УДК 004.056:519.81

Асимптотические свойства оценки вероятности ошибки тестирования систем информационной безопасности

© В.А. Матвеев, М.А. Басараб, И.И. Троицкий

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Исследуются асимптотические свойства оценки вероятности ошибок тестирования систем информационной безопасности при условии независимости тестов. Состояние системы информационной безопасности описывается тремя параметрами. Первый параметр – состояние средства информационной безопасности (работоспособное или неработоспособное), второй параметр – результат тестирования (средство признано работоспособным или неработоспособным) и третий параметр – номер средства информационной безопасности. Определены математическое ожидание и дисперсия оценки вероятности ошибки на основе полиномиального распределения оценок ошибок для каждого теста. Доказано асимптотически нормальное распределение оценки вероятности ошибки тестирования с определенными параметрами (математическое ожидание и дисперсия). Знание закона распределения оценки вероятности тестирования и его параметров позволяет построить доверительный интервал для искомой вероятности ошибки тестирования систем информационной безопасности.

Ключевые слова: *ошибка тестирования, оценка, вероятность, средство информационной вероятности.*

Данная статья является логическим продолжением статьи [1], в которой рассматривалось тестирование одного средства системы информационной безопасности (СИБ).

Пусть СИБ состоит из n средств информационной безопасности (ИБ). Контроль функционирования l-го средства ИБ осуществляется с помощью l-го теста, где $l = \overline{1,n}$.

Будем предполагать, что тесты независимы, тогда вероятность правильного тестирования $P_{\text{пр}}$ СИБ определяется следующим образом:

$$P_{\text{пр}} = \prod_{l=1}^{n} P_{\text{пр}}^{l},$$

где $P_{\text{пр}}^{l}$ — вероятность правильного тестирования l-го средства ИБ, $l = \overline{1,n}$.

Следовательно, вероятность ошибки тестирования систем ИБ

$$P_{\text{ош}} = 1 - P_{\text{пр}} = 1 - \prod_{l=1}^{n} \left(1 - P_{\text{ош}}^{l}\right),$$

где $P_{\text{ош}}^{l}$ — вероятность ошибки тестирования l-го средства ИБ, $l=\overline{1,n}$.

Состояние СИБ будем описывать тройкой (i, j, l), где i — состояние средства ИБ ($i=0$ — работоспособное, $i=1$ — неработоспособное); j — результаты тестирования ($j=0$ — средство признано работоспособным, $j=1$ — средство признано неработоспособным); l — номер теста (или номер средства ИБ), $l=\overline{1,n}$.

Пусть проводится N испытаний и число выпадений тройки (i, j, l) равно N_{ijl}, тогда

$$N=\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{l=1}^{n}N_{ijl}.$$

Обозначим через $P(i,j,l)$ вероятность появления события (i, j, l). Тогда

$$P_{\text{ош}}^{l}=P(0,1,l)+P(1,0,l),$$

где $l=\overline{1,n}$.

Следовательно,

$$P_{\text{ош}}=1-\prod_{l=1}^{n}\left[1-\left(P(0,1,l)+P(1,0,l)\right)\right]=\sum_{k=1}^{n}P_{\text{ош}}^{k}-\sum_{k,m}P_{\text{ош}}^{k}P_{\text{ош}}^{m}+$$
$$+\sum_{k,m,l}P_{\text{ош}}^{k}P_{\text{ош}}^{m}P_{\text{ош}}^{l}+\ldots+(-1)^{n-1}P_{\text{ош}}^{1}\cdots P_{\text{ош}}^{n}.$$

В качестве оценки $P_{\text{ош}}$ по результатам тестирования целесообразно взять

$$\hat{P}_{\text{ош}}=\sum_{k=1}^{n}\hat{P}_{\text{ош}}^{k}-\sum_{k,m}\hat{P}_{\text{ош}}^{k}\hat{P}_{\text{ош}}^{m}+\sum_{k,m,l}\hat{P}_{\text{ош}}^{k}\hat{P}_{\text{ош}}^{m}\hat{P}_{\text{ош}}^{l}+\ldots+(-1)^{n-1}\hat{P}_{\text{ош}}^{1}\cdots\hat{P}_{\text{ош}}^{n},$$

где $\hat{P}_{\text{ош}}^{l}=\hat{P}(0,1,l)+\hat{P}(1,0,l)$, $\hat{P}(0,1,l)=N_{01l}/N$, $\hat{P}(1,0,l)=N_{10l}/N$, $l=\overline{1,n}$.

Определим математическое ожидание оценки $\hat{P}_{\text{ош}}$, используя полиномиальное распределение оценок $\hat{P}(0,1,l)$, $\hat{P}(1,0,l)$, $l=\overline{1,n}$ и результаты теоремы [2, с. 388]:

$$M\left[\hat{P}_{\text{ош}}\right]=P_{\text{ош}}+M\left[\hat{R}_{2}\right]+O\left(\frac{1}{N^{3/2}}\right),$$

где $\hat{R}_2$ — второй член разложения функции $\hat{P}_{\text{ош}}$ в ряд Тейлора в окрестности точки $P_{\text{ош}}$.

Следовательно,

$$\hat{R}_2 = \sum_{k_1=1}^{l} \sum_{k_2=k_1+1}^{l} \sum_{\substack{\text{по наборам} \\ (k_3, k_4, \ldots, k_{l-2})}} \left(\hat{P}_{\text{ош}}^{k_1} - P_{\text{ош}}^{k_1}\right)\left(\hat{P}_{\text{ош}}^{k_2} - P_{\text{ош}}^{k_2}\right)\left(P_{\text{ош}}^{k_3, \ldots, k_{l-2}} - 1\right),$$

где $P_{\text{ош}}^{k_3, \ldots, k_{l-2}} = \sum_{k=k_3}^{l-2} P_{\text{ош}}^{k} - \sum_{k,m} P_{\text{ош}}^{k} P_{\text{ош}}^{m} + \ldots + (-1)^{l-3} P_{\text{ош}}^{k_3} \cdots P_{\text{ош}}^{k_{l-2}}$.

В наборах $(k_3, k_4, \ldots, k_{l-2})$ значения k_i встречаются ровно один раз и $k_i \neq k_1, k_i \neq k_2, i = \overline{3, l-2}$. Тогда по свойству полиномиального распределения вероятностей

$$M\left[\hat{R}_2\right] = \sum_{k_1=1}^{l} \sum_{k_2=k_1+1}^{l} \sum_{\substack{\text{по наборам} \\ (k_3, k_4, \ldots, k_{l-2})}} \frac{P_{\text{ош}}^{k_1} P_{\text{ош}}^{k_2}}{N}\left(1 - P_{\text{ош}}^{k_3, \ldots, k_{l-2}}\right) =$$

$$= \frac{1}{N} \sum_{k_1=1}^{l} \sum_{k_2=k_1+1}^{l} P_{\text{ош}}^{k_1} P_{\text{ош}}^{k_2} \sum_{\substack{\text{по наборам} \\ (k_3, k_4, \ldots, k_{l-2})}} \left(1 - P_{\text{ош}}^{k_3, \ldots, k_{l-2}}\right).$$

Следовательно,

$$M\left[\hat{P}_{\text{ош}}\right] = P_{\text{ош}} + \frac{1}{N} \sum_{k_1=1}^{l} \sum_{k_2=k_1+1}^{l} P_{\text{ош}}^{k_1} P_{\text{ош}}^{k_2} \sum_{\substack{\text{по наборам} \\ (k_3, k_4, \ldots, k_{l-2})}} \left(1 - P_{\text{ош}}^{k_3, \ldots, k_{l-2}}\right) + \quad (1)$$

$$+ O\left(\frac{1}{N^{3/2}}\right).$$

Таким образом, оценка вероятности ошибки $\hat{P}_{\text{ош}}$ является смещенной.

Для вычисления дисперсии оценок $\hat{P}_{\text{ош}}$ также воспользуемся теоремой [2, с. 388] и свойствами полиномиального распределения оценок $\hat{P}(0,1,l), \hat{P}(1,0,l)$, где $l = \overline{1,n}$:

$$D\left[\hat{P}_{\text{ош}}\right] = \sum_{i=0}^{1} \sum_{j=0}^{1} \sum_{k=1}^{l} H^2(i,j,k)\,\delta(i,j)\,D\left[\hat{P}(i,j,k)\right] +$$

$$+ 2 \sum_{i=0}^{1} \sum_{j=0}^{1} \sum_{l=1}^{n} \sum_{k=1}^{n} H(i,j,k) H(i,j,l)\,\delta(i,j)\,\hat{\delta}(l,k)\,\operatorname{cov}\left(\hat{P}(i,j,l)\,\hat{P}(i,j,k)\right) +$$

$$+ O\left(\frac{1}{N^{3/2}}\right),$$

где $H(i,j,k)$ — частная производная функции $\hat{P}_{\text{ош}}$ в точке $P_{\text{ош}}$ по переменной $\hat{P}(i,j,k)$; $\delta(i,j) = \begin{cases} 1, \text{ если } i \neq j, \\ 0 \text{ в противном случае;} \end{cases}$

$$\hat{\delta}(l,k) = \begin{cases} 1, \text{ если } l \neq k, \\ 1, \text{ если } l = k \text{ на наборах } (0,1,l) \text{ и } (1,0,l), \\ 0 \text{ в противном случае.} \end{cases}$$

Тогда

$$H(i,j,k) = \frac{\partial \hat{P}_{\text{ош}}(P_{\text{ош}})}{\partial \hat{P}(i,j,k)} = 1 - P_{\text{ош}\backslash k},$$

где $P_{\text{ош}\backslash k} = \sum\limits_{\substack{l=1 \\ l \neq k}}^{n} P_{\text{ош}}^{l} - \sum\limits_{\substack{l,m \\ l \neq m, \\ m \neq k}} P_{\text{ош}}^{l} P_{\text{ош}}^{m} + \ldots + (-1)^{n-1} P_{\text{ош}}^{1} \cdots P_{\text{ош}}^{k-1} P_{\text{ош}}^{k+1} \cdots P_{\text{ош}}^{n}.$

По свойствам полиномиального распределения вероятностей имеем:

$$D\left[\hat{P}(i,j,k)\right] = \frac{P(i,j,k)\left[1 - P(i,j,k)\right]}{N},$$

$$\operatorname{cov}\left(\hat{P}(i,j,l), \hat{P}(i,j,k)\right) = -\frac{P(i,j,l)P(i,j,k)}{N}.$$

Следовательно,

$$D\left[\hat{P}_{\text{ош}}\right] = \sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=1}^{n}\left(1 - P_{\text{ош}\backslash k}\right)^2 \delta(i,j) \frac{P(i,j,k)\left[1 - P(i,j,k)\right]}{N} -$$

$$-2\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{l=1}^{n}\sum_{k=1}^{n}\left(1 - P_{\text{ош}\backslash k}\right)\left(1 - P_{\text{ош}\backslash l}\right)\delta(i,j)\hat{\delta}(l,k)\frac{P(i,j,l)P(i,j,k)}{N} +$$

$$+O\left(\frac{1}{N^{3/2}}\right). \qquad (2)$$

В [2] доказано, что случайная величина $\hat{P}_{\text{ош}}$ имеет асимптотическое нормальное распределение с параметрами (1) и (2). Тогда нетрудно построить доверительный интервал для искомой величины — вероятности ошибки $P_{\text{ош}}$.

ЛИТЕРАТУРА

[1] Басараб М.А., Медведев Н.В., Троицкий И.И. К вопросу об оценке вероятности ошибки тестирования систем информационной безопасности. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение,* спец. вып. № 5, 2012, с. 279–283.

[2] Крамер Г. *Математические методы статистики*. Москва, Наука, 1975, 648 с.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Матвеев В.А., Басараб М.А., Троицкий И.И. Асимптотические свойства оценки вероятности ошибки тестирования систем информационной безопасности. *Инженерный журнал: наука и инновации,* 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/997.html

Матвеев Валерий Александрович родился в 1939 г. Д-р техн. наук, профессор, руководитель Научно-учебного комплекса «Информатика и системы управления», заведующий кафедрой «Информационная безопасность» МГТУ им. Н.Э. Баумана. Заслуженный деятель науки РФ, лауреат государственных премий СССР и РФ, лауреат премий Правительства РФ в области науки и образования.

Басараб Михаил Алексеевич родился в 1970 г., окончил Харьковский авиационный институт им. Н.Е. Жуковского в 1993 г. Д-р физ.-мат. наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор 5 монографий и более 100 научных работ в области прикладной математики, информатики, цифровой обработки сигналов, радиофизики.

Троицкий Игорь Иванович родился в 1955 г., окончил Московский инженерно-физический институт в 1978 г. Канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор около 40 работ в области информационной безопасности и исследования систем обработки информации и управления. e-mail: iitroickiy@mail.ru