УДК 681.3+681.5:007

ПОСЛЕДОВАТЕЛЬНЫЕ АЛГОРИТМЫ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ, ПОМЕХОУСТОЙЧИВЫЕ К НЕСИММЕТРИЧНЫМ НЕРЕГУЛЯРНЫМ ВИРТУАЛЬНЫМ ПОСЛЕДОВАТЕЛЬНОСТЯМ

АЛИПОВ Н.В., АЛИПОВ И.Н., РЕБЕЗЮК Л.Н.

Строятся последовательные алгоритмы, помехоустойчивые к виртуальным последовательностям, у которых интервал времени между соседними выбросами является случайной величиной. Эти алгоритмы описывают дискретные автоматы с псевдослучайными переходами из одного состояния в другое.

В любые времена информация представляла большую ценность [1]. Поэтому проблема ее защиты существовала всегда. В настоящее время для решения данной проблемы в основном используются симметричные и несимметричные криптографические методы [1]. Наряду с этим направлением развивается новое, связанное с применением конечных автоматов [2]. В работе [3] описывается структура одного из таких автоматов, отличительной особенностью которого является псевдослучайный переход автомата из начального состояния в одно и то же конечное. Для организации такого «блуждания» автомата используют алгоритмы помехоустойчивого поиска точки с характерным признаком [3], структура которых определяется параметрами виртуальной последовательности [4].

Известно [4], что виртуальная последовательность описывается такими параметрами: амплитудой выброса (a), длительностью выброса (ℓ) и интервалом времени между соседними выбросами последовательности. Эти параметры могут быть неслучайными либо случайными величинами. К настоящему моменту разработаны алгоритмы поиска точки (x) с характерным признаком, помехоустойчивые к последовательностям, у которых все их параметры являются неслучайными величинами [5] либо случайной величиной является только длительность выброса (ℓ).

Цель исследования – синтез последовательных алгоритмов поиска точки с характерным признаком, помехоустойчивых к нерегулярным виртуальным последовательностям, для которых интервал времени (h) между соседними выбросами последовательности – случайная величина.

Формулировка задачи синтеза помехоустойчивых алгоритмов поиска дана в работе [4]. Решением этой задачи является построение стратегий поиска (размещение точек эксперимента в интервале неопределенности) в условиях действия конкретной виртуальной последовательности и правил формирования нового интервала неопределенности относительно точки с характерным признаком. В дальнейшем будем полагать, что $h \in [h_1, h_2]$, $\ell, a = const$, $k = 1$ (количество точек эксперимента); виртуальная последовательность – однополярная, посредством которой точка с характерным признаком смещается в направлении $(0 \to 1)$; h_1 – минимальное значение параметра h; h_2 – максимальное значение параметра h; h – целое положительное число.

Первоначально положим: $h_1 = 1$, $h_2 = 2$, $\ell = 1$, a - целое положительное число, $x \in [0,1]$, $k = 1$. Пусть некоторым образом выбрана точка x_1^1 первого эксперимента. Тогда, как известно [2,3], может возникнуть один из исходов:

$$\text{а)}\ x(t_1) < x_1^1; \quad \text{б)}\ x(t_1) > x_1^1, \qquad (1)$$

где $x(t_1)$ – смесь значения координаты точки x и $\xi(t_1)$; $\xi(t_1)$ – значение амплитуды виртуальной последовательности в момент времени t_1 (моменты выполнения первого эксперимента).

Поскольку виртуальная последовательность только увеличивает значение координаты точки x, то первый исход в этом случае является достоверным. Предполагается, что алгоритм за i шагов разбивает исходный интервал неопределенности $(0,1)$ на $\varphi_1^{h_1,h_2,\ell,a}(i,1)$ равных частей. Поскольку первый исход достоверный, а в распоряжении алгоритма осталось $(i-1)$ шагов, то выделенный полуоткрытый интервал неопределенности $(0, x_1^1]$ будет разбит на $\varphi_1^{h_1,h_2,\ell,a}(i-1,1)$ равных частей. Для второго исхода однозначно нельзя утверждать: наблюдалось или не наблюдалось проявление виртуальной последовательности. В этом случае на основании принципа "пересечения" формируется такой полуоткрытый интервал неопределенности:

$$x \in [x_1^{1,1}, 1), \qquad (2)$$

где $x_1^{1,1} = \begin{cases} x_1^1 - a\delta, x_1^1 - a\delta > 0; \\ 0 \text{ в противном случае,} \end{cases}$ δ – дискретность квантования. Для данного исхода используют принцип "повторных сравнений" либо оптимистическую стратегию [3].

Предположим, что на втором шаге применяют принцип "повторных сравнений" (пессимистическую стратегию) $x_1^2 = x_1^1$. Тогда при возникновении исхода $x(t_2) > x_1^2$ выделяем такой полуоткрытый интервал $x \in [x_1^1, 1)$, который за остальные $(i-2)$ шага алгоритмом будет разбит на $\varphi_1^{h_1,h_2,\ell,a}(i-2,1)$ равных частей.

Покажем, что если $h_1 = 1$, то оптимистическая стратегия не позволяет уменьшить исходный интервал неопределенности. Действительно, пусть $x(t_1) > x_1^1$ и $x_1^2 > x_1^1$, а при выполнении второго шага алгоритма возник исход $x(t_2) < x_1^2$.

Тогда $x \in [0, x_1^2)$, $l([0, x_1^2)) > \ell([0, x_1^1))$, где $\ell([\circ])$ – длина отрезка $[\circ]$, а виртуальная последовательность может проявиться снова. Поскольку в распоряжении алгоритма осталось $(i-2)$ шага, то выделенный полуоткрытый интервал неопределенности будет разбит на $\varphi_1^{h_1,h_2,\ell,a}(i-2,1)$ равных частей. Если же в этом случае на втором шаге алгоритма применить пессимистическую стратегию, то данный исход будет свидетельствовать о действии виртуальной последовательности на первом шаге алгоритма. Поскольку ее проявление обнаружено, то применяется такая комбинация алгоритмов. Если $h_2 = 2$, то на третьем шаге алгоритма можем применить стратегию классического алгоритма поиска $x_1^3 = 1/2\,(\ell[0, x_1^1])$.

При этом если возникает исход $x(t_3) \in [0, x_1^3)$, то это свидетельствует о том, что на третьем шаге алгоритма виртуальная последовательность не проявлялась. На этом основании устанавливаем: $x \in [0, x_1^3)$.

Затем пропускаем четвертый шаг (по условию на четвертом шаге снова будет проявление виртуальной последовательности). Пятый шаг выполняется по стратегии классического алгоритма

$$x_1^5 = 1/2\,(\ell[0, x_1^3)).$$

Поскольку по условию на этом шаге не может быть проявления виртуальной последовательности, то для любого исхода а) или б) устанавливаем соответственно

$$\text{а)}\ x \in [0, x_1^5); \quad \text{б)}\ x \in [x_1^5, x_1^3).$$

В дальнейшем поступаем таким же образом, как и на третьем шаге. Рассмотрим второй исход, который может возникнуть на третьем шаге алгоритма, $x(t_3) \in [x_1^3, x_1^1)$.

Этот исход свидетельствует о неопределенности в принятии решения (на третьем шаге могло или не могло быть проявления виртуальной последовательности). Для устранения этой неопределенности выполняем повторный эксперимент на четвертом шаге в точке x_1^1. При этом могут возникнуть исходы $x(t_4) < x_1^1$; $x(t_4) > x_1^1$.

Первый исход свидетельствует о действии виртуальной последовательности на третьем шаге, по этой причине $x \in [0, x_1^1)$. Нетрудно заметить, что данная ситуация повторяет ситуацию второго шага алгоритма.

Для второго исхода характерно то, что на четвертом шаге алгоритма действовала виртуальная последовательность. Этот исход создает новую ситуацию. Однако в совокупности с первым исходом стратегия третьего шага алгоритма приводит процесс поиска к началу второго шага алгоритма. При этом интервал неопределенности, выделенный на втором шаге, за два последующих шага алгоритма не уменьшается. Следовательно, описанная стратегия третьего шага алгоритма не может быть использована. Отсюда заключаем, что на третьем шаге алгоритма не может быть применена оптимистическая стратегия. Поскольку на каждом шаге алгоритма эксперимент выполняется только в одной точке, а множество стратегий включает оптимистическую и пессимистическую, то приходим к выводу: на третьем шаге следует воспользоваться пессимистической стратегией $x_1^3 = x_1^1$.

При этом если возникает исход $x(t_3) < x_1^1$, то это свидетельствует о том, что на третьем шаге не наблюдалось проявления виртуальной последовательности. Как следует из условий, такое проявление в обязательном порядке возникнет на четвертом шаге алгоритма. Этот шаг пропускают, а пятый шаг является первым шагом классического алгоритма поиска на отрезке $[0, x_1^1]$. При этом $x_1^5 = 1/2\,(\ell[0, x_1^1])$. В дальнейшем в зависимости от выделенного полуоткрытого интервала неопределенности $[0, x_1^5]$, $[x_1^5, x_1^1)$ шестой шаг алгоритма совершают в точке x_1^5 или в точке x_1^1. Описанный процесс продолжают до окончания поиска.

Если же при выполнении третьего шага алгоритма возникает исход $x(t_3) > x_1^1$, то это означает, что виртуальная последовательность проявилась на третьем шаге. Исходя из условий поиска точки с характерным признаком, виртуальная последовательность не будет проявляться на четвертом шаге алгоритма. На этом основании утверждаем, что четвертый шаг является первым шагом классического алгоритма поиска на отрезке $[0, x_1^1]$. В этом случае эксперимент выполняют в точке $x_1^4 = 1/2\,(\ell[0, x_1^1))$. Пятый шаг алгоритма выполняют таким же образом, как шестой шаг для ранее рассмотренного исхода (используют принцип “повторных сравнений”): $x_1^5 = x_1^4$; $x_1^5 = x_1^1$.

Такой процесс продолжают до завершения поиска. Из приведенного детального рассмотрения процесса поиска для случая, когда $h_1 = 1$, следует подтверждение ранее высказанного и такого утверждения: на эффективность процесса поиска оказывает влияние только минимально возможное значение параметра h, а максимально возможное значение и длительность виртуального выброса определяет количество шагов, которые пропускают в процессе поиска точки с характерным признаком. Это количество шагов определяется соотношением

$$I = h_2 + \ell. \qquad (3)$$

Как уже было сказано, на втором шаге алгоритма необходимо всегда использовать принцип “повторных сравнений”, однако при этом следует знать, на какое количество равных частей будет разбит вновь выделенный полуоткрытый интервал неопределенности за оставшиеся шаги алгоритма комбинированным алгоритмом в случае появления исхода $x(t_2) < x_1^2$.

Из описания комбинированного алгоритма поиска следует, что в распоряжении алгоритма остается

$(i-2)$ шага, третий и четвертый шаги пропускаются, на пятом используется классический алгоритм поиска; затем пропускаются шестой и седьмой шаги, а на восьмом используется классический алгоритм поиска и таким образом действуют до конца поиска.

Количество эффективных шагов определяется соотношением:

$$\alpha_1 = \left]\frac{i-2}{\ell + h_2}\right[, \qquad (4)$$

где ℓ – длительность выброса виртуальной последовательности; h_2 – максимальное значение параметра паузы между двумя соседними выбросами; $\left]\frac{a}{b}\right[$ – целая часть от деления числа a на число b.

Поскольку на каждом шаге алгоритма выполняется эксперимент в одной точке, то классический алгоритм поиска точки с характерным признаком разобьет выделенный полуоткрытый интервал неопределенности на $\psi_1^{h_1,h_2,\ell,a}(i-2,1)$ равных частей. При этом для данной функции справедливо

$$\psi_1^{h_1,h_2,\ell,a}(i-2,1) = 2^{\left]\frac{i-2}{\ell+h_2}\right[},$$

здесь $\ell = 1$; $h_1 = 1$; $h_2 = 2$; a – целое положительное число.

На втором шаге в результате применения принципа "повторных сравнений" выделяется один из полуоткрытых интервалов: $[x_1^{1,1}, x_1^1)$, $[x_1^1, 1)$,

где $x_1^{1,1} = \begin{cases} x_1^1 - a\delta, x_1^1 - a\delta > 0; \\ 0 \text{ в противном случае;} \end{cases}$ $[x_1^{1,1}, x_1^1) \in [0, x_1^1)$.

Как уже было показано, полуоткрытый интервал неопределенности $[0, x_1^1)$ разбивается на $\varphi_1^{h_1,h_2,\ell,a}(i-1,1)$ равных частей; полуоткрытый интервал неопределенности $[x_1^1, 1]$ – на $\varphi^{h_1,h_2,\ell,a}(i-2,1)$ равных частей; полуоткрытый интервал неопределенности $[x_1^{1,1}, 1]$ – на $\psi_1^{h_1,h_2,\ell,a}(i-2,1)$ равных частей.

Для i-шагового алгоритма выбираем конструкцию, исходя из наихудшего случая:

$$\varphi_1^{h_1,h_2,\ell,a}(i,1) = \varphi_1^{h_1,h_2,\ell,a}(i-2,1) + \begin{cases} \varphi_1^{h_1,h_2,\ell,a}(i-1,1), \delta_1 > \delta_2; \\ \frac{x_1^1}{\delta_2}, \delta_2 > \delta_1, \end{cases} \qquad (5)$$

где $\delta_1 = \dfrac{x_1^1}{\varphi_1^{h_1,h_2,\ell,a}(i-1,1)}$; $\delta_2 = \dfrac{x_1^1 - x_1^{1,1}}{\varphi_1^{h_1,h_2,\ell,a}(i-2,1)}$.

Обобщим сформулированный комбинированный алгоритм и полученные соотношения для произвольного h_1 $(h_1 > 1)$.

Как известно, в результате выполнения первого шага алгоритма может появиться один из исходов (1). Для первого из них однозначно устанавливается полуоткрытый интервал неопределенности $[0, x_1^1)$, а для второго он формируется на основе принципа "пересечения" (см. соотношение (2)).

В выделенном полуоткрытом интервале может быть использована одна из стратегий: оптимистическая либо пессимистическая. Пусть на втором шаге выбрана первая из них и эксперимент выполняется в точке x_1^2, для которой справедливо неравенство $x_1^2 > x_1^1$.

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

$$x(t_2) < x_1^2; \qquad x(t_2) > x_1^2. \qquad (6)$$

Для первого исхода, на основании свойств виртуальной последовательности (она всегда только увеличивает значение координаты точки x), формируют полуоткрытый интервал $[x_1^{1,1}, x_1^2)$.

Для второго исхода, согласно длительности выброса виртуальной последовательности $(\ell = 1)$ и результатам первого и второго экспериментов $x(t_1) > x_1^1$, $x(t_2) > x_1^2$, устанавливаем истинность соотношения: $x \in [x_1^1, 1)$.

Как видим, формировать новый интервал неопределенности можно не только на основании принципа "пересечения", но и по результатам экспериментов, разнесенных во времени на ℓ шагов алгоритма.

В общем случае такое правило можно сформулировать в следующем виде: если на j-м шаге алгоритма установлено, что $x(t_j) > x_1^j$, а на $(j + j_1)$-м получим исход $x(t_{(j+j_1)}) > x_1^{j+j_1}$, то для $j_1 = \ell$ справедливо соотношение $x > x_1^j$.

Нетрудно заметить, что, используя только оптимистическую стратегию для первого исхода (см. соотношение (6)), уменьшить длину полуоткрытого интервала $[x_1^{1,1}, x_1^1)$ невозможно (точки экспериментов выбираются правее точки x_1^1). Поэтому для уменьшения длины интервала следует на каком-нибудь шаге алгоритма применить пессимистическую стратегию (повторить эксперимент в точке x_1^1).

Первоначально выясним: как долго можно откладывать проведение подобного эксперимента. Пусть на втором шаге возник подобный исход. Тогда самым неблагоприятным будет случай, когда виртуальная последовательность имела место на первом шаге алгоритма. По определению виртуальной последовательности она не будет проявляться еще на втором, третьем, ..., $(h_1 + 1)$-м шагах алгоритма. По этой причине пессимистическую стратегию для нашего исхода можно применить на третьем, ..., $(h_1 + 1)$-м шагах (на втором шаге была использована оптимистическая стратегия).

Пусть на третьем шаге планируется применить пессимистическую стратегию, в результате ее выполнения получим исход $x(t_3) > x_1^3$.

Тогда это будет свидетельством того, что проявление виртуальной последовательности имело место на первом шаге алгоритма, на втором, третьем шагах оно отсутствовало. Виртуальная последовательность не будет еще наблюдаться на четвертом, пятом, ..., (h_1+1)-м шагах. Для данного исхода полуоткрытым интервалом неопределенности будет $[x_1^{1,1}, x_1^1)$. По этой причине на четвертом, ..., (h_1+1)-м шагах алгоритма следует применить классический алгоритм поиска, который разобьет выделенный интервал неопределенности на 2^{h_1-2} равные части. Затем, используя описанную ранее комбинацию алгоритмов, пропустить $(h_2 - h_1 + \ell)$ шагов алгоритма; потом на последующих h_1 шагах применить классический алгоритм и т.д. до конца поиска. В результате такой комбинации полуоткрытый интервал неопределенности $[x_1^{1,1}, x_1^1)$ будет разбит на $\psi_1^{h_1,h_2,\ell,a}(i-3,1)$ равных частей. При этом для данной функции справедливо соотношение

$$\psi_1^{h_1,h_2,\ell,a}(i-3,1) = 2^{h_1-2} \cdot 2^{h_1\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil} \cdot 2^{\alpha_1}, \qquad (7)$$

где

$$\alpha_1 = \begin{cases} 0, \text{если 1);} \\ (i-h_1-1)-(\ell+h_2)\left\lceil \dfrac{i-h_1-1}{\ell+h_2}\right\rceil - (\ell+h_2-h_1), \text{если 2),} \end{cases}$$

$$1)\ (i-h_1-1)-(\ell+h_2)\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil \le (\ell+h_2-h_1),$$

$$2)\ (i-h_1-1)-(\ell+h_2)\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil > (\ell+h_2-h_1).$$

Если пессимистическую стратегию применить на четвертом шаге алгоритма, то будем иметь такое соотношение:

$$\psi_1^{h_1,h_2,\ell,a}(i-4,1) = 2^{h_1-3} \cdot 2^{h_1\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil} \cdot 2^{\alpha_1}. \qquad (8)$$

Нетрудно заметить, что последний шаг, на котором еще возможно применить пессимистическую стратегию, есть (h_1+1)-й шаг алгоритма.

Соотношения (7), (8) позволяют обоснованно подходить к выбору шага алгоритма, на котором следует в обязательном порядке применить пессимистическую стратегию. Для того чтобы на третьем шаге ее не применять, необходимо, чтобы были истинными такие соотношения:

$$\ell([x_1^{1,1}, x_1^1)) \le \delta(2^{h_1-2} \cdot 2^{h_1\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil} \cdot 2^{\alpha_1}), \qquad (9)$$

$$\ell([x_1^{1,1}, x_1^1)) \le \delta(2^{h_1-3} \cdot 2^{h_1\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil} \cdot 2^{\alpha_1}).$$

Если хотя бы одно из соотношений (9) не выполняется, то на третьем шаге следует применить пессимистическую стратегию.

Если в результате применения на третьем либо на четвертом шагах возникли соответственно исходы

$$x(t_3) > x_1^3;\ x(t_4) > x_1^4,$$

то это свидетельствует об их истинности. На этом основании устанавливаем: $x \in [x_1^1, x_1^2)$ либо $x \in [x_1^1, x_1^3)$. В первом случае в распоряжении алгоритма осталось $(i-3)$, а во втором $(i-4)$ шагов. На этом основании заключаем, что первый полуоткрытый интервал будет разбит на $\varphi^{h_1,h_2,\ell,a}(i-3,1)$ равные части, а второй – на $\varphi^{h_1,h_2,\ell,a}(i-4,1)$.

Обобщим соотношения (9) для произвольного шага алгоритма. Пусть на $(j-1)$-м шаге был выделен некоторый полуоткрытый интервал неопределенности относительно x, а на j-м шаге в точке x_1^j был выполнен эксперимент, в результате которого сформирован исход

$$x(t_j) > x_1^j. \qquad (10)$$

На последующих $j+1$, $j+2$, ..., $j+z-1$ шагах алгоритма $(z < h_1)$ применялась оптимистическая стратегия и всякий раз возникал исход $x(t_{j+\rho}) < x_1^{j+\rho}$, $\rho = \overline{1, z-1}$. Тогда пессимистическая стратегия не используется на $(j+z)$-м шаге в том случае, когда будут истинными соотношения:

$$\ell([x_1^{j,1}, x_1^j)) \le \delta(2^{h_1-z} \cdot 2^{h_1\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil} \cdot 2^{\alpha_2}), \qquad (11)$$

$$\ell([x_1^{j,1}, x_1^j)) \le \delta(2^{h_1-z-1} \cdot 2^{h_1\left\lceil \frac{i-h_1-1}{\ell+h_2}\right\rceil} \cdot 2^{\alpha_2}),$$

где

$$\alpha_2 = \begin{cases} 0, \text{если 1);} \\ (i-j-h_1)-(\ell+h_2)\left\lceil \dfrac{i-j-h_1}{\ell+h_2}\right\rceil - (\ell+h_2-h_1), \text{если 2),} \end{cases}$$

$$1)\ (i-j-h_1)-(\ell+h_2)\left\lceil \frac{i-j-h_1}{\ell+h_2}\right\rceil \le (\ell+h_2-h_1),$$

$$2)\ (i-j-h_1)-(\ell+h_2)\left\lceil \frac{i-j-h_1}{\ell+h_2}\right\rceil > (\ell+h_2-h_1).$$

Очевидным является заключение: если $z = h_1$, то на $(j+z)$-м шаге алгоритма необходимо применить пессимистическую стратегию.

Подобные алгоритмы строят методом индукции. Нетрудно убедиться для $\ell = 1$ в истинности соотношений:

$$\varphi_1^{h_1,h_2,\ell,a}(1,1) = 1;\ \ \varphi_1^{h_1,h_2,\ell,a}(2,1) = 2. \qquad (12)$$

Для произвольного значения ℓ будут справедливы такие соотношения:

$$\varphi_1^{h_1,h_2,\ell,a}(0,1) = \varphi_1^{h_1,h_2,\ell,a}(1,1) = \ldots = \varphi_1^{h_1,h_2,\ell,a}(\ell,1) = 1;$$
$$\varphi_1^{h_1,h_2,\ell,a}(\ell+1,1) = 2. \qquad (13)$$

Приведенная схема комбинированного алгоритма, правила выделения нового интервала неопределенности и выбора стратегии поиска совместно с соотношениями (12), (13) позволяют методом индукции построить последовательный помехоустойчивый алгоритм поиска точки с характерным признаком для любых значений параметров виртуальной последовательности и, тем самым, задать функционирование конечного автомата с псевдослучайными переходами.

Литература: **1.** *Спесивцев А.В., Вегнер В.А. и др.* Защита информации в персональных ЭВМ. М.: Радио и связь, 1992. 191 с. **2.** *Ecker A.* Abctrakte kriptographische Mashinen // Angew. Informatik. 1975. Bol.17, Nr 5. S.201-205. **3.** *Алипов Н.В.* Дискретные автоматы с псевдослучайными переходами и подстановочные методы защиты информации на их основе // Радиоэлектроника и информатика. 2001. № 4. С.95-98. **4.** *Алипов Н.В.* Разработка теории и методов решения задач помехоустойчивого поиска и преобразования информации // Автореф. дис. на соиск. уч. степени докт. техн. наук. Харьков: ХИРЭ, 1986. 50 с. **5.** *Алипов Н. В., Ребезюк Л.Н., Охапкин А.А.* Защита информации в дискретном канале на основе устойчивых к периодическим помехам алгоритмов поиска точки с характерным признаком // АСУ и приборы автоматики. 1999. Вып.109. С.108-115.

Поступила в редколегию 20.01.2003

Рецензент: д-р техн. наук, проф. Петров Э.Г.

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры электронно-вычислительных машин ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронно-вычислительных средств, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина,14, тел. 70-21-354.

Алипов Илья Николаевич, канд. техн. наук. Научные интересы: защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина,14, тел. 70-21-354.

Ребезюк Леонид Николаевич, канд. техн. наук, доцент кафедры системотехники ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронно-вычислительных средств, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина,14, тел. 70-21-306.

УДК 621.391 + 519.81

МНОГОФАКТОРНОЕ ОЦЕНИВАНИЕ ПРОВОДНОЙ СЕТИ ЭЛЕКТРОСВЯЗИ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЕЁ ИСПОЛЬЗОВАНИЯ

ГРЕБЕННИК И.В., ХАБАРОВ А.Ю.

Проводится анализ характеристик проводной сети электросвязи, которые могут быть использованы для оценки ее технического состояния и качества предоставляемых клиентам услуг. Формулируются критерии оценки, предлагаются способы их свертки для получения интегрального показателя эффективности использования всей сети или ее фрагмента.

Введение. Проводная сеть электросвязи является сложной технической системой, бесперебойное и качественное функционирование которой обеспечивается постоянным решением большого набора задач разного уровня сложности и компетенции лиц, принимающих конкретные решения (ЛПР). Одной из самых сложных и практически нереализуемых без применения ЭВМ задач является комплексный анализ качества сети и предоставляемых услуг, дающий возможность мониторинга ее состояния и выявления сильных и слабых сторон технического оснащения предприятия электросвязи. Благодаря такому анализу можно сделать выводы об эффективности использования того или иного оборудования и, главное, принять научно обоснованное управленческое решение по развитию сети, устранению «узких» мест. Естественно, такая задача не решается ежедневно. В большинстве случаев не требуется детализация до отдельно взятой линии, но сводная укрупненная информация по предприятию необходима для руководителей среднего и высшего звена.

Ранее уже предпринимались попытки оценить эффективность сети с точки зрения качества ее структуры [1-3] или функционирования отдельных ее элементов [4, 5], однако решение задачи в предлагаемой постановке авторам не известно.

Постановка задачи. Общую задачу многофакторного оценивания проводной сети электросвязи и анализа эффективности ее использования сформулируем следующим образом. Исходя из текущего состояния сети, дать количественную оценку эффективности ее функционирования и качества предоставляемых услуг для всей сети или ее фрагмента, используя указанные ниже критерии оценки.

Формализация и решение. Один из конструктивных методов оценивания основывается на теории полезности [6]. При этом задача оценки качества сети формально сводится к применению того или иного вида обобщенного критерия для некоторого набора частных критериев. Наиболее широко известны аддитивная и мультипликативная формы:

$$P(x) = \sum_{i=1}^{n} a_i k_i(x) \quad \text{и} \quad P(x) = \prod_{i=1}^{n} a_i k_i(x),$$
$$0 \le a_i \le 1, \quad \sum a_i = 1,$$