Методическая разработка

для проведения лекции

Занятие 8. Классификация образов с помощью функций правдоподобия

Учебные вопросы занятия:
1. Классификация образов как задача теории статистических решений
2. Байесовский классификатор в случае образов, характеризующихся нормальным распределением

Заключительная часть

Введение

Одной из важнейших задач информационной безопасности является задача распознавания образов, будь то обнаружение атаки, идентификация нарушителя, определение вида уязвимости и т.д. Острота решаемой проблемы заключается в том, что приходится решать следующие задачи:

- при огромнейших объемах обрабатываемой информации и постоянном дефиците сил и средств сохранять свою полную работоспособность. Следовательно, необходимо внедрение автоматизации процессов приема и обработки;

- постоянно обеспечивать признаковую доступность к объектам и источникам информации.

Очевидно, что эти задачи относятся к задачам распознавания образов и принятия решений. В силу огромнейших объемов обрабатываемой информации и требований к системе по обработке данной информации в реальном масштабе времени решить данные задачи ручными методами невозможно.

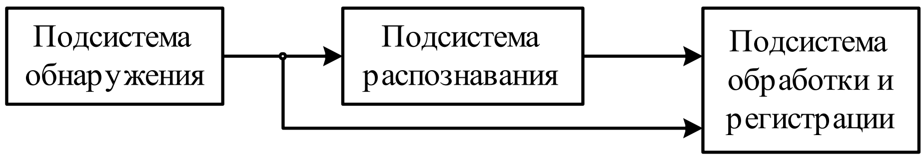
Для автоматизации решения задач такого типа необходим математический аппарат при описании происходящих процессов и процедур принятия решения. Этим занимается теория распознавания образов. Следовательно, для обеспечения работоспособности какого-либо устройства, подсистемы или системы в целом необходимо изучить элементы математического анализа и теории распознавания образов.

1. Классификация образов как задача теории статистических решений

С позиций системного подхода для изучения систем классифицирования (распознавания) необходимо сформулировать цель распознавания как такового и определить место распознавателя в технологическом процессе приема и обработки информации.

Целью функционирования любой системы распознавания является отнесение анализируемого образа к какой-либо группе объектов (классу) в соответствии с выбранной системой признаков.

Место устройств распознавания в структуре автоматизированного комплекса показано на рисунке.



Поскольку в рамках любого конкретного исследования все используемые термины и понятия должны быть точно и четко определены, введем основные определения, связанные с классифицированием.

Класс – множество объектов (предметов, явлений), объединенных некоторыми общими свойствами.

Объект является представлением своего класса.

Признак – общее свойство, объединяющее объекты в классы. Признаками могут быть только те свойства объектов, численные значения которых можно измерить.

Образ – совокупность значений признаков, характеризующих объект, и дающих его описание.

Так как прием и обработка информации осуществляются в условиях наличия различного рода случайных воздействий, то измеренные значения признаков – случайные величины. В зависимости от них реализацию образа относят к одному из заданных классов по выбранным правилам принятия решения. При этом обычно принятие решения производится сравнением реализации сигнала с эталонами классов.

Эталон – типичный представитель класса или образец с усредненными значениями параметров.

На основании введенных определений задачи системы распознавания можно представить в следующем виде:

– разбиение множества элементов на классы $\{A_i\}$;

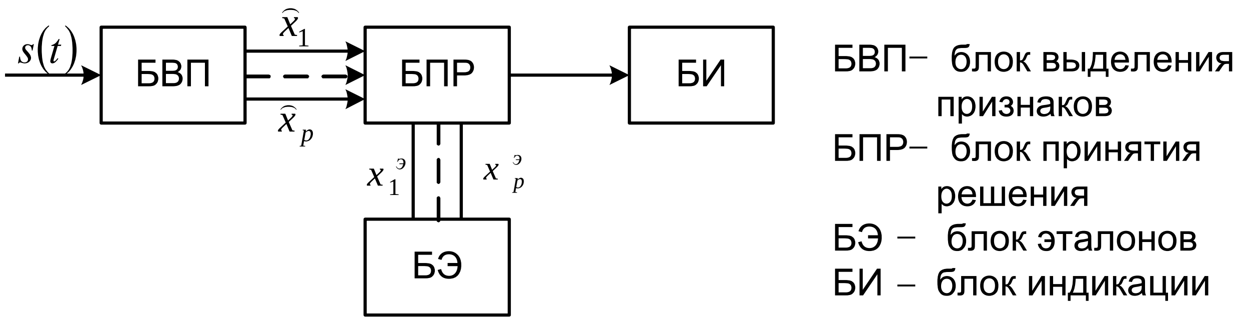
– выбор пространства признаков распознавания $A_i \Rightarrow P_i = \{p_k\}$;

– обучение системы распознавания (изменение эталона и признакового пространства, создание новых классов);

– разработка методов и алгоритмов распознавания (измерение порогов, выбор решающего правила);

– оценка эффективности системы распознавания в различных условиях ее функционирования (степень достижения цели функционирования системой распознавания).

Исходя из поставленных задач и преследуемой цели следует определить модель системы распознавания и представить ее в виде структурной схемы.



При распознавании воздействий на ПЭВМ или сервер первоначально выделяются (измеряются) признаки, которыми могут быть различные характеристики (параметры) воздействий и их сочетания. Принятая реализация воздействия поступает в блок выделения признаков (БВП), где измеряются его параметры. Оценки этих параметров сравниваются в блоке принятия решения (БПР) с эталонными значениями признаков, поступающими из блока эталонов (БЭ). Регистрация и отображение принятого решения производится в блоке индикации (БИ).

Рассмотрим основные виды методов распознавания: детерминистские, статистические, логические и синтаксические (лингвистические). Наибольшее внимание будет сосредоточено на статистических методах, поскольку они в наилучшей степени учитывают условия обеспечения информационной безопасности.

Математическое описание наиболее важных элементов этой модели базируется на принципах статистического описания различных образов и классификационных правилах, являющихся *оптимальными* в том смысле, что их использование обеспечивает в среднем наименьший риск от принятия неправильного решения о классификации.

Оптимальному качеству классификации со статистической точки зрения соответствует байесовский классификатор. Алгоритм его действия определяется выражением для математического ожидания потерь, обусловленных отнесением описания к некоторому классу *j*.

Выражение для средних потерь, возникающих при отнесении образа к классу *j*, сводится к следующему уравнению:

$$R_j(x) = \sum_{i=1}^{M} L_{ij}\, \omega(x/A_i) P(A_i),$$

где $L_{i\,j}$ – величина потерь, связанных с отнесением образа *x* к классу *j*, когда в действительности он принадлежит классу *i*;

$\omega(x/A_i)$ – плотность распределения вероятностей признака *x*.

В теории статистических решений величину $R_j(x)$ часто называют *условными средними потерями*.

При распознавании каждого образа его можно отнести к одному из *M* возможных классов. Если для каждого образа *X* вычисляются значения условных средних потерь $R_1(x), R_2(x), \ldots, R_M(x)$, и классификатор причисляет его к классу, которому соответствуют наименьшие условные потери, то очевидно, что и математическое ожидание полных потерь на множестве всех решений будет минимизировано. Классификатор, минимизирующий математическое ожидание общих потерь, называется байесовским классификатором.

Если *M* = 2, то при выборе класса 1 средние потери для предъявленного образа *X* составляют

$$R_1(x) = L_{11}\,\omega(x/A_1)P(A_1) + L_{21}\,\omega(x/A_2)P(A_2),$$

а для класса 2 –

$$R_2(x) = L_{12}\,\omega(x/A_1)P(A_1) + L_{22}\,\omega(x/A_2)P(A_2).$$

Как уже отмечалось, байесовский классификатор обеспечивает отнесение образа *X* к классу A_i с наименьшим значением средних потерь R_j, значит, образ *X* зачисляется в класс A_1, если выполняется условие $R_1(x) < R_2(x)$.

Подставив в данное неравенство значения условных средних потерь, получим

$$L_{11}\,\omega(x/A_1)P(A_1) + L_{21}\,\omega(x/A_2)P(A_2) <$$

$$< L_{12}\,\omega(x/A_1)P(A_1) + L_{22}\,\omega(x/A_2)P(A_2)$$

или

$$(L_{21} - L_{22})\omega(x/A_2)P(A_2) < (L_{12} - L_{11})\omega(x/A_1)P(A_1),$$

$$\frac{\omega(x/A_1)}{\omega(x/A_2)} > \frac{(L_{21} - L_{22})P(A_2)}{(L_{12} - L_{11})P(A_1)}.$$

Выполнение этого условия определяет отнесение образа X к классу A_1. Левую часть неравенства называют *отношением правдоподобия* (оно является отношением двух функций правдоподобия). Величину

$$\Theta_{12} = \frac{(L_{21} - L_{22})P(A_2)}{(L_{12} - L_{11})P(A_1)}$$

часто называют *пороговым значением*.

В большинстве задач распознавания образов потери равны нулю (отсутствие потерь) при принятии правильного решения и единице – неправильного. Это соотношение устанавливает нормированную величину потерь, равную единице при неправильной классификации, и отсутствие потерь в случае правильной классификации образа. Поэтому функцию потерь можно представить следующим выражением:

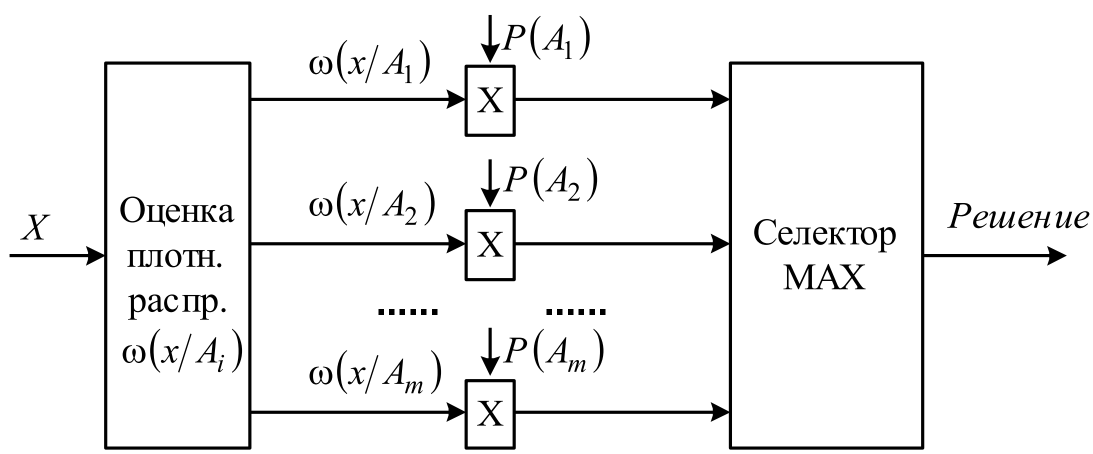
$$L_{ij} = 1 - \delta_{ij},$$

где δ_{ij} – число Кронекера; $\delta_{ij} = 1$ при $i=j$, $\delta_{ij} = 0$ при $i \neq j$.

Отсюда следует, что байесовский классификатор обеспечивает отнесение образа X к классу A_i, если выполняется условие

$$\omega(x/A_i)P(A_i) > \omega(x/A_j)P(A_j), \quad j = 1, 2, .., M, \quad i \neq j.$$

Приведенные рассуждения позволяют на основе этого выражения реализовать схему распознавания, изображенную на рисунке.



Выводы:

Оптимальным с точки зрения нормирования потерь является байесовский классификатор.

Синтез байесовского классификатора требует знания априорных вероятностей и плотностей распределения для каждого класса образов, а в общем случае и стоимостей принятия решений.

2. Байесовский классификатор в случае образов, характеризующихся нормальным законом распределения

Одномерная плотность нормального распределения одной случайной величины x может быть представлена следующим выражением:

$$\omega(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\frac{(x-m)^2}{\sigma^2}}$$

Основными параметрами указанного закона распределения являются среднее значение m и дисперсия σ^2, поэтому часто его представляют в виде функции $N(m, \sigma^2)$. Эти параметры, в свою очередь, определяются следующим образом:

$$m = M[x] = \int_{-\infty}^{\infty} x\,\omega(x)\,dx,$$

$$\sigma^2 = M\left[(x-m)^2\right] = \int_{-\infty}^{\infty} (x-m)^2\,\omega(x)\,dx.$$

Образы, характеризующиеся нормальным распределением, проявляют тенденцию к группировке вокруг среднего значения, а их рассеяние – пропорционально среднеквадратическому отклонению σ. Около 95 % объектов, извлеченных из совокупности с нормальным распределением, попадут в интервал, равный 2σ и имеющий в качестве центра среднее значение m.

Рассмотрим M классов образов. Элементы этих классов описываются p-мерными случайными величинами $x_1, x_2, \ldots, x_p$. Совокупность p случайных величин будем обозначать вектором или матрицей-столбцом $x = \begin{bmatrix} x_1 \\ x_2 \\ \ldots \\ x_p \end{bmatrix}$. Будем рассматривать случайные величины, которые имеют в каждом классе p-мерную нормальную плотность распределения:

$$\omega(x/A_i) = \frac{1}{(2\pi)^{p/2}\left|C_i\right|^{1/2}} e^{-\frac{1}{2}(x-m_i)^T C_i^{-1}(x-m_i)},$$

где i=1, 2, …, M;

$\left|C_i\right|$ – определитель ковариационной матрицы C_i;

$(x-m_i)^T$ – транспонированная матрица $(x-m_i)$.

Каждая условная плотность распределения полностью определена вектором средних значений m_i и ковариационной матрицей C_i, заданных соответственно:

$$m_i = M_i[x],$$

$$C_{jk}^i = \operatorname{cov}(x_i x_k) = M[(x_j - m_j^i)(x_j - m_k^i)],$$

где i=1, 2, …, M – номер класса;

j,k=1, …, p – номер случайной величины;

$$C_i = M_i[(x-m)(x-m)^T],$$

где M_i обозначает оператор математического ожидания, определенный на образах класса A_i:

$$C_i = \begin{bmatrix} c_{11}^i & c_{12}^i & \dots & c_{1p}^i \\ c_{21}^i & c_{22}^i & \dots & c_{2p}^i \\ \dots & & & \\ c_{p1}^i & c_{p2}^i & \dots & c_{pp}^i \end{bmatrix}.$$

Ковариационная матрица C_i является симметрической и положительно полуопределенной. Ее диагональный элемент c_{kk} есть дисперсия k-го элемента вектора образов. Элемент c_{jk}, не стоящий на диагонали матрицы, представляет собой ковариацию случайных переменных x_j и x_k (*ковариация* – смешанный момент второго порядка $\operatorname{cov}(x_i, x_j)$). Если переменные x_j и x_k независимы, то элемент $c_{jk} = 0$. Многомерная плотность нормального распределения сводится к произведению одномерных плотностей нормальных распределений, если все недиагональные элементы ковариационной матрицы равны нулю.

Отношение правдоподобия нормально распределенных случайных величин можно представить выражением

$$\frac{\omega(x/A_i)}{\omega(x/A_j)} = e^{-\frac{1}{2}\left[(x-m_i)^T C_i^{-1}(x-m_i) - (x-m_j)^T C_j^{-1}(x-m_j)\right]}.$$

Так как ковариационная матрица симметрическая, данное отношение сводится к следующему выражению:

$$\frac{\omega(x/A_i)}{\omega(x/A_j)} = e^{x^T C_i^{-1}(m_i - m_j) - \frac{1}{2}(m_i + m_j)^T C_j^{-1}(m_i - m_j)}.$$

Введем функцию

$$u_{ij}(x) = \ln\left(\frac{\omega(x/A_i)}{\omega(x/A_j)}\right).$$

Тогда для разделяющей функции получаем

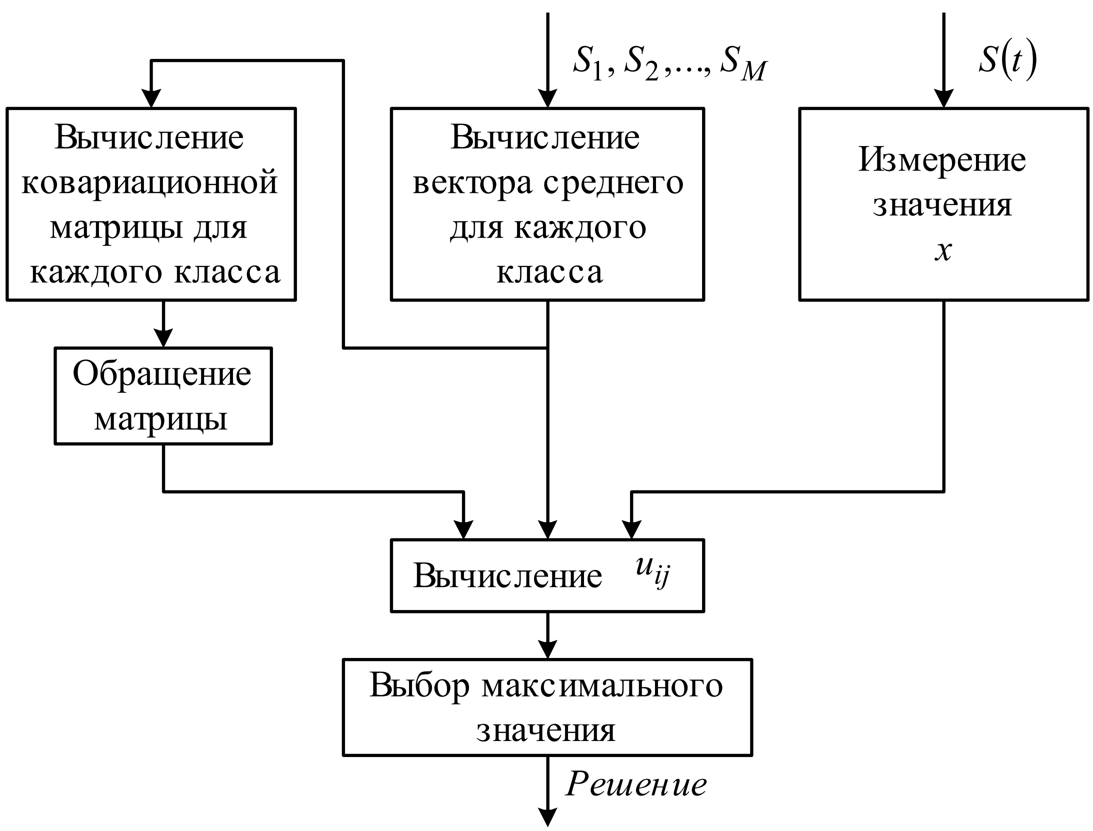
$$u_{ij}(x) = x^T C_i^{-1}(m_i - m_j) - \frac{1}{2}(m_i + m_j)^T C_j^{-1}(m_i - m_j).$$

Для определения оптимальной разделяющей функции требуется вычислить M(M минус 1) значений функции $u_{ij}(x)$ для всех i, j: $i \neq j$ и выбрать наибольшее из полученных значений. Если окажется, что этот максимум равен u_{kj}, то относим x к классу A_k. Схема оптимального распознавания, воспроизводящая описанный метод, представлена на рисунке.

Следующее уравнение описывает гиперплоскость, проведенную в n-мерном гиперпространстве и разделяющую его в случае наличия двух классов на две части:

$$u_{ij}(x) = x^T C_i^{-1}(m_i - m_j) - \frac{1}{2}(m_i + m_j)^T C_j^{-1}(m_i - m_j) = 0.$$

Решающее правило можно представить в общем виде:



$$u_{ij} > 0 \quad \textit{для} \quad X \in A_i,$$
$$u_{ij} < 0 \quad \textit{для} \quad X \in A_j.$$

Вектор средних значений определяют в соответствии со следующим выражением (равенство приближенное, так как значение рассчитывается по экспериментальным данным):

$$m = M[x] \approx \frac{1}{N}\sum_{j=1}^{N} x_j ,$$

где N – объем выборки.

Элементы ковариационной матрицы C задаются следующим образом:

$$c_{lk} = M[(x_1 - m_1)(x_k - m_k)] = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}(x_1 - m_1)(x_k - m_k)\omega(x_1, x_k)dx_1dx_k$$

или в векторной форме

$$C = M[(x-m)(x-m)^T] = M[xx^T - 2xm^T - mm^T] = M[xx^T] - mm^T .$$

Так как логарифм отношения правдоподобия u_{ij} является линейной комбинацией компонентов образа x, подчиняющихся нормальному распределению, то u_{ij} также описывается нормальным распределением. Поэтому математическое ожидание логарифма отношения правдоподобия для класса ω_i в случае равных ковариационных матриц можно представить в виде

$$M[u_{ij}] = m_i^T C^{-1}(m_i - m_j) - \frac{1}{2}(m_i + m_j)^T C^{-1}(m_i - m_j)$$

Обозначим математическое ожидание разделяющей функции через r_{ij}:

$$M[u_{ij}] = \frac{1}{2} r_{ij} .$$

Величину r_{ij} часто называют *расстоянием Махаланобиса* между плотностями распределений $\omega(x/A_i)$ и $\omega(x/A_j)$. Если C – единичная матрица, то расстояние Махаланобиса представляет собой квадрат расстояния между средними значениями величин $\omega(x/A_i)$ и $\omega(x/A_j)$:

$$[u_{ij}] = M[(u_{ij} - \bar{u}_{ij})^2] = r_{ij} .$$

Вероятность ошибки при распознавании зависит от расстояния Махаланобиса между классами, которое выражается следующим образом:

$$r_{ij} = (m_i - m_j)^T C^{-1}(m_i - m_j),$$

где m_i и m_j – соответственно векторы средних для каждого класса;

C^{-1} – матрица, обратная ковариационной.

Зависимость вероятности ошибки от r_{ij} можно записать в виде выражения

$$P_{\text{ош}} = \Phi(-\frac{1}{2}\sqrt{r_{ij}}) + (1 - \Phi(\frac{1}{2}\sqrt{r_{ij}})),$$

где Ф – интеграл вероятности.

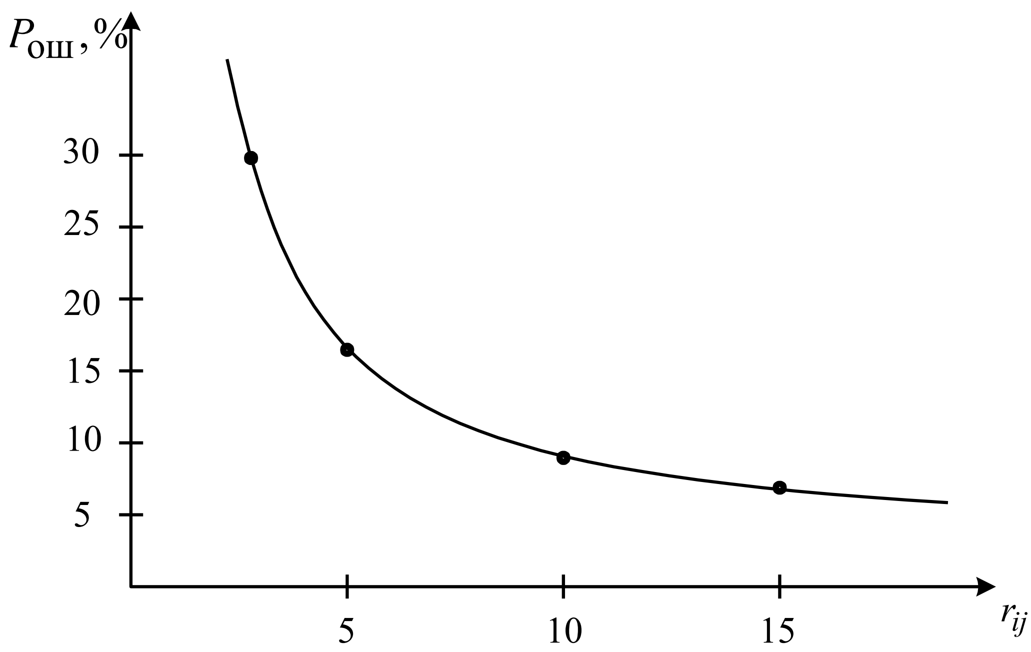
График зависимости вероятности ошибки классификации от величины расстояния Махаланобиса представлен на рисунке.

Выводы:

Огромные объемы обрабатываемой информации, состояние собственных сил и средств делает задачу распознавания одной из самой важной задачей обеспечения информационной безопасности.

Актуальность решения этой задачи определяется тем, что проблемы связанные с распознаванием образов в полном объеме не решены.

Существуют математические методы, реализация которых позволяет подойти к решению поставленной задачи. Оптимальным с точки зрения нормирования потерь является байесовский классификатор.



В случае многомерной случайной величины необходимо определение оптимальной разделяющей функции. Эта процедура трудоемкая, но разработаны оптимальные схемы распознавателей, и при введении некоторых допущений эти схемы технически реализуемы. Оптимальным с точки зрения нормирования потерь является байесовский классификатор.

Вероятность ошибки при распознавании зависит от расстояния Махаланобиса между классами.

Заключительная часть.

Подвожу итоги занятия.

Рекомендованная литература:

1. Хемминг Р.В. Численные методы. – М.: Наука, 1972.

2. Левин Б.Р. Теоретические основы статистической радиотехники. – М.: Сов. радио и связь, 1974.

3. Ту Дж., Гонсалес Р. Принципы распознавания образов. – М.: Мир, 1978.

4. Горелик А.Л., Скрипкин В.А. Методы распознавания. – М.: Высшая школа, 1989.

5. Фомин Я.А., Тарловский Г.Р. Статистическая теория распознавания образов. – М.: Радио и связь, 1986.