ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 621.372:004.415.24

СИСТЕМНЫЙ ПОДХОД: ЗАЩИТА ИНФОРМАЦИИ, ПОМЕХОЗАЩИЩЕННОСТЬ, ПОМЕХОУСТОЙЧИВОСТЬ

д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, канд. техн. наук Д.С. РЯБЕНКО, С.В. ЛАВРОВ
(Полоцкий государственный университет)

Опираясь на основные положения системного подхода, разработана модель защиты информации во взаимосвязи с помехозащищенностью и помехоустойчивостью. Помехозащищенность в низкочастотном диапазоне оценивают сформированным стабильным шумовым сигналом с помощью колец Гельмгольца. На основании помехоустойчивости оптимальным приемником устанавливают меру защиты речевой информации научно-обоснованным численным значением показателя разборчивости речи. Полноту оценки защищенности объектов информатизации обеспечивают в соответствии с требованиями научно-методических документов.

Ключевые слова: *защита информации, помехоустойчивость, помехозащищенность.*

Введение. Информационная безопасность устанавливает необходимость разработки системы защиты информации (ЗИ), включающей требования, положения и рекомендации основных законодательных актов, нормативно-методических документов государственных учреждений и организаций, материалов международных конференций в области ЗИ, а также международных стандартов в области безопасности информации и информационных технологий. Основными принципами, на которых строится такая система, являются [1]:

- системность и комплексный подход создания системы ЗИ с учетом всех взаимосвязанных изменяющихся во времени элементов, условий и значимых факторов;
- разумная достаточность при создании системы ЗИ, предполагающая такой уровень защиты, при котором затраты, риски от возможного ущерба были бы приемлемыми;
- гибкость системы ЗИ с последующим (поэтапным) наращиванием уровня защищенности;
- непрерывности ЗИ на всех этапах жизненного цикла ее функционирования;
- ценности информации при использовании ее в различных областях целенаправленной деятельности по разработке и эксплуатации сложных высокотехнологичных систем [1].

Основной проблемой создания системы ЗИ являются показатели ее безопасности. Системные меры безопасности реализуют показатели [1]:

- защищенности охраняемых сведений системы;
- защищенности целостности оперативной информации;
- защищенности от блокирования информации;
- защищенности информации от силовых воздействий.

Угрозами информационной безопасности являются модели [1]:

- вскрытия охраняемых сведений;
- нарушения целостности оперативной информации;
- блокирования информации;
- силового воздействия на информацию.

Модель защиты информации. Объекты информатизации (ОИ) включают автоматизированные системы формирования, обработки, преобразования, анализа, синтеза моделирования сигналов различного назначения в аналоговой, цифровой форме. Системы многофункционального и многомерного назначения представляются многоуровневыми моделями. Анализ таких моделей характеризуется при недостаточном объеме априорных сведений.

К априорным сведениям любого назначения информационных систем предъявляют требования высокой точности, чувствительности, помехозащищенности, высокого разрешения по частоте. Не менее сложной задачей является определение целевой функции и критериальных показателей. К таковым предъявляются требования полноты, обобщенности, непротиворечивости, предпочтительности, эффективности.

Защищенность на ОИ устанавливается как приоритетное направление. Параметры, важнейшие характеристики защищенности определяют тесную связь с параметрами и характеристиками информационных систем ОИ. Информационные поля рассеивания формируют каналы утечки информации (КУИ) информационных систем. Параметры информационных сигналов, наведенные информационными полями рассеивания, являются случайными. Представление информационных полей рассеивания является векторным со случайными численными значениями и направлениями. Уровни излучений информационных полей рассеивания снижают их локализацией и схемно-конструктивными решениями. Нормированный показатель, устанавливающий защищенность КУИ от утечки, соответствует значению δ. В случае недостижимости значения δ используют методы активного подавления маскирующими шумовыми сигналами, снижая помехозащищенность информационных систем ОИ. Повышение помехозащищенности ОИ обеспечивает их энергетическую и структурную скрытность [2]. Модель ЗИ представлена на рисунке 1.

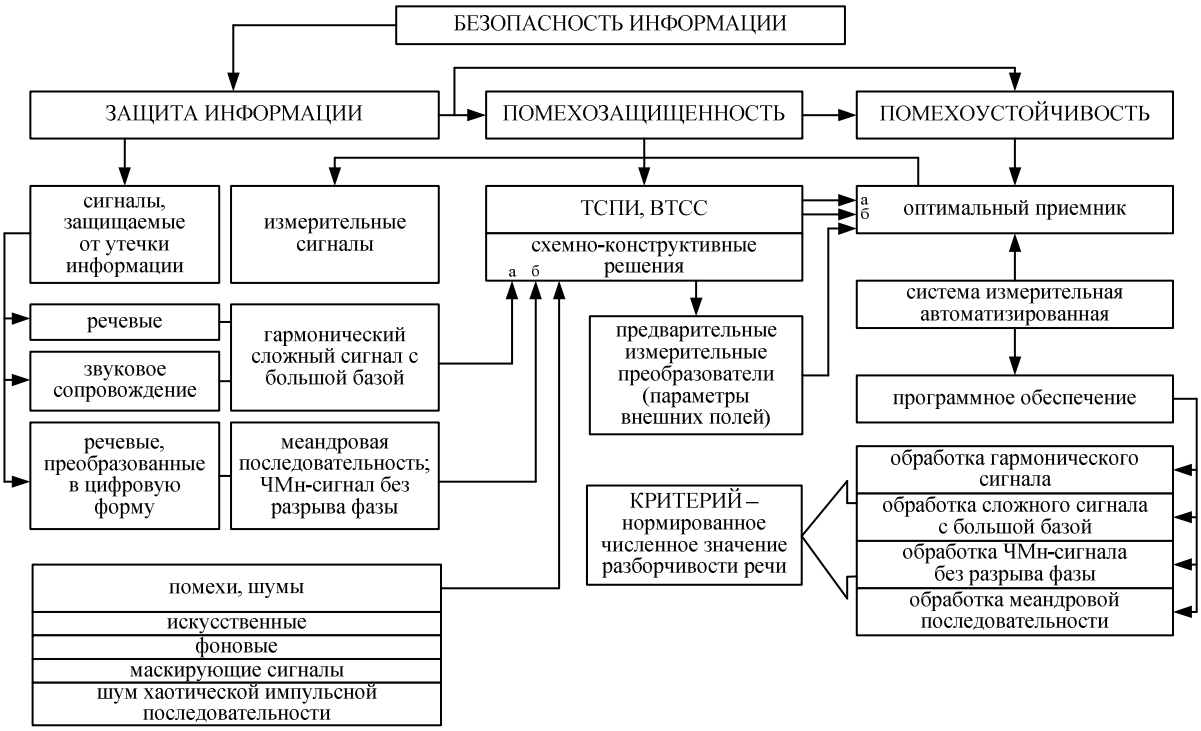

Рисунок 1 – Модель защиты информации

На рисунке 1 представлены следующие сокращения: ТСПИ – технические средства передачи информации; ВТСС – вспомогательные технические средства и системы; а, б – параметры сигналов на входе.

Система измерительная автоматизированная с программными компонентами генерирует измерительные сигналы и измерение их параметров, преобразовывает физические поля рассеивания в сигналы КУИ первичными измерительными преобразователями и обрабатывает оптимальным приемником. В зависимости от сигналов, защищаемых от утечки информации, различают измерительные сигналы:

- гармонический сложный сигнал с большой базой (линейно-частотно-модулированный – ЛЧМ) – для речевых сигналов и сигналов звукового сопровождения видео;
- меандровая последовательность – для речевых сигналов, преобразованных в битовую последовательность;
- частотно-манипулированный сигнал без разрыва фазы – для речевых сигналов, преобразованных в цифровую форму.

Система измерительная автоматизированная осуществляет сбор первичной информации от всех видов КУ речевой информации (акустический, виброакустический, электроакустический, магнитный, электрический, наводок сигналов рассеивания этих каналов на цепи управления, питания и заземления) путем преобразования физических информационных полей рассеивания в электрический сигнал. Сис-

тема оценивает величину разборчивости речи в КУИ со слабыми сигналами в шумах высокого уровня в соответствии с требованиями нормативно-методических документов и обеспечивает полноту оценки защищенности ОИ.

Контроль защищенности речевой информации и принятых мер ЗИ опирается на оценку физических параметров сигналов и фоновых шумов в КУИ с последующим автоматизированным расчетом обоснованного критерия – нормированного значения величины разборчивости речи.

Для оценки помехозащищенности в НЧ-диапазоне частот формируют стабильный шумовой сигнал. Такой сигнал формируется мерами напряженности магнитного поля в виде катушек (колец) Гельмгольца, по которым протекает электрический ток [3]. К таким катушкам предъявляются требования высокой точности, высокой стабильности по времени, обеспечения большого объема рабочего однородного поля. Кроме колец Гельмгольца используют системы контуров с током и соленоиды, обеспечивающие однородное поле и малые поля рассеивания за их пределами при наименьшем числе элементов системы [3–5].

Катушка Гельмгольца представляет два круговых контура одинакового радиуса R либо два квадратных контура с одинаковыми сторонами квадратов (рис. 2). Катушка Гельмгольца в виде круговых либо квадратных контуров должна обеспечивать выполнение следующего условия $2a = R$, где $2a$ – расстояние между катушками, R – радиус каждого из круговых контуров. Весьма высокой однородностью магнитного поля обладает катушка Гельмгольца, выполненная на квадратном каркасе, который проще в изготовлении. Они пригодны для использования при формировании достаточно однородного поля в большом объеме.

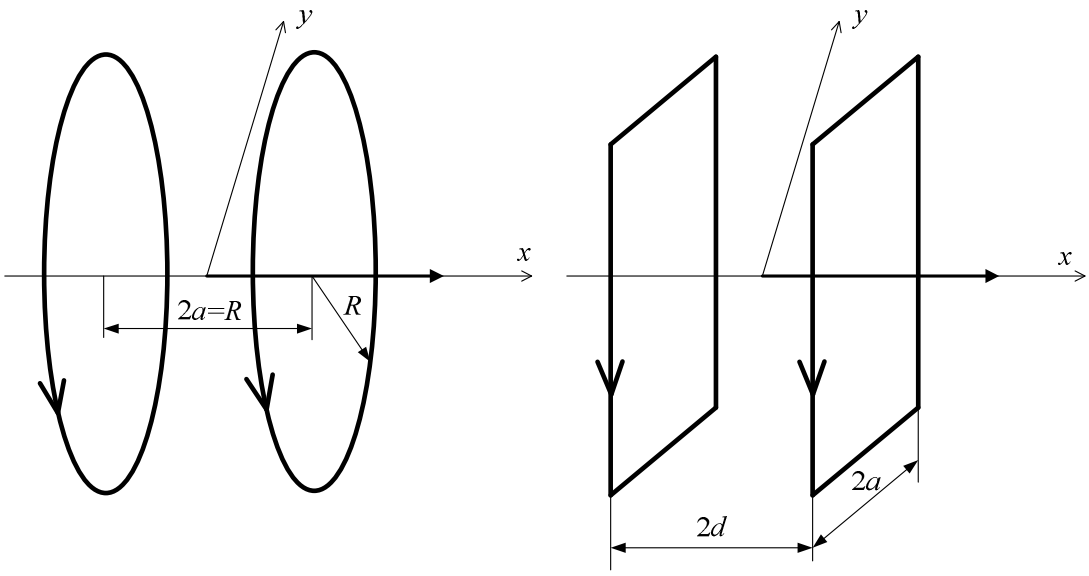

Рисунок 2 – Кольца Гельмгольца:
$2d$ – расстояние между секциями; $2a$ – сторона квадрата, образуемая обмоткой

Достаточно высокая равномерность поля квадратной катушки достигается при соотношении размеров $d/a = 0{,}5445$ [3].

Напряженность поля в центре квадратной катушки Гельмгольца определяется [3]:

$$H_{\text{ц}} = \frac{0{,}64806In}{a}\left(1 - 0{,}5388\frac{\Delta}{a}\right), \tag{1}$$

где n – число витков одной секции;

Δ – параметр неточности изготовления катушки, $\Delta = (2d - 0{,}5445 \cdot 2a)$.

Напряженность поля в центре квадратных катушек при значительном отклонении от числа 0,5445 определяют по отношению d/a [3]:

$$H_{\text{ц}} = \frac{4a^2 In}{\pi(a^2 + d^2)\sqrt{2a^2 + d^2}}. \tag{2}$$

Сдвоенные кольцевые и квадратные катушки колец Гельмгольца применяют в системах сдвоенных катушек для получения высокой степени равномерности поля. Напряженность поля уменьшается для квадратных катушек [3]:

$$H_{д} = \frac{0,64806In_1}{a_1}\left(1-\frac{a_2^4}{a_1^4}\right). \quad (3)$$

Проблема повышения помехозащищенности и защищенности от утечки информации ОИ является актуальной. Локализацию информационных магнитных полей рассеивания реализуют их экранированием с одновременной вынужденной деформацией полезного сигнала. Снижение весогабаритных характеристик аппаратуры весьма актуально. Экранам присуще изменять свои экранирующие свойства при воздействии на них ударов и вибраций. Актуальным является локализация полей рассеивания. Пассивные методы ЗИ повышают энергетическую и структурную скрытность [2], но не решают в полной мере поставленную проблему помехозащищенности и ЗИ, так как эти проблемы взаимоисключающие.

Для повышения защищенности информации практикуют активные методы защиты. Активные методы защиты основаны на формировании маскирующих сигналов, которые повышают порог чувствительности при приеме информационных полей рассеивания. Таким образом, при определенных энергетических показателях (отношение сигнал/шум) обеспечивается защищенность ОИ повышением порога чувствительности приема информационных полей рассеивания. Информационные поля рассеивания характеризуются многовекторностью, формирующих информационное векторное поле.

Важным является разрушение КУИ активными способами – путем маскирования информационных и демаскирующих параметров сигналов маскирующими помехами. Активные методы ЗИ основаны на формировании преднамеренных шумов, обладающих необходимой эффективностью по заданному критерию эффективности, выбор которого обоснован в [6].

Для маскирования широко используют белый шум с ограниченной полосой [7]. Спектральные составляющие белого шума равномерно распределены по всему диапазону задействованных частот. Функция распределения плотности вероятности имеет вид [7]

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-A)^2}{2\sigma^2}}, \quad (4)$$

где σ^2 – дисперсия шума;

A – математическое ожидание случайной величины.

Полностью свойства случайного процесса описываются этим распределением. Методика обработки результатов наблюдений случайного процесса на статистическую устойчивость наблюдений известна [7]. Функция распределения и ее числовые характеристики являются полными характеристиками случайных величин.

Маскирующие помехи, сформированные непосредственно из сигнала (видео-, речевой), наиболее адаптированы к его параметрам [8]. В качестве источников генерации преднамеренных маскирующих шумов широко распространены шумовые диоды.

Основные параметры и характеристики помехи определяются источниками генерации преднамеренных маскирующих шумов, а усилительные каскады формируют частотный диапазон, при необходимости ограничивая его. Необходимые коррекции вводятся для регулировки напряжения, мощности выходных сигналов, согласования с нагрузкой, выполнения измерительных и контролирующих функций параметров и характеристик.

Генератор маскирующих сигналов. Структура маскирующих шумов представляет сумму флуктуационной (шумовой) и импульсной компонент [7]. В импульсной компоненте сосредоточена значительная часть энергии, поэтому она оказывает существенное влияние на прием и обработку информационного сигнала в КУИ:

$$f(x) = \frac{1-\alpha}{\sqrt{2\pi}\sigma_{ф}}\exp\left(-\frac{x^2}{2\sigma_{ф}^2}\right) + \frac{\alpha}{\sqrt{2\pi}\sigma_{и}}\exp\left(\frac{x^2}{2\sigma_{и}^2}\right). \quad (5)$$

Функция $f(x) = f(x;t)$ состоит из двух гауссовых плотностей вероятности, параметры которых $\sigma_{ф}^2$ и $\sigma_{и}^2$ характеризуют соответственно дисперсии флуктуационной и импульсной компонент. Коэффициент α определяет импульсную составляющую шума.

Применительно к спектральному оцениванию очень важной является матрица Тёплица. Матрица обладает тем свойством, что все ее элементы, расположенные на любой диагонали, идентичны.

Спектральное оценивание шумов генератора маскирующего шума соответствует теплицевой диагональной матрице, т.е. оно $t\,[i, j]$ идентично.

Моделирование невырожденного многомерного нормального распределения определяется корреляционной матрицей

$$\begin{bmatrix} K_{11} & K_{12} & . & K_{1n} \\ K_{21} & K_{22} & . & K_{2n} \\ . & . & . & . \\ K_{n1} & K_{n2} & . & K_{nn} \end{bmatrix}, \qquad (6)$$

где $K_{ij} = M\left(\left(\xi_i - m_1\right)\left(\xi_i - m_j\right)\right)$, вектор ξ определяется специальным линейным преобразованием вектора $\eta = \left(\eta_1, ..., \eta_n\right)$, компоненты которого суть нормально распределенные случайные величины с параметрами $m = 0$, $\sigma = 1$.

Для формирования маскирующего сигнала из шумового сигнала выделяют такие частотные спектры, которые соответствуют резонансным, т.е. усиленным частотным областям спектра речи (формантам) [9], каждого гласного звука речи. Затем выбирают по одному резонансному частотному спектру из каждой i-й группы частотных спектров, соответствующих спектру речевого сигнала, и смешивают между собой, где $i = 1, 2, ..., N$. После чего спектральные составляющие усиливают. Причем смешиваемые усиленные (резонансные) частотные области спектра выбирают по случайному закону через установленные интервалы времени.

Актуальным является повышение надежности защиты речевых сигналов одновременно в аналоговой и цифровой форме, видеосигналов и сигналов звукового сопровождения, сигналов передачи данных.

Маскирующий сигнал формируют для энергетического подавления маскируемого сигнала. Предложен вариант формирования маскирующей помехи [10], основной принцип которого заключается в том, что формируют шумовой сигнал, из которого создают маскирующий сигнал, затем шумовой и маскирующий сигналы суммируют. Для формирования маскирующего сигнала сформированный шумовой сигнал усиливают и разделяют на n параллельных полос от нижней частоты $f_{\text{н}}$ до верхней $f_{\text{в}i}$, где $i = \overline{1, n}$, причем каждая последующая полоса от $f_{\text{н}}$ до $f_{\text{в}i+1}$ шире всех предыдущих полос $(f_{\text{н}} \div f_{\text{в}1}) < (f_{\text{н}} \div f_{\text{в}2}) < ... < (f_{\text{н}} \div f_{\text{в}i})$.

Усиливают сигнал каждой полосы. Затем такие сигналы преобразуют в хаотическую импульсную последовательность (ХИП) с различными случайными длительностями τ и случайными периодами. Полученные ХИП каждой полосы регулируют по амплитуде, суммируют ХИП всех полос, и сигнал полученной ХИП нормируют. В результате получают маскирующий сигнал, который суммируют с шумовым сигналом. Суммарный сигнал возводят в квадрат по амплитуде, в результате получают шумовую помеху. Данную шумовую помеху суммируют с другой шумовой помехой, сформированной аналогичным образом, сумму сигналов усиливают, согласуют с нагрузкой, получая маскирующую помеху.

Предложенный метод [10] формирования маскирующей помехи реализуют следующим образом. Формируют шумовой сигнал. Сформированный шумовой сигнал усиливают и разделяют параллельной фильтрацией на n сигналов. Развязывающие согласующие усилительные каскады согласуют по входу и выходу фильтров нижних частот. Следовательно, изменяется верхняя частота шумового процесса (шумового сигнала), при увеличении $f_{\text{в}}$ – увеличивается и число пересечений случайного процесса и соответственно уменьшается среднее значение длительности импульсов [11]. Разбивая полосу шумового сигнала на ряд полос с различными частотами $f_{\text{в}}$, формируют импульсы с различной шириной и скважностью.

Из импульсов с различной шириной и скважностью формируют N входов ХИП. Поскольку частоты среза $f_{\text{в}}$ полосовых шумовых сигналов отличны, длительность импульсов и частота повторения ХИП случайны. Чем ниже частота среза $f_{\text{в}}$, тем большая длительность импульсов превышает длительность импульсов ХИП, сформированных более высокими по частоте $f_{\text{в}}$ шумовыми сигналами, из которых образуют импульсную последовательность. Далее формируют спектральные характеристики ХИП, близкие к спектральным характеристикам видеосигнала или речевого сигнала в цифровой форме, или цифровых сигнальных последовательностей. Для формирования маскирующей помехи производят возведение в квадрат по закону хи-квадрат распределения суммы маскирующего сигнала и шумового, которые являются нормально распределенными случайными величинами.

Хаотическую импульсную последовательность каждой полосы регулируют по амплитуде и суммируют последовательности всех полос. Сигнал полученной ХИП нормируют, в результате получают маскирующий сигнал. Данный маскирующий сигнал суммируют с шумовым сигналом с нормальным распределением, суммарный сигнал возводят в квадрат по закону хи-квадрат распределения [12] с известным числом степеней свободы $\upsilon = 2$.

В результате получаем шумовую помеху. Данную шумовую помеху суммируют с другой шумовой помехой, сформированной аналогичным образом, сумму сигналов усиливают, согласуют с нагрузкой, получая маскирующую помеху.

В суммарном сигнале на выходе сумматора присутствуют низкочастотные, среднечастотные и высокочастотные составляющие ХИП. Их отображение на экране представляется в виде линий различной длины и точек. Суммированием хаотических импульсных сигналов, возведенных в квадрат, реализуется закон хи-квадрат распределения. Наличие среднечастотных и высокочастотных составляющих хорошо разрушает краевые очертания изображений.

ЛИТЕРАТУРА

1. Общесистемные вопросы защиты информации / под. общ. ред. А.А. Сахнина – М. : Радиотехника, 2003.
2. Помехоустойчивость систем со сложными сигналами / Г.И. Тузов [и др.] ; под. ред. Г.И. Тузова. – М. : Радио и связь. 1985. – 264 с.
3. Магнитные измерения / Е.Т. Чернышев [и др.]. – М. : Изд-во стандартов, 1969. – 248 с.
4. Средства измерения параметров магнитного поля / Ю.В. Афанасьев [и др.]. – Л. : Энергия, 1979. – 320 с.
5. Студенцов, Н.В., Построение безмоментных мер магнитной индукции с однородным полем / Н.В. Студенцов, В.Н. Хорев // Проблемы повышения точности средств измерений магнитной индукции : сб. науч. тр. ; под ред. Н.В. Студенцова и В.Я. Ширмана. – Л. : Энергоатомиздат, 1983. – С. 7–13.
6. Железняк, В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – СПб. : ГУАП, 2006. – 188 с.
7. Тихонов, В.И. Проблема пересечений уровней случайными процессами / В.И. Тихонов, В.И. Хименко // Радиотехника и электроника. – 1998. – № 5, Т. 43. – С. 501–523.
8. Железняк, В.К., Автоматизированная оценка маскирующего шума вречевом диапазоне частот / В.К. Железняк, Р.С. Карасев // Информационные системы и технологии (IST 2009) : материалы V Междунар. конференции-форума, Минск, 16-17 ноября 2009 г. : в 2 ч. / редкол.: Н.И. Листопад [и др.]. – Минск, 2009. – Ч. 2. – С. 42–46.
9. Военные коммутационные системы и телефония / Л.П. Щербина [и др.] ; под ред. Л.П. Щербины. – Л. : ВАС, 1990. – 424 с.
10. Способ формирования сигнала для маскирования речевых сигналов, видеосигналов и сигналов передачи данных : пат. 19227 Респ. Беларусь, МПК H 04K 1/00, H 04K 3/00 / В.К. Железняк, Д.С. Рябенко ; дата публ. 30.06.2015.
11. Бендат, Дж.С. Основы теории случайных шумов и ее применение / Дж.С. Бендат ; пер. с англ. под ред. В.С. Трачева. – М. : Наука, 1965. – 464 с.
12. Иган, Дж. Теория обнаружения сигналов и анализ рабочих характеристик / Дж. Иган ; пер. с англ. под ред. Б.Ф. Ломова. – М. : Наука, 1983. – 216 с.
13. Тихонов, В.И. Оптимальный прием сигналов / В.И. Тихонов. – М. : Радио и связь, 1983. – 320 с.

Поступила 02.03.2016

SYSTEM APPROACH: INFORMATION PROTECTION, NOISE IMMUNITY, NOISE STABILITY

V. ZHELEZNYAK, D. RYABENKO, S. LAVROV

The model of protection of the information in interrelation with noise immunity and a noise stability by means of the system concept is developed. Noise immunity in low frequency range of frequencies estimate a stable noise signal by means of Helmholtz coils. The optimum receiver establishes a measure of protection of the speech information the scientifically-proved numerical value of an indicator of legibility of speech on the basis of noise stability. Requirements of scientifically-methodical documents realize completeness of an estimation of security in information objects.

Keywords: *information protection, noise immunity, noise stability.*