.В.* Принцип "пересечения" и его применение при алгоритмическом синтезе преобразователей информации. К.: Наук. думка. 1980. С.10-13.

Поступила в редколлегию 22.01.2001

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

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина,14, тел. 40-94-94.

Алипов Илья Николаевич, канд. техн. наук. Научные интересы: защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина,14, тел. 40-94-94.

Литвинова Евгения Ивановна, канд. техн. наук, доцент кафедры проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 61166, Харьков, пр. Ленина,14, тел. 40-94-94.