Методическая разработка

для проведения лекции

Занятие 9. Критерии принятия решения при обнаружении воздействий

Учебные вопросы занятия:
1. Критерии принятия решения при обнаружении воздействий
2. Последовательные процедуры принятия решения
Заключительная часть

1. Критерии принятия решения при обнаружении воздействий

Любой процесс анализа начинается с обнаружения объектов. Оно состоит в том, что по результатам обработки наблюдаемого процесса, который может быть либо разрешенным воздействием (запросом или передаваемой информацией), либо воздействием нарушителя или злоумышленника, решают, содержится ли вредоносная информация в принятом блоке. Иначе говоря, задача обнаружения сводится к различению двух гипотез:

- разрешенная информация;
- вредоносная информация.

Обнаружение обеспечивает принятие решения о наличии или отсутствии вредоносной информации в данный момент времени на данном устройстве. Поскольку содержание указанной информации носит случайный характер, для построения обнаружителей применяются, как правило, статистические методы. Сущность их сводится к выделению информативных признаков и сравнению их с эталонными значениями.

Под *информативными признаками* подразумеваются общие свойства и характеристики, присущие различным видам воздействий, например, число двоичных символов определенного вида и др. Под *эталонами* понимаются усредненные значения характеристик воздействий, например средние значения характеристик.

В силу стохастичности воздействий информативные признаки, использующиеся для обнаружения, являются случайными процессами или случайными величинами.

Наиболее полное представление о случайной величине дает ее *плотность распределения вероятностей* (для непрерывной случайной величины) или *распределение вероятностей* (для дискретной случайной величины). Поэтому классы, соответствующие гипотезам «разрешенная информация» и «вредоносная информация», обычно представляют в виде набора информативных признаков, описываемых соответствующими плотностями распределения или распределениями вероятностей. Чтобы подчеркнуть зависимость от номера гипотезы, их обычно выражают в виде условных плотностей

$\omega\left(x/A_i\right)$ (рис. 1) или условных вероятностей $P\left(x_j/A_i\right)$ (рис. 2), где x – текущее значение признака, A_i (i = 1,k) – гипотеза с номером i (например i = 1 – для помехи, i = 2 – для смеси "сигнал + помеха"), x_j (j = 1,m) – значение дискретного признака с номером j.

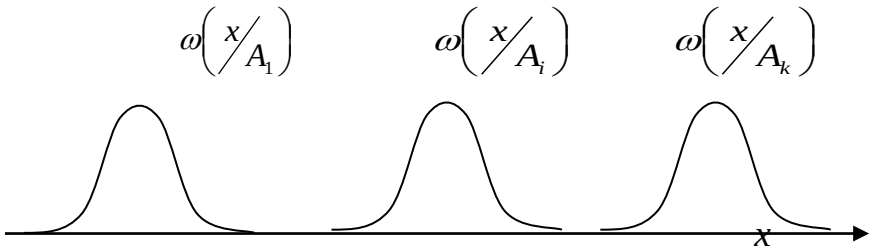


Рис. 1. Плотности распределения вероятностей в случае k гипотез

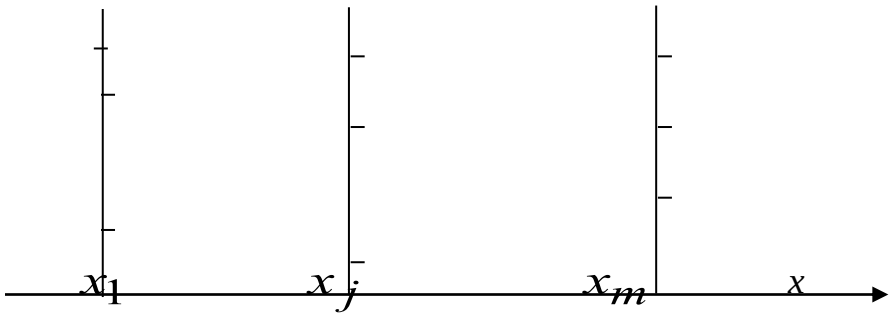


Рис. 2. Распределения условных вероятностей в случае m гипотез

Помимо описания классов в виде плотности распределения вероятностей (распределения вероятностей) на практике каждому из них иногда придают свой вес, показывающий частоту их появления и степень важности.

Частота появления класса выражается его *априорной вероятностью* $P(A_i)$. Значимость класса определяется *потерями* $L(A_i)$. Величина потерь характеризует последствия принятого ошибочного решения в отношении конкретной гипотезы.

Если какие-либо из этих величин неизвестны, то их полагают равными для всех классов. Например, если неизвестны потери при принятии ошибочного решения в пользу одного из классов, то считают

$$L(A_i) = L(A_l) = 1. \qquad (1)$$

Если неизвестны априорные вероятности появления классов, то полагают

$$P(A_i) = P(A_l) = 1/k, \qquad (2)$$

где k – количество классов.

Однако в любом случае при принятии решения должны быть известны плотности распределения вероятностей или распределение вероятностей значений признаков.

Предположим, что на вход обнаружителя поступает реализация излучения в виде разрешенной информации (класс A_1) или вредоносной информации (класс A_2). Дадим описание первого класса в виде выражения

$$L(A_1) \cdot P(A_1) \cdot \omega\left(x/A_1\right) = 1 \cdot \frac{1}{2} \cdot \omega\left(x/A_1\right) = \frac{1}{2}\omega\left(x/A_1\right), \qquad (3)$$

а второго – $\frac{1}{2}\omega\left(x/A_2\right)$.

Предположим, что и последствия неправильных решений и априорные вероятности у различных классов одинаковы:

$$L(A_1) = L(A_2) = 1,$$
$$P(A_1) = P(A_2) = \frac{1}{2}.$$

По измеренному значению признака $\hat{x}$ необходимо принять решение в пользу класса A_1, если на входе обнаружителя имеется разрешенная информация, или в пользу класса A_2, если имеется вредоносная информация. Описание классов представлено на рисунке.

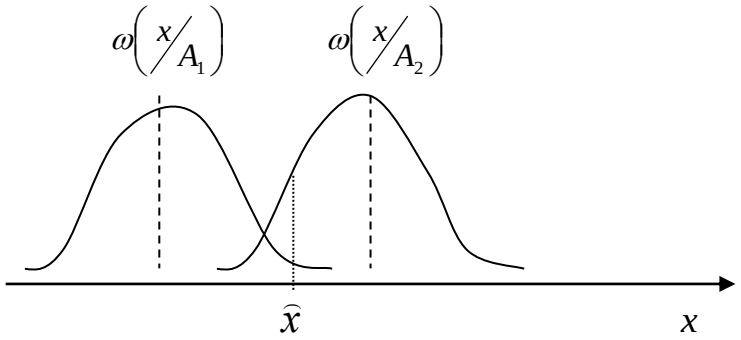


Рис. 3. Пример описания классов

Критерий максимального правдоподобия

Плотность распределения вероятностей признака *x* характеризует частоту появления того или иного его значения. Например, для ситуации на рисунке 3 значение $\hat{x}$ чаще проявляется у второго класса, поэтому решение целесообразно принять в его пользу.

Следует отметить, что решение принимается в пользу класса, плотность распределения вероятностей признака которого больше, что формально можно записать в виде

$$\frac{1}{2}\omega\left(\hat{x}/A_2\right) \geq \frac{1}{2}\omega\left(\hat{x}/A_1\right) \quad \Rightarrow \quad A_2 \tag{4}$$

или

$$\frac{\omega\left(\hat{x}/A_2\right)}{\omega\left(\hat{x}/A_1\right)} = L_{2/1}(\hat{x}) \geq 1 \quad \Rightarrow \quad A_2, \tag{5}$$

где $L_{2/1}(\hat{x})$ – отношение правдоподобия.

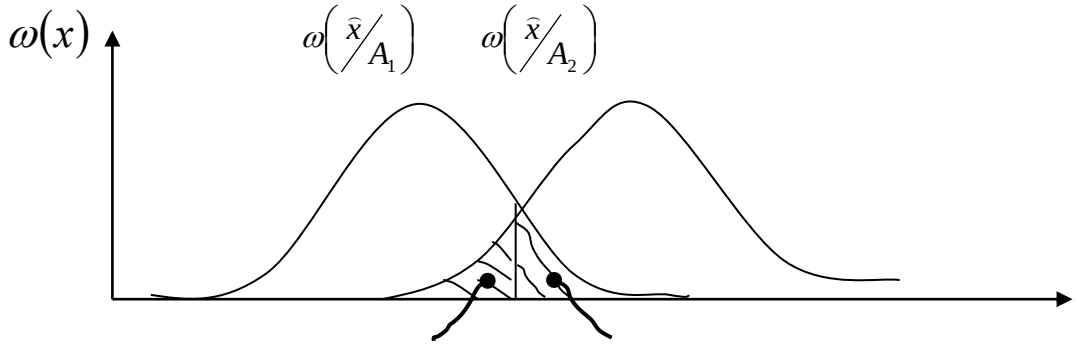
В противном случае решение принимается в пользу класса A_1. Это правило получило название «критерий максимального правдоподобия».

В соответствии с этим правилом вычисляется отношение правдоподобия и сравнивается с пороговой величиной, называемой *порогом отношения правдоподобия*, равной единице. По результатам сравнения принимается решение в пользу того или иного класса.

При принятии решения возможна ошибка, так как в точке $\hat{x}$ функция $\omega\left(\hat{x}/A_1\right)$ отлична от нуля. Следовательно, существует некоторая вероятность принадлежности реализации излучения и к первому классу.

Для оценки вероятности ошибочного решения необходимо упростить процедуру его принятия. Вместо вычисления отношения правдоподобия для каждой реализации признака можно установить *порог принятия решения* x_0. Если значение признака находится правее этого порога или равно ему, то реализация относится ко второму классу, а если левее – к первому.

Таким образом, вместо многократного вычисления отношения правдоподобия для каждой поступающей реализации признака $\hat{x}$ достаточно один раз найти порог принятия решения и сравнивать с ним измеренные значения признака. От порога принятия решения существенно зависит вероятность ошибочных решений. Действительно, площадь под кривой $\omega\left(\hat{x}/A_1\right)$ справа от точки x_0 определяет так называемую вероятность *ошибки первого рода* α (*вероятность ложной тревоги*), которая характеризует долю ошибочных решений в пользу класса A_2, в то время как реализация признака принадлежала классу A_1 (рис. 4).



β x_0 α x

Рис. 4. Вероятности ошибок

Площадь под кривой $\omega\left(\hat{x}/A_2\right)$ слева от точки x_0 соответствует так называемой вероятности *ошибки второго рода* β (*вероятность пропуска цели*), определяющей долю ошибочных решений в пользу класса A_1, хотя реализация признака принадлежала классу A_2. Общая величина вероятности ошибочных решений составляет

$$P_{\text{ош}} = \frac{1}{2}(\alpha + \beta), \tag{6}$$

где

$$\alpha = \int_{x_0}^{\infty} \omega\left(x/A_1\right)dx; \tag{7}$$

$$\beta = \int_{-\infty}^{x_0} \omega\left(x/A_2\right)dx. \tag{8}$$

Минимум ошибочных решений достигается в том случае, когда величина порога принятия решения соответствует точке пересечения графиков функций $\omega\left(\hat{x}/A_1\right)$ и $\omega\left(\hat{x}/A_2\right)$, найти которую можно в ходе решения уравнения относительно x_0:

$$\omega\left(x_0/A_1\right) = \omega\left(x_0/A_2\right). \tag{9}$$

Если величина порога принятия решения вычисляется из уравнения (9), то критерий максимального правдоподобия обеспечивает минимум вероятности ошибочных решений.

Критерий максимума апостериорной вероятности

Если для принятия решения привлечь дополнительную информацию в виде априорных вероятностей появления классов, то отношение правдоподобия можно записать в следующем виде:

$$\frac{\omega\left(\hat{x}/A_2\right)}{\omega\left(\hat{x}/A_1\right)} = L_{2/1}(\hat{x}) \geq \frac{P(A_1)}{P(A_2)} \quad \Rightarrow \quad A_2. \tag{10}$$

Это правило получило название «*критерий максимума апостериорной вероятности»* и позволяет минимизировать априорную вероятность ошибок:

$$P_{\text{ош}} = P(A_1)\alpha + P(A_2)\beta. \tag{11}$$

Как и для правила принятия решения по критерию максимального правдоподобия, можно упростить процедуру принятия решения, заменив вы-

численение отношения правдоподобия порогом принятия решения, величина которого определяется исходя из уравнения относительно x_0:

$$P(A_1)\cdot\omega\left(x_0/A_1\right)=P(A_2)\cdot\omega\left(x_0/A_2\right). \qquad (12)$$

Критерий Байеса

Если в качестве дополнительной информации использовать потери, определяющие последствия неправильно принятого решения, то по аналогии с вышеприведенными критериями можно записать

$$\frac{\omega\left(\hat{x}/A_2\right)}{\omega\left(\hat{x}/A_1\right)}=L_{2/1}(\hat{x})\geq\frac{P(A_1)\cdot L(A_1)}{P(A_2)\cdot L(A_2)}\quad\Rightarrow\quad A_2. \qquad (13)$$

Это правило получило название «*критерий Байеса»* или критерий минимума среднего риска. В нем отношение правдоподобия сравнивается с порогом принятия решения, представляющего собой отношение произведения потерь за неправильно принятые решения и априорных вероятностей появления классов.

Как и в предыдущих случаях, можно найти величину порога принятия решения из уравнения

$$P(A_1)\cdot L(A_1)\cdot\omega\left(x_0/A_1\right)=P(A_2)\cdot L(A_2)\cdot\omega\left(x_0/A_2\right). \qquad (14)$$

Критерий Неймана – Пирсона

При уменьшении объема априорной информации в процессе принятия решения может быть использован *критерий Неймана – Пирсона*.

В соответствии с этим критерием выбирается правило, обеспечивающее минимально возможную величину вероятности ошибки второго рода β при условии, что вероятность ошибки первого рода не больше $\alpha_з$.

Обычно из составляющих вероятности ошибки наибольшее значение имеет ложная тревога, так как она приводит к дополнительной загрузке системы обнаружения и предупреждения компьютерных атак, что снижает пропускную способность системы. В связи с этим допустимой вероятности ложной тревоги обычно присваивают значение, определяемое с учетом требуемой пропускной способности системы обработки.

Значению $\alpha_з$ соответствует порог принятия решения, определяемый из уравнения

$$\alpha_3=\int_{x_0}^{\infty}\omega\left(x/A_1\right)dx. \qquad (15)$$

Для принятия решения с использованием рассматриваемого критерия достаточно знать только плотность $\omega\left(x/A_1\right)$, соответствующую классу «полезная информация», и величину $\omega_з$. Таким образом, объем априорной информации оказывается гораздо меньшим, чем для приведенных ранее правил принятия решения.

Величина порога принятия решения может быть получена на основе следующих выражений:

– для нормального закона распределения шума

$$x_0 = \sigma_1 \cdot \Phi^{-1}(1-\alpha_з); \tag{16}$$

– для рэлеевского закона распределения шума

$$x_0 = \sqrt{2 \cdot \sigma_1 \cdot (-\ln \alpha_з)}, \tag{17}$$

где σ_1 – дисперсия;

Φ^{-1} – функция, обратная интегралу вероятности $\Phi(x)$:

$$\Phi(x) = \frac{1}{\sqrt{2 \cdot \pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt . \tag{18}$$

Критерий К из N

Уменьшение вероятности ложных тревог неизбежно приводит к снижению вероятности обнаружения $P_{обн}$. Устранить это противоречие можно неоднократным повторением процесса обнаружения одного и того же воздействия по нескольким его реализациям.

Естественным требованием к таким актам обнаружения является их статистическая независимость. Как известно, неоднократное повторение опыта позволяет существенно уменьшить случайность его исхода. На этом принципе основано снижение вероятности ложных тревог.

Если известна или задана вероятность ложных тревог для одной реализации признака $\alpha_з$, а решение о наличии сигнала на выходе обнаружителя принимается по *k* положительным исходам из *N* реализаций излучения, то итоговая вероятность ложной тревоги может быть представлена следующим выражением:

$$\alpha_\Sigma = \sum_{i=k}^{N} C_N^i \cdot \alpha_1^i \cdot (1-\alpha_i)^{N-i}, \tag{19}$$

где C_N^k – число сочетаний из *N* по *k*.

Такое правило принятия решения называется *критерием k из N* («по большинству голосов», «мажоритарный прием»). Принятие решения в этом случае сводится к «голосованию» за наличие или отсутствие вредоносной информации на входе обнаружителя. Большинство голосов должно удовлетворять следующему условию:

$$N \geq k \geq \frac{N}{2} + 1. \qquad (20)$$

Аналогично вероятности ложных тревог определяется и вероятность обнаружения:

$$P_{\text{обн}\Sigma} = \sum_{i=k}^{N} C_N^i \cdot P_{\text{обн1}}^i \cdot \left(1 - P_{\text{обн1}}\right)^{N-i}, \qquad (21)$$

где $P_{\text{обн1}}$ – вероятность обнаружения вредоносной информации по одной реализации признака.

Вывод.

Анализ рассмотренных процедур выявляет два присущих им принципиальных недостатка:

– значительный объем априорной информации по каждому распознаваемому классу;

– большие объемы выборок признаков для формирования условных плотностей распределения их вероятностей.

2. Последовательные процедуры принятия решения

Для устранения второго недостатка, присущего правилам принятия решения на основе критерия Байеса и его разновидностей, используют так называемые *последовательные процедуры принятия решения* (*критерий Вальда*), обеспечивающие минимум среднего размера выборки при формировании описаний классов. При этом вероятность ложных тревог составляет величину не более чем $\alpha_з$, а вероятность пропуска сигнала не превышает $\alpha_З$.

Сущность методов сводится к тому, что вся область определения признака, в которой принимается решение, разбивается не на две, а на три части для обеспечения заданных вероятностей $\alpha_з$ и $\alpha_З$, в соответствии с которыми вычисляются пороги принятия решения x_{01} и x_{02} (рис. 5).

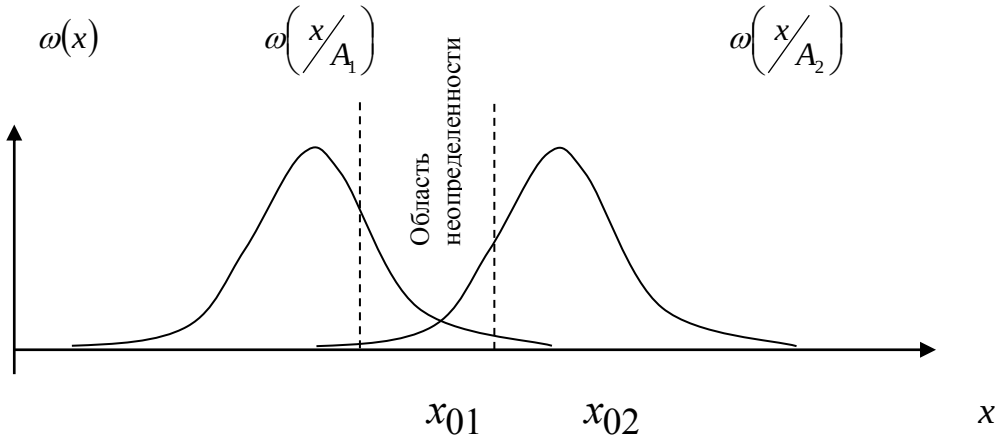


Рис. 5. Критерий Вальда

На основе выборки ограниченного объема строят ориентировочные описания классов.

Если реализация признака попадает в область левее порога принятия решения (ППР) x_{01}, принимается решение в пользу класса A_1, если правее ППР x_{02} – в пользу класса A_2, а если между ними (область неопределенности) – делается вывод о необходимости увеличения выборки. Накопление выборки продолжается до тех пор, пока не будет принято решение в пользу класса A_1 или A_2.

Правило принятия решения выглядит следующим образом:

$$\frac{\omega\left(\hat{x}/A_2\right)}{\omega\left(\hat{x}/A_1\right)} \le C_0 \quad \Rightarrow \quad A_1, \qquad \frac{\omega\left(\hat{x}/A_2\right)}{\omega\left(\hat{x}/A_1\right)} \ge C_1 \quad \Rightarrow \quad A_2, \tag{22}$$

$$C_0 < \frac{\omega\left(\hat{x}/A_2\right)}{\omega\left(\hat{x}/A_1\right)} < C_1 \quad \Rightarrow \quad \begin{matrix}\text{Продолжение}\\ \text{накопления}\\ \text{выборки}\end{matrix}$$

Пороги отношения правдоподобия C_0 и C_1 определяются из соотношений:

$$C_0 \ge \min\left(\frac{\beta_3}{1-\alpha_3}, \frac{1-\beta_3}{\alpha_3}\right),$$
$$C_1 \le \max\left(\frac{\beta_3}{1-\alpha_3}, \frac{1-\beta_3}{\alpha_3}\right). \tag{23}$$

Пороги принятия решения можно определить на основе решения уравнений:

$$\omega\left(x_{01}/A_2\right) = C_0 \cdot \omega\left(x_{01}/A_1\right),$$
$$\omega\left(x_{02}/A_2\right) = C_1 \cdot \omega\left(x_{02}/A_1\right). \tag{24}$$

Следует отметить, что в этом случае неизменным остается только вид законов распределения (плотностей распределения вероятностей), а параметры законов меняются по мере накопления объема выборки. При этом меняются и значения порогов принятия решения x_{01} и x_{02} при неизменных порогах C_0 и C_1.

Заключительная часть.

Существует ряд правил принятия решения. Эти правила носят название критерии. Сущность их заключается в вычислении отношения правдопо-

добия и сравнении его с некоторой пороговой величиной, называемой порогом отношения правдоподобия.

Вместо многократного вычисления отношения правдоподобия для каждой поступающей реализации признака $\hat{x}$ достаточно один раз найти порог принятия решения и сравнивать с ним измеренные значения признака.

Рекомендованная литература:

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

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

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