$$\mathrm{tg}\varphi = \frac{A_1 \sin\varphi_1 + A_2 \sin\varphi_2}{A_1 \cos\varphi_1 + A_2 \cos\varphi_2},$$

На основе этих формул можно рассчитать амплитуду и фазу гармонического сигнала в любой точке помещения.

Список литературы

1. *Макаров Г. В., Быковников В. В., Пятунин А.Н.* Тональный алгоритм обнаружения радиомикрофонов. // Журнал радиоэлектроники. - 2000. - №11.

2. *Теория* обнаружения сигналов. / П.С. Акимов, П.А. Бакут, В.А. Богданович и др.; Под ред. П.А. Бакута. - М.: Радио и связь, 1984. - 440 с.

3. *Маньковский В.С.* Акустика студий и залов для звуковоспроизведения. - М.: Искусство, 1966. -376 с.

Поступила 04.09.2006

УДК 004. 681

Гордиенко С.Б., Хорошко В.А.

ОПТИМАЛЬНОЕ РАЗМЕЩЕНИЕ ДАТЧИКОВ АКУСТИЧЕСКОГО ЗАШУМЛЕНИЯ ПОМЕЩЕНИЙ ПРИ ПОСТРОЕНИИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ

Актуальность задачи защиты информации (ЗИ) от утечки по акустическим и виброакустическим каналам, порождаемым речевой деятельностью человека несомненна и занимает ведущее место в общем ряду существующих в области безопасности информации проблем. С другой стороны, ряд аспектов, влияющих на эффективность защиты речевой информации, зачастую остается за пределами внимания при организации системы информационной безопасности объектов, разработке и производстве средств защиты речевой информации (СЗРИ), их практическом применении. К аспектам, влияющим на снижение качества закрытия каналов утечки информации, а иногда и их непреднамеренному созданию в случае неквалифицированного проведения мер по ЗИ, в первую очередь следует отнести:

- необеспеченность оценок качества информационной безопасности, в том числе и при настройке СЗРИ, инструментальными средствами контроля;
- невнимание к угрозам компенсации излучаемых СЗРИ помех и перехвата содержания скрываемых переговоров при поверхностном соблюдении норм и требований по ЗИ;
- недооценку опасности выхода из строя (по различным причинам) аппаратуры ЗИ.

Первая проблема связана с активно развивающейся в настоящее время нормативной базой в области ЗИ: требования руководящих документов по номенклатуре измеряемых в ходе контроля параметров и точности их оценки.

Технические проблемы, стоящие перед разработчиками аппаратуры и специалистами, обеспечивающих нейтрализацию акустических каналов, могут быть проиллюстрированы на примере контроля сигналов электроакустических преобразований. Данная задача связана с наличием у некоторых технических устройств микрофонных свойств, вследствие чего под воздействием акустических волн в них наводятся электрические сигналы, которые по различным электрическим цепям и токопроводящим элементам конструкций могут распространяться за пределы контролируемой территории. Актуальность задачи подтверждается и тем, что уровни сигналов от незащищенных телефонных аппаратов на 2-3

порядка превосходят нормы по требованиям безопасности информации. При широком использовании незащищенной техники данный канал утечки информации становится одним из наиболее опасных.

Поэтому в качестве количественных показателей эффективности работы таких каналов можно использовать вероятности правильной передачи информации, в данном случае языковых конструкций: звуков (фонем), слогов, слов, фраз. Усредненные по многообразию возможных реализаций конструкций каждого из перечисленных видов эти вероятности называются фонемной, слоговой, словесной и фразеологичной разборчивостями речи. Основным показателем эффективности технической защиты речевой информации является словесная разборчивость речи P_w.

Практический опыт показывает, что составление подробной справки о содержании перехваченного разговора невозможно при P_w менее 60-70 %, а краткой справки-аннотации – при P_w менее 40-50%. При P_w менее 20-30% значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости менее 10% это становиться практически невозможным даже при использовании современных технических средств фильтрации помех [1].

В общем случае создание злоумышленником каналов утечки могут быть разбиты на группы таким образом, что в отсутствие речевого сигнала каналы одной группы статистически независимы от каналов другой. Современные методы совместной обработки речевой информации, поступающей с одной группы, позволяют снизить (в том случае, если в группе несколько каналов) эффективный уровень шума, на фоне которого воспринимается информативный речевой сигнал. В этом случае каналы утечки одной группы при оценках степени связанных с ними угроз безопасности могут быть сведены к одному эффективному каналу с измененным уровнем (как правило, более низким) помех, а ситуация в целом – к некоторой совокупности эффективных, статистически независимых каналов утечки. Как, следствие, можно говорить о некотором числе эффективных, статистически независимых каналов утечки информации $N_{эф}$ характерным для данного объекта защиты. Потенциально достижимую разборчивость языковых конструкций по совокупности этих каналов (в силу вероятностной природы этих показателей) можно выразить через соответствующие разборчивости в отдельных каналах соотношением:

$$P_{\alpha,o} = 1 - \prod_{i=1}^{N_{эф}} (1 - P_{\alpha,i}), \qquad (1)$$

где $P_{\alpha,0}$ – разборчивость по совокупности каналов; $P_{\alpha,i}$ – разборчивость в отдельном i-канале; (α – это индекс, обозначающий тип разборчивости (f_n – фонемная; s – слоговая; w – словесная; f_r - фразеологическая)); $N_{эф}$ – число статистически независимых каналов утечки. Если на объекте средствами технической защиты речевой информации обеспечиваются условия, в которых словесная разборчивость речи в возможном канале утечки $P_w \approx 0.2$, то при трех статистических независимых каналах утечки потенциальная разборчивость по объекту в целом составит $P_{w,0} = 0.48$, а при четырех – 0,72, то есть орган разведки вместо констатации факта разговора получит краткую его справку-аннотацию или даже подробный отчет о нем.

Более продуктивным представляется двухпараметрическое задание состояния безопасности речевой информации на объекте на основе нормирования значений эффективного числа возможных, статистически независимых каналов утечки $N_{эф}$, по совокупности которых должна обеспечиваться словесная разборчивость перехватываемых сообщений $P_{w,0}$. Требования к нормативному значению разборчивости на канал в этом случае могут определяться из обратного (1) выражения:

$$P_w = 1 - \sqrt[N_{эф}]{1 - P_{w,0}}, \qquad (2)$$

где P_w – словесная разборчивость на статически независимый канал, при не превышении которой в каждом канале разборчивость по всей их совокупности на объекте не превысит $P_{w,0}$.

Экспериментальное определение P_w – чрезвычайно трудоемкий процесс, поэтому оценка словесной разборчивости речи в том или ином канале передачи ею информации проводится по аналитическим соотношениям, установленным на основе ряда артикуляционных испытаний, выполненных в интересах разработки информативной базы контроля качества телефонных линий связи [2]. Основные положения и соотношения этой методики могут интерпретироваться следующим образом. Правильный прием фонемы эквивалентен распознаванию слуховым аппаратом человека характерного спектра соответствующего ей звукового колебания. Произвольный частотный диапазон звуковых колебаний может быть охарактеризован вероятностью правильной идентификацией фонем по результатам ее приема в ограниченной этим диапазоном полосе частот. Можно ввести «спектральную плотность вероятности» $r_{f_n}(f)$ так, что для фонемной разборчивости речи при регистрации ее в ограниченном диапазоне частот $[f_н, f_в]$ будет справедливо выражение:

$$P_{f_n} = \int_{f_н}^{f_в} r_{f_n}(f)df. \qquad (3)$$

Эта величина, в свою очередь, может быть выражена через произведение вероятности $dk(f)$ идентификации помехи по ее спектральным демаскирующим признакам в поддиапазоне $[f, f+df]$ на вероятность $p(f)$ обнаружения этих признаков:

$$r_{f_n}(f) = p(f)dk(f). \qquad (4)$$

Разбивая частотный диапазон на достаточно малые непересекающиеся конечные интервалы, можно для оценки P_{f_n} воспользоваться выражениями [2]:

$$P_{f_n} = \sum_{i=1}^{N} p_i k_i; \qquad (5)$$

$$K_i = k(f_{в_i}) - k(f_{н_i}); \qquad (6)$$

$$k(f) = \begin{cases} 2.57 \cdot 10^{-8} \cdot f^{2.4}, & \text{если} \quad 100 < f \le 400 \ \text{Гц}; \\ 1 - 1.074 \ \exp(-10^{-4} f^{1.18}), & \text{если} \quad 400 < f \le 10000 \ \text{Гц}. \end{cases} \qquad (7)$$

$$p_i = \begin{cases} \dfrac{0.78 + 5.46 \exp\left[-4.3 \cdot 10^{-3} \cdot (27.3 - |Q_i|)^2\right]^2}{1 + 10^{0.1|Q_i|}}, & \text{если} \quad Q \le 0; \\ 1 - \dfrac{0.78 + 5.46 \exp\left[-4.3 \cdot 10^{-3} \cdot (27.3 - |Q_i|)^2\right]^2}{1 + 10^{0.1|Q_i|}}, & \text{если} \quad Q > 0, \end{cases} \qquad (8)$$

где $f_{в_i}$ и $f_{н_i}$ – верхняя и нижняя границы i-го поддиапазона; $Q_i = q_i - \Delta A_i$; q_i – выраженное в децибелах отношение сигнал/шум для поддиапазона; а ΔA_i – форматный параметр, характеризующий энергетическую избыточность поддиапазона, оцениваемую из соотношения

$$\Delta A(f_{cp_i}) = \begin{cases} 200/f_{cp_i}^{-0.43} - 0.37, & если \quad f_{cp_i} \le 1000\ Гц; \\ 1.37 + 1000/f_{cp_i}^{-0.69}, & если \quad f_{cp_i} > 1000\ Гц. \end{cases} \qquad (9)$$

В выражении (9) $f_{cp_i} = \sqrt{f_{в_i} - f_{н_i}}$ – среднегеометрическая частота поддиапазона. При наличии информативного речевого сигнала с интегральной мощностью H и долевым ее распределением по поддиапазонам h_i, фонемная разборчивость речи зависит, как это следует из выражений (5) – (9), не только от интегральной мощности помехи G, но и от ее долевого распределения по поддиапазонам g_i. Если зафиксировать интегральное отношение сигнал/шум $R = H/G$ и распределение h_i, фонемная разборчивость становиться однозначной функцией распределения помехи g_i. Действительно, для отношений сигнал/шум в поддиапазонах выполняется соотношение:

$$q_i = R\frac{h_i}{g_i} \qquad (10)$$

(или в децибелах $q_i = R + [10\lg(h_i) - 10\lg(g_i)]$), определяющие необходимые исходные данные для оценок P_{f_n} из выражений (5) – (9). Поскольку область определения функций ограничена условиями:

$$0 \le g_i \le 1 \qquad \text{и} \qquad \sum_{i=0}^{N} g_i = 1, \qquad (11)$$

где P_{f_n} достигает в этой области или на ее границе свои максимальные и минимальные значения. Известны, что сосредоточение помехи в одном поддиапазоне, ассоциированное с границами области определения P_{f_n}, не приводит к значительному уменьшению разборчивости речи, поэтому экстремальное значение функции P_{f_n} (соответствующее ее минимуму) будет достигаться внутри ее области определения. Поскольку слоговая и словесная разборчивость речи является монотонными функциями фонемной разборчивости, точки экстремума P_{f_n}, P_s и P_w совпадают.

Таким образом, долевое распределение оптимизированной по спектру помехи g_i может быть определено на основании решения системы N уравнений, которые состоят из выражений: (8) для определения $p(Q)$; (9) - ΔA_i; выражения (6), (7) для вычисления K_i. Причем индекс i в них изменяется от 1 до N-1.

Следовательно, для того чтобы обеспечить эффективное противодействие утечки информации по акустическому каналу необходимо создать такую помеху, которая обеспечила словесную разборчивость речи очень низкого уровня.

Создание пространственных помех в помещениях объекта тесно связано с акустическими характеристиками самих помещений [3]. Акустическая классификация помещений осуществляется на основании трех параметров: высоты h, ширины b и длины l. На основании существующих требований принято три группы помещений:

1. Соизмерные $l/h \le 5$,.
2. Плоские $l/h \ge 5$ и $b/h > 4$.
3. Длинные $l/h > 5$ и $b/h < 4$.

Акустические параметры помещений позволяют проводить оптимизацию количества датчиков, используемых для обеспечения требуемой защищенности помещения. Кроме того необходимо обеспечить отсутствие «мертвых» зон в помещении.

Несмотря на то, что каждый объект по-своему уникален, при решении задач по защите зачастую приходится сталкиваться с достаточно похожими ситуациями. Это

происходит по причине схожести организации структур предприятий, зданий, построенных по типовым проектам, а главное, задач, которые необходимо решать в результате разработки системы защиты информации.

К наиболее типичным задачам можно отнести:

1. Необходимость защитить информацию специально в выделенном помещении, предназначенном для проведения конфиденциальных переговоров.

2. Необходимость защитить информацию в служебным кабинетах руководства объекта.

3. Необходимость защитить информацию на абонентском участке телефонной линии.

Из трех задач нас интересуют первые две, в которых необходимо решить вопросы с акустическим зашумлением помещений объекта.

Для создания требуемой помеховой обстановки в помещении необходимо такое размещение акустических датчиков в нем, чтобы исключить мертвые зоны и обеспечить требуемый уровень разборчивости речи.

Исходя из этих предпосылок имеем множество датчиков $V = (V_1, V_2, ..., V_l)$ разногабаритных и различных по конструкции, которые требуется разместить в заданном трехмерном параллелепипеде. Положение некоторых датчиков из множества V может быть заранее зафиксирована разработчиком.

Для рассмотрения задачи будем считать вектор $X = (x_1, x_2, ..., x_n)$ в n-мерном пространстве варьируемых координат положения датчиков и вектор $F(x) = (F_1(x), F_2(x), ..., F_m(x))$ в m-мерном пространстве локальных критериев оптимальности. При этом должны выполнятся следующие ограничения:

- параметрические:

$$x_i^{\min} \le x_i \le x_i^{\max}; \qquad i = \overline{1,n}; \tag{12}$$

- функциональные:

$$f_p^{\min}(x) \le f_p(x) \le f_p^{\max}(x); \qquad \rho = \overline{1,w}; \tag{13}$$

- критериальные:

$$F_j(x) \le F_j^*(x); \qquad j = \overline{1,m}, \tag{14}$$

где x_i – координаты положения позиций датчиков по осям X, Y, Z и угол поворота позиций датчиков плоскости; $F_j^*(x)$ – заданная точность поиска экстремума по каждому локальному критерию; $f_p(x)$ – конструктивно – технические и технологические ограничения. Символами min и max отмечены допустимые границы соответствующих параметров в (12) и (14).

Допустимая область D решения задачи образуется пересечением множеств, заданных неравенствами (12) – (14). Оптимальное размещение датчиков определяется из условия $\underset{x \in \alpha}{extr} F_u(x) = F_u(x^\circ)$, где $F_u(x^\circ)$ – интегральная целевая функция; x° – вектор оптимальных параметров, при котором получено экстремальное значение F_u.

Исследование результатов исследований позволяет выделить следующий ряд особенностей, характерных для решения задачи размещения акустических датчиков в помещении.

1. Неявная форма задания констант в неравенствах (12) – (14) в условиях отсутствия информации о $F_j(x)$.

2. Несвязность и невыпуклость области решения D, например, из-за выделения запретных зон для размещения.

3. Многоэкстремальность критериев $F_j(x)$ с «глубоким» локальным критерием в области D.

4. Локальные критерии $F_j(x)$ антагонистичны относительно друг друга.

Исходя из указанных выше особенностей задачу размещения датчиков (12) – (14) следует рассматривать, как многокритериальную задачу линейного программирования.

С этой точки зрения интерес представляют статистические алгоритмы поиска, случайный поиск [4]. Привлекательной стороной этого метода, наряду с хорошим быстродействием и сходимостью, является его универсальность в том, что он не предъявляет существенных требований к виду множества X, а также зависимостями $F_j(x)$ и $f_p(x)$.

Для поиска глобального экстремума F_u нами использован алгоритм с направляющим конусом [4].

Блок-схема алгоритма, реализующего решение задачи в постановке (12) – (14) приведена рис.1, где Q_i – вектор равномерно распределенных точек ξ_{ij}; x_{ij} - значение координаты позиции элемента в точке ξ_{ij}; $F_j^{'}(x)$, $F_j^{''}(x)$ – соответственно наилучшее и наихудшее значение локального критерия, полученного при исследовании пространства X и $F_j(x)$ с помощью равномерно распределенных точек ξ_{ij}; ψ_i – псевдослучайное число; w_i – вектор памяти; φ - угол раскрыва конуса; α – нижняя граница угла раскрытия конуса; γ_j – случайный угол поворота вектора памяти; a – величина шага в пространстве координат позиций; $\Delta x_i''$ – нормализованное на отрезке [0,1] приращение координаты x_i; Δx_i – разность между $x_i^{\max}$ и $x_i^{\min}$; b_g – величина «штрафа» при нарушении g-го ограничения (13); G_j – нормированное значение трудности достижения экстремума по j-му критерию; F_u – интегральный критерий; λ_j – коэффициент веса (приоритет) локального критерия $F_j(x)$; ΔF_u – приращение интегрального критерия на N-ом шаге поиска; N, N_1, N_2 – соответственно счетчик числа шагов поиска, поворотов вектора памяти w_i, отскоков от ограничения; M, M_1, M_2 – допустимые значения для N, N_1, N_2; h, ν – соответственно коэффициенты забывания предистории поиска и скорости обучения алгоритма поиска.

Шаг 2 – следуя [4], определяем в области D вектор Q равномерно распределенных точек $0 < \xi_{ij} < 1$, $i = \overline{1,n}$; $\gamma = \overline{1,H}$; $H = 2^K$, где K – целое число. Находим компоненты x_{ij} вектора варьируемых координат размещения X.

Шаг 3 – на множестве полученных точек x_{ij} определим $F_j^{'}(x)$ и $F_j^{''}(x)$.

Шаги 4 – 5 генерируем ψ_i, вычисляем w_i и γ_j.

Шаг 6 – определяем нормализованное приращение $\Delta x_i''$ и текущую величину координаты позиции x_i.

Шаг 7 – проверка ограничений (13).

Шаг 8 – вычисляем $F_j(x)$ с учетом «штрафа» за нарушение ограничений (13).

Шаг 9 – вычисление $F_j(x)$ при выполнении ограничений (13).

Шаги 10 – 12 – вычисления G_j, F_u, ΔF_u на N-ом шаге поиска.

Шаги 13 – 14 – проверяем величину приращения ΔF_u и выполнения ограничений (14).

Шаг 15 – выдача итоговых результатов решения задачи размещения датчиков.

Шаги 16 – 17 – наращивание числа шагов поиска экстремума F_u и проверка счетчика шагов N.

Шаг 18 – изменение величин шага поиска a, нижней границы угла раскрытия конуса α и самого угла раскрытия φ.

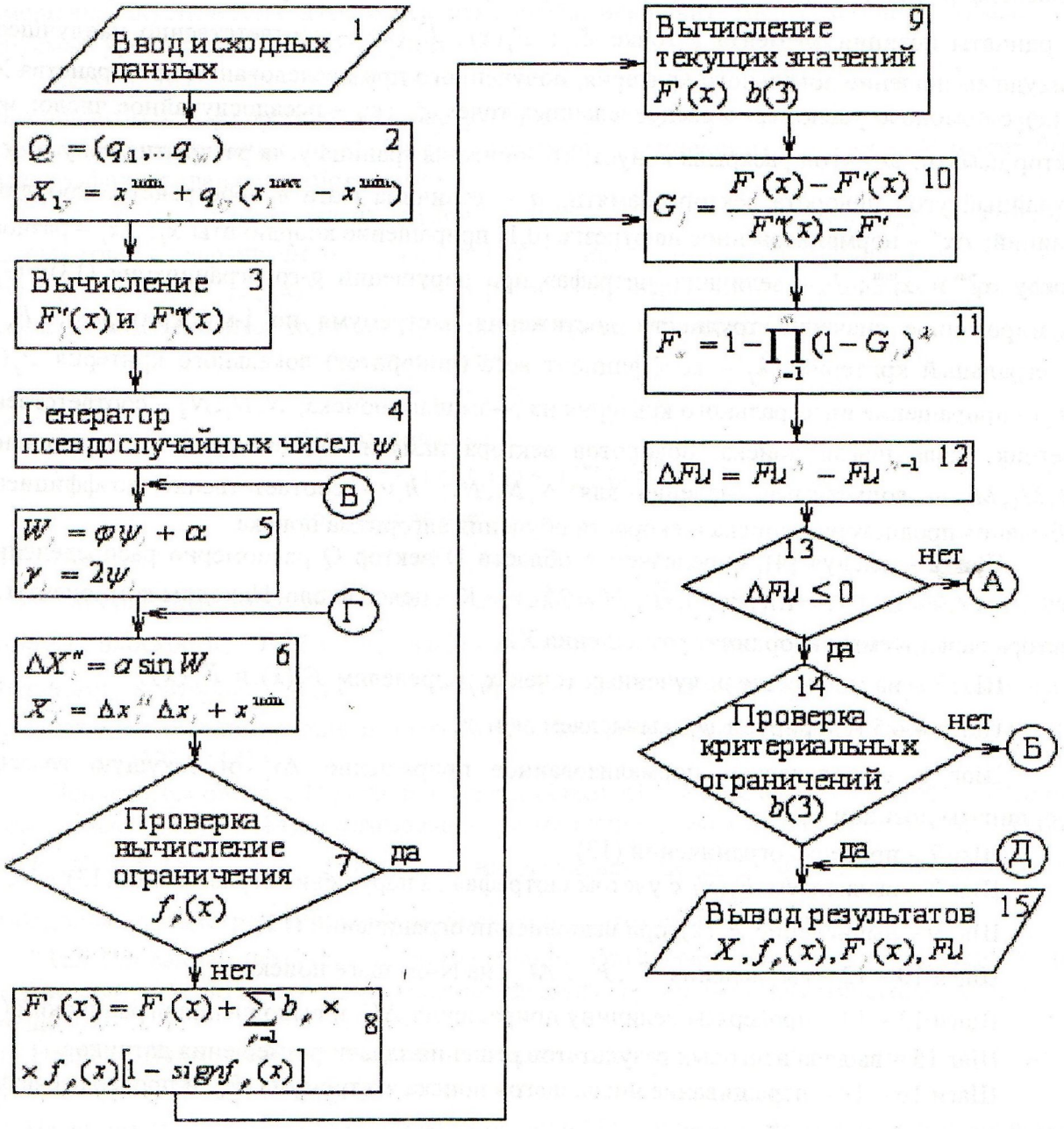
Шаги 19 – 20 – наращивание числа поворотов N_1 вектора памяти w_i и проверка счетчика по N_1.

Шаг 21 – корректировка w_i с учетом случайного угла поворота γ_j.

Шаги 22 -23 – наращивание числа отскоков N_2 от ограничения с целью выхода из локального экстремума и проверка счетчика по N_2.

Шаг 24 – определение нового значения w_i.

С помощью рекурентного выражения w_i, алгоритм поиска реагирует как на результат шага поиска, так и на степень участия определенной координаты позиции x_i на величину F_u.



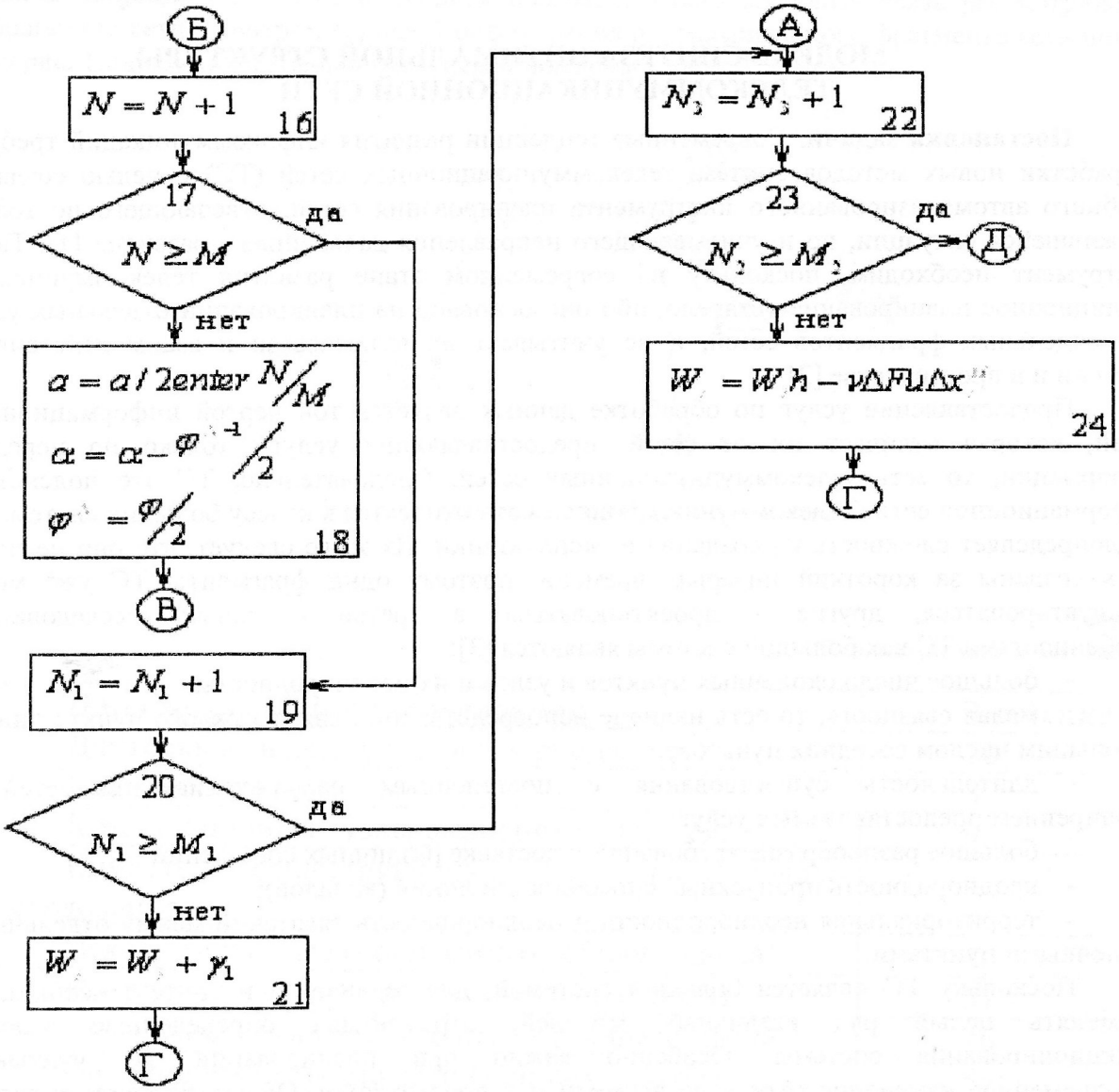


Рис. 1. Блок-схема алгоритма

Список литературы

1. *Хорев А.А., Макаров Ю.К.* Методы защиты речевой информации и оценка их эффективности//Защита информации. Конфидент. – 2001. - №4. – с.22 – 33.

2. *Покровский Н.Б.* Расчет и измерение разборчивости речи. М.: Связьиздат, 1962. – 391с.

3. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504с.

4. *Растригин Л.А.* Статистические методы поиска. – М.: Наука, 1988. – 320с.

Поступила 07.09.2006