УДК 004.056: 519.81

М.А. Басараб, Н.В. Медведев,
И.И. Троицкий

К ВОПРОСУ ОБ ОЦЕНКЕ ВЕРОЯТНОСТИ ОШИБКИ ТЕСТИРОВАНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрена задача определения оценки вероятности ошибки тестирования систем информационной безопасности. Получены формулы для математического ожидания и дисперсии оценки вероятности ошибки, а также построен доверительный интервал для вероятности ошибки.

E-mail: basarab@mail.ru

Ключевые слова: *оценка ошибки, информационная безопасность.*

При тестировании системы информационной безопасности (СИБ) необходимо определить, в каком состоянии она находится: работоспособном или неработоспособном. Один из основных показателей тестирования — вероятность ошибки. При каждом тестировании выпадает пара i, j где i — реальное состояние СИБ; j — результаты тестирования*.

Обозначим работоспособное состояние через 0, неработоспособное — 1. Тогда i и j принимают значения 0 или 1. Пусть N — число тестирований, $N_{i,j}$ — число выпадений пары (i, j). Вероятность наступления события (i, j) обозначим через $P(i, j)$, а оценку этой вероятности определим как $P^*(i, j) = N_{i,j}/N$, где $i, j = 0,1$. Тогда вероятность ошибки $P_{\text{ош}} = P(0,1) + P(1,0)$. В качестве оценки вероятности ошибки целесообразно взять оценку $P^*_{\text{ош}} = P^*(0,1) + P^*(1,0)$.

Найдем математическое ожидание и дисперсию оценки $P^*_{\text{ош}}$, для чего используем полиноминальное распределение оценок вероятности $P^*(0,1)$ и $P^*(1,0)$:

$$M\left[P^*_{\text{ош}}\right] = M\left[P^*(0,1)\right] + M\left[P^*(1,0)\right] = P(0,1) + P(1,0) = P_{\text{ош}}.$$

Таким образом, оценка вероятности ошибки $P^*_{\text{ош}}$ является несмещенной оценкой.

При вычислении дисперсии оценки $P^*_{\text{ош}}$ воспользуемся уравнением связи дисперсии случайной величины со вторым моментом: $d = \alpha_2 - m^2$, где d — дисперсия; α_2 — второй момент; m — математическое ожидание. Откуда

* Крамер Г. Математические методы статистики. — М.: Наука, 1975. — 648 с.

$$D\left[P^*_{\text{ош}}\right] = D\left[P^*(0,1) + P^*(1,0)\right] =$$

$$= D\left[P^*(0,1)\right] + D\left[P^*(1,0)\right] + 2\operatorname{cov}\left(P^*(0,1), P^*(1,0)\right) =$$

$$= \frac{P(0,1)\left(1 - P(0,1)\right)}{N} + \frac{P(1,0)\left(1 - P(1,0)\right)}{N} +$$

$$+2M\left[\left(P^*(0,1) - P(0,1)\right)\left(P^*(1,0) - P(1,0)\right)\right]. \qquad (1)$$

Определим последнее слагаемое в (1):

$$2M\left[\left(P^*(0,1) - P(0,1)\right)\left(P^*(1,0) - P(1,0)\right)\right] =$$

$$= 2\left\{M\left[(P^*(0,1), P^*(1,0)\right] - P(0,1)P(1,0)\right\} =$$

$$= 2\left\{P(0,1)P(1,0) - \frac{P(0,1)P(1,0)}{N} - P(0,1)P(1,0)\right\} =$$

$$= -2\frac{P(0,1)P(1,0)}{N}. \qquad (2)$$

Подставим (2) в (1) и получим

$$D\left[P^*_{\text{ош}}\right] = \frac{P(0,1)\left(1 - P(0,1)\right)}{N} + \frac{P(1,0)\left(1 - P(1,0)\right)}{N} - 2\frac{P(0,1)P(1,0)}{N} =$$

$$= \frac{1}{N}\left[\left(P(0,1) + P(1,0)\right)\left(1 - \left(P(0,1) + P(1,0)\right)\right)\right]. \qquad (3)$$

С учетом весов вероятностей $P(0,1)$ и $P(1,0)$ вероятность ошибки $P_{\text{ош}}$ определяется по формуле

$$\widehat{P_{\text{ош}}} = \alpha_1 P(0,1) + \alpha_2 P(1,0),$$

где α_i — веса вероятностей, $i = 1, 2$.

В этом случае в качестве оценки вероятности ошибки $\widehat{P_{\text{ош}}}$ целесообразно взять

$$\widehat{P^*_{\text{ош}}} = \alpha_1 P^*(0,1) + \alpha_2 P^*(1,0).$$

Вычислим математическое ожидание и дисперсию оценки $\widehat{P^*_{\text{ош}}}$:

$$M\left[\widehat{P^*_{\text{ош}}}\right] = M\left[\alpha_1 P^*(0,1) + \alpha_2 P^*(1,0)\right] =$$

$$= \alpha_1 P(0,1) + \alpha_2 P(1,0) = \widehat{P_{\text{ош}}}; \qquad (4)$$

$$D\left[\widehat{P^*_{\text{ош}}}\right]=D\left[\alpha_1P^*\left(0,1\right)\right]+D[\alpha_2P^*\left(1,0\right)\Big]+2\operatorname{cov}\left(\alpha_1P^*\left(0,1\right),\alpha_2P^*\left(1,0\right)\right)=$$

$$=\frac{\alpha_1{}^2P\left(0,1\right)\left(1-P\left(0,1\right)\right)}{N}+\frac{\alpha_2{}^2P\left(1,0\right)\left(1-P\left(1,0\right)\right)}{N}+$$

$$+2M\left[\left(\alpha_1P^*\left(0,1\right)-\alpha_1P\left(0,1\right)\right)\left(\alpha_2P^*\left(1,0\right)-\alpha_2P\left(1,0\right)\right)\right]=$$

$$=\frac{\alpha_1{}^2P\left(0,1\right)\left(1-P\left(0,1\right)\right)}{N}+\frac{\alpha_2{}^2P\left(1,0\right)\left(1-P\left(1,0\right)\right)}{N}-2\frac{\alpha_1\alpha_2P\left(0,1\right)P\left(1,0\right)}{N}=$$

$$=\frac{\alpha_1{}^2P\left(0,1\right)+\alpha_2{}^2P\left(0,1\right)-(\alpha_1P\left(0,1\right)+\alpha_2P\left(1,0\right))^2}{N}. \qquad (5)$$

Если в (5) подставить $\alpha_1=\alpha_2=1$, то получим формулу (3).

Особый практический интерес вызывает случай, если $\alpha_1=1$ и $\alpha_2>1$. Это соответствует увеличению веса условной вероятности ошибки — «пропуск цели», которая всегда очень критична для СИБ. Тогда

$$\widehat{P^*_{\text{ош}}}=P^*\left(0,1\right)+\alpha_2P^*\left(1,0\right);$$

$$M\left[\widehat{P^*_{\text{ош}}}\right]=P\left(0,1\right)+\alpha_2P\left(1,0\right)=\widehat{P_{\text{ош}}};$$

$$M\left[\widehat{P^*_{\text{ош}}}\right]=\frac{P\left(0,1\right)+\alpha_2{}^2P\left(1,0\right)-(P\left(0,1\right)+\alpha_2P\left(1,0\right))^2}{N}.$$

В работе [1] доказано, что случайная величина $\widehat{P^*_{\text{ош}}}$ имеет асимптотически нормальное распределение с параметрами, определяемыми по (4) и (5). В результате нетрудно построить доверительный интервал для искомой вероятности ошибки $\widehat{P_{\text{ош}}}$.

Проиллюстрируем полученные результаты на примере. Пусть $N=1\,000$, $\alpha_1=\alpha_2=1$, $N_{00}=400$, $N_{11}=500$, $N_{01}=40$, $N_{10}=60$, отсюда $P^*\left(0,0\right)=0{,}4$, $P^*\left(1,1\right)=0{,}5$, $P^*\left(0,1\right)=0{,}04$, $P^*\left(1,0\right)=0{,}06$. Следовательно,

$$P^*_{\text{ош}}=P^*\left(0,1\right)+P^*\left(1,0\right)=0{,}1.$$

Дисперсия оценки $D\left[P^*_{\text{ош}}\right]=9\cdot10^{-5}$, среднее квадратическое отклонение $\Omega=\sqrt{D\left[P^*_{\text{ош}}\right]}=9{,}48\cdot10^{-3}$.

С учетом правила «трех сигм»

$$P(|\ |)\ P\left(\left|P_{\text{ош}}^{*} - |\ P_{\text{ош}}\right| < 2\Omega\right) = 0,997,$$

доверительный интервал для искомой вероятности ошибки $P_{\text{ош}}$ с уровнем доверия $\alpha = 0,997$ будет равен

$$P_{\text{ош}}^{*} - 3\Omega < P_{\text{ош}} < P_{\text{ош}}^{*} + 3\Omega.$$

Для рассматриваемого примера

$$0,072 < P_{\text{ош}} < 0,128.$$

Статья поступила в редакцию 4.07.2012