УДК 519.248

А. А. Евдокимов,
Институт радиоэлектроники и информационных технологий,
Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, Екатеринбург
Научный руководитель: ст. преподаватель А. А. Кныш

Анализ ошибок обнаружения аномалий методами статистического анализа

Аннотация. В данной статье проведен анализ способов минимизации количества ошибок 1-го и 2-го рода с использованием статистических методов, а именно Байесовского критерия.

Ключевые слова: обнаружение аномалий, статистический анализ, Байесовский критерий.

В современном мире очень важно точно определять аномалии (угрозы) в системе, ведь любая незамеченная аномалия может привести к утечке данных, неработоспособности системы или даже эксплуатации системы третьими лицами.

В процессе поиска таких аномалий неизбежны два типа ошибок:

– ошибка первого рода (ложноположительная) — система ошибочно определяет нормальное, легитимное событие как аномалию;

– ошибка второго рода (ложноотрицательная) — система ошибочно определяет аномалию как абсолютно нормальное событие.

Рассмотрим способы минимизации количества ошибок 1-го и 2-го рода с помощью статистического метода, а именно с помощью Байесовского коэффициента.

Сформулируем задачу.

Задача обнаружения аномалий формализуется как проверка гипотез. Система принимает одно из двух решений на основе данных наблюдения. Рассмотрим гипотезы:

H_0 — событие соответствует нормальному поведению;

H_1 — событие является аномалией.

Каждая гипотеза имеет риск ошибки. Главная цель — найти правило принятия финального решения, минимизирующего ущерб от обоих типов ошибок.

Переформулируем типы ошибок на языке гипотез:

Ошибка первого рода (α) — отклонение H_0, когда оно истинно. Это «ложная тревога».

Ложноотрицательная ошибка (β) — реакция как на H_0, когда истинно H_1. Это «пропуск угрозы».

Важный момент: ошибки 1-го и 2-го рода имеют разный вес. Ложноотрицательная ошибка способна нанести гораздо больший вред системе, поэтому при расчете важно учитывать не только вероятность, но и последствия ошибок нашей модели.

В основе нашей модели будет лежать Байесовский критерий.

Распишем формулу Байеса:

$$P\left(H_i|x\right)=\frac{f\left(x|H_i\right)\cdot P\left(H_i\right)}{\sum f\left(x|H_j\right)\cdot P\left(H_j\right)},\ j\in\{0,1\},$$

где $P(H_i)$ — *априо*рные вероятности (до определения x),

$f(x|H_i)$ — условная плотность вероятности (насколько возможно получить x при гипотезе H_i),

$P(H_i|x)$ — апостериорные вероятности (после определения x).

Итоговое решение принимается по следующему правилу:

Если $P(H_i|x)>P(H_j|x)$, то выбирается H_i.

Учтем теперь стоимости ошибок, так как в реальном алгоритме нам необходимо делать поправку на вес или стоимость ошибок 1-го и 2-го рода. Для этого введем матрицу потерь L:

L_{01} — стоимость при ошибке 1-го рода;

L_{10} — стоимость при ошибке 2-го рода.

С учетом этого проверка меняется на:

$$P\left(H_1|x\right)>\frac{L_{01}}{L_{01}+L_{10}}.$$

Это задает порог принятия решения в зависимости от стоимости ошибки.

Приведем пример:

Если пропуск атаки в 100 раз дороже ложного срабатывания системы безопасности, то достаточно всего $\frac{1}{1+100}\approx 0,0099\ \%$ для того, чтобы бить тревогу.

Порог принятия решения зависит от конкретных параметров нашей системы. За счет него наш алгоритм превращается из детектора отклонений в интеллектуальную программу, способную очень грамотно управлять рисками в системе.

В курсе «Математики» можно использовать задачи, аналогичные данной, для студентов, обучающихся на направлении «Информационная безопасность». Для составления аналогичных задач рекомендуется литература [1; 2].

1. *Васильев А. А.* Теория вероятностей и математическая статистика : учеб. и практикум для вузов. — М. : Юрайт, 2025. — 224 с.

2. Теория вероятностей и математическая статистика. Математические модели : учеб. для вузов / В. Д. Мятлев, Л. А. Панченко, Г. Ю. Ризниченко, А. Т. Терехин. — М. : Юрайт, 2025. — 321 с.