

# ДИАГНОСТИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ И КАЧЕСТВА СЛОЖНЫХ СИСТЕМ

УДК 519.24; 57.017

## СРАВНЕНИЕ МОЩНОСТИ ХИ-КВАДРАТ КРИТЕРИЯ И КРИТЕРИЯ КРАМЕРА – ФОН МИЗЕСА ДЛЯ МАЛЫХ ТЕСТОВЫХ ВЫБОРОК БИОМЕТРИЧЕСКИХ ДАННЫХ

А. И. Иванов, А. И. Газин, С. Е. Вятчанин, К. А. Перфилов

### *Введение*

Информационное общество предполагает активное использование интернет-ресурсов. Государственные и частные структуры создают на своих сайтах личные кабинеты пользователей. К сожалению, существующая практика парольной защиты доступа к личным кабинетам обладает существенными признаками уязвимости. Пользователи не способны запоминать длинные случайные пароли. Владелец информационного ресурса не может быть уверен в том, что к личному электронному кабинету получил доступ именно его хозяин. Пароль может быть перехвачен программной закладкой, также не составляет проблемы подменить IP-адрес интернет-пользователя.

Для усиления защиты доступа к электронным кабинетам в настоящее время разрабатываются технологии биометрической аутентификации личности путем преобразования личных биометрических данных человека в его криптографический ключ или длинный случайный пароль доступа. Используются такие биометрические образы, как: рисунок отпечатка пальца [1], рисунок радужной оболочки глаза [2], голосовой пароль [3], рукописный пароль [4], рисунок кровеносных сосудов глазного дна или ладони руки [5]. Естественно, что преобразователи биометрия-код не могут быть идеальными и имеют вероятности ошибок первого и второго рода. Возникает необходимость тестирования ошибок первого и второго рода на реальных биометрических данных. Кроме того, при настройке «нечетких экстракторов» [1–3] и при обучении нейросетевых преобразователей [4, 5] необходимо контролировать отсутствие в биометрических данных грубых ошибок. По сути дела, на небольшом числе примеров биометрического образа необходимо контролировать показатель близости распределения биометрических данных к многомерному нормальному закону [6]. Формально для этой цели может быть использован классический одномерный хи-квадрат критерий Пирсона [7, 8], однако такой подход далек от оптимального. В рамках данной статьи мы попытаемся доказать, что контроль нормальных плотностей распределения биометрических данных выгоднее осуществлять статистическим критерием Крамера – фон Мизеса. Мощность критерия Крамера – фон Мизеса на малых выборках примеров биометрических данных оказывается существенно выше, чем мощность аналогичного критерия хи-квадрат.

### *Появление шумов квантования при статистической обработке малых выборок*

Рассмотрим простейшую ситуацию, когда тестовая или обучающая выборка представлены девятью примерами образа «Свой». Из-за того, что непрерывная функция вероятности  $P(x)$  пер-

вого биометрического параметра –  $v_1$  малой выборки, мы вынуждены описывать ее ступенчатой монотонно возрастающей функцией  $\tilde{P}(x)$ , как это показано в левой части рис. 1.

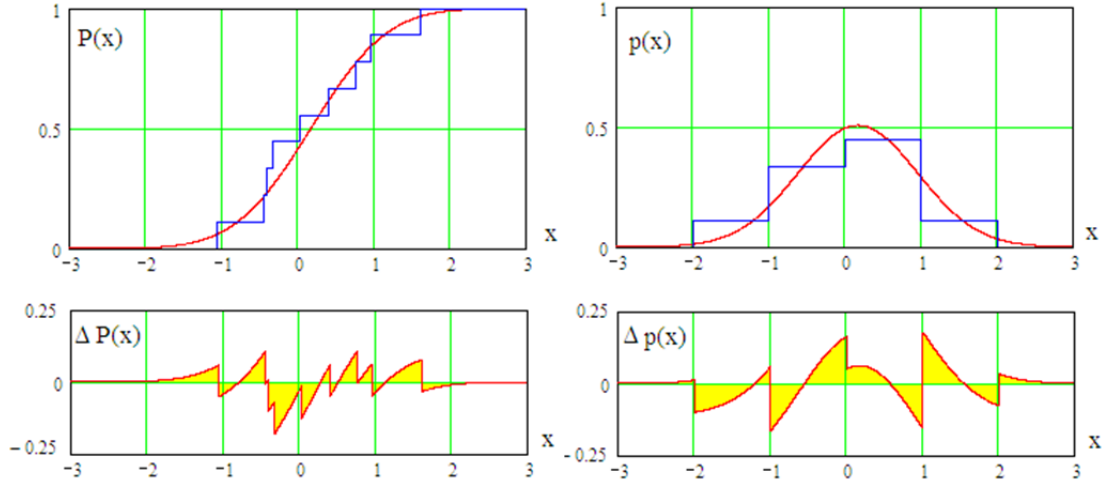


Рис. 1. Эффекты квантования непрерывной вероятности распределения значений и непрерывной плотности распределения значений путем их представления девятью примерами

Для того, чтобы построить ступенчатое монотонно возрастающее приближение  $\tilde{P}(x)$ , необходимо осуществить сортировку биометрических данных по их возрастанию:

$$x_i = \text{sort}(v_{1,i}) \text{ для } i = 0, 1, 2, \dots, n, \quad (1)$$

где  $n$  – размер тестовой выборки или число квантов приближения монотонной функции вероятности.

В этом случае монотонно возрастающая ступенчатая функция будет описываться следующим кусочно-постоянным приближением

$$\tilde{P}(x_i) = \frac{i}{n}. \quad (2)$$

Ошибка приближения или шум квантования находится как разность непрерывной функции вероятности и ее ступенчатого приближения:

$$\Delta P(x) = P(x) - \tilde{P}(x). \quad (3)$$

В нижней части рис. 1 отображены функции ошибки квантования или шумы квантования, возникающие из-за малых тестовых выборок.

В контексте вышеизложенного статистический критерий Колмогорова – Смирнова [7] следует рассматривать как поиск максимального значения модуля ошибки приближения:

$$\sup_{-\infty < x < +\infty} |P(x) - \tilde{P}(x)| = \max |\Delta P(x_i)| \quad (4)$$

или выбор наибольшего из локальных максимумов шума квантования.

С этих же позиций статистический критерий Крамера – фон Мизеса [7] является оценкой стандартного отклонения шума квантования непрерывной функции вероятности:

$$y = \int_{-\infty}^{\infty} \{P(x) - \tilde{P}(x)\}^2 dx = \int_{-\infty}^{\infty} \{E(\Delta P(x)) - \Delta P(x)\}^2 dx = \int_{-\infty}^{\infty} \{\Delta P(x)\}^2 dx = \sigma^2(\Delta P(x)), \quad (5)$$

если выполняется условие нулевого математического ожидания шума квантования  $E(\Delta P(x)) = 0$ .

Следует подчеркнуть, что статистический критерий Колмогорова – Смирнова (4) всегда имеет меньшую мощность в сравнении с критерием Крамера – фон Мизеса (5). Критерий Колмогорова – Смирнова (4) точечный, а критерий Крамера – фон Мизеса (5) интегральный.

Очевидно, что с ростом размеров тестовой выборки  $n$  оба эти статистических критерия набирают мощность оценок, однако оценка по интегральному критерию всегда оказывается надежнее, чем оценка по точечному критерию.

**Использование точки равной вероятности ошибок первого и второго рода при оценке мощности критерия Крамера – фон Мизеса**

Будем исходить из того, что биометрические данные по каждому из контролируемых параметров распределены нормально. Тогда качество данных одного параметра можно оценивать и по критерию Крамера – фон Мизеса. При этом качество принимаемого решения будет существенно зависеть от порога сравнения и размеров тестовой выборки. Получить зависимости мы можем численным моделированием. Результаты численного моделирования для выборок из девяти примеров и 32 примеров приведены на рис. 2.

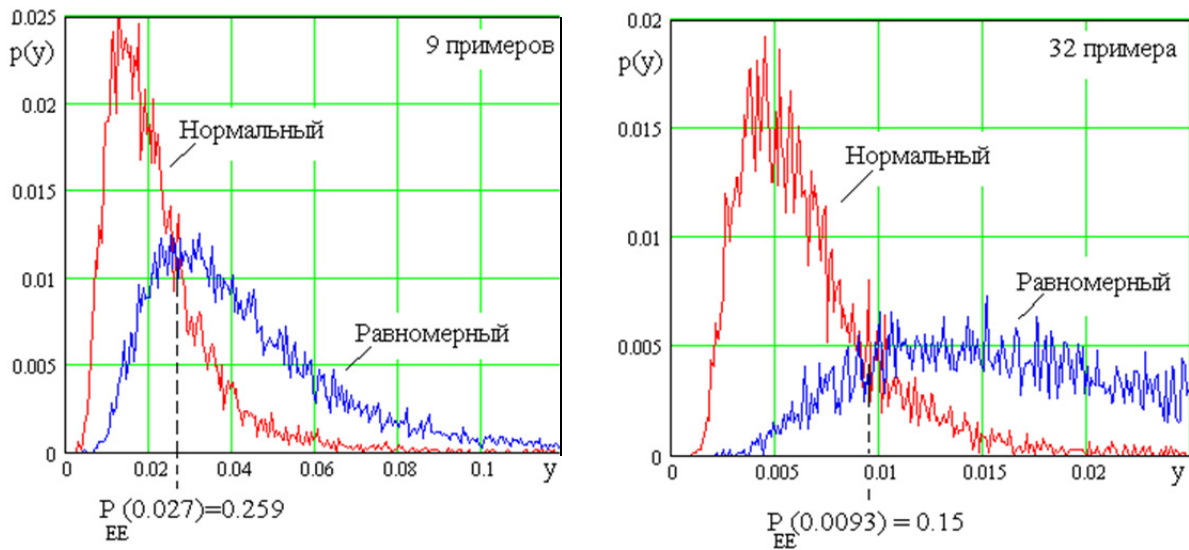


Рис. 2. Гистограммы плотностей распределения значений критерия Крамера – фон Мизеса, построенные для выборок из 9 примеров и 32 примеров

Как видно из рис. 2, плотности распределения значений критерия Крамера – фон Мизеса существенно зависят от размеров тестовой выборки. Для малых выборок динамический диапазон изменения значений критерия оказывается значительным. По мере роста числа примеров в обучающей выборке динамический диапазон существенно снижается.

При использовании любого статистического критерия проверки гипотез необходимо задать порог сравнения, получив для него значения вероятностей ошибок первого и второго рода. Выбор значения порога принятия решения во многом субъективен. Для того, чтобы уйти от субъективности, будем назначать пороги в точке равной вероятности ошибок первого и второго рода:

$$P_1(y) = P_2(y) = P_{EE}(y). \tag{6}$$

Как видно из левой части рис. 2, точка равной вероятности ошибок находится при значении  $y = 0,027$ , при этом значение равной вероятности составляет  $P_{EE}(0,027) = 0,259$ . Это значение отражает тот факт, что на малых выборках добиться малых значений вероятностей первого и второго рода невозможно.

Если выборку увеличить до объема в 32 примера, то происходит существенное снижение вероятности ошибок первого и второго рода  $P_{EE}(0,0093) = 0,15$ . Очевидно, что, повышая размеры тестовой выборки, мы можем монотонно снижать значения вероятностей ошибок первого и второго рода.

**Сравнение по мощности критерия Крамера – фон Мизеса и хи-квадрат критерия Пирсона**

Для представления значения равной вероятности ошибок первого и второго рода критерия Крамера – фон Мизеса как функции, зависящей от размера тестовой выборки, наиболее удобна логарифмическая шкала (рис. 3).

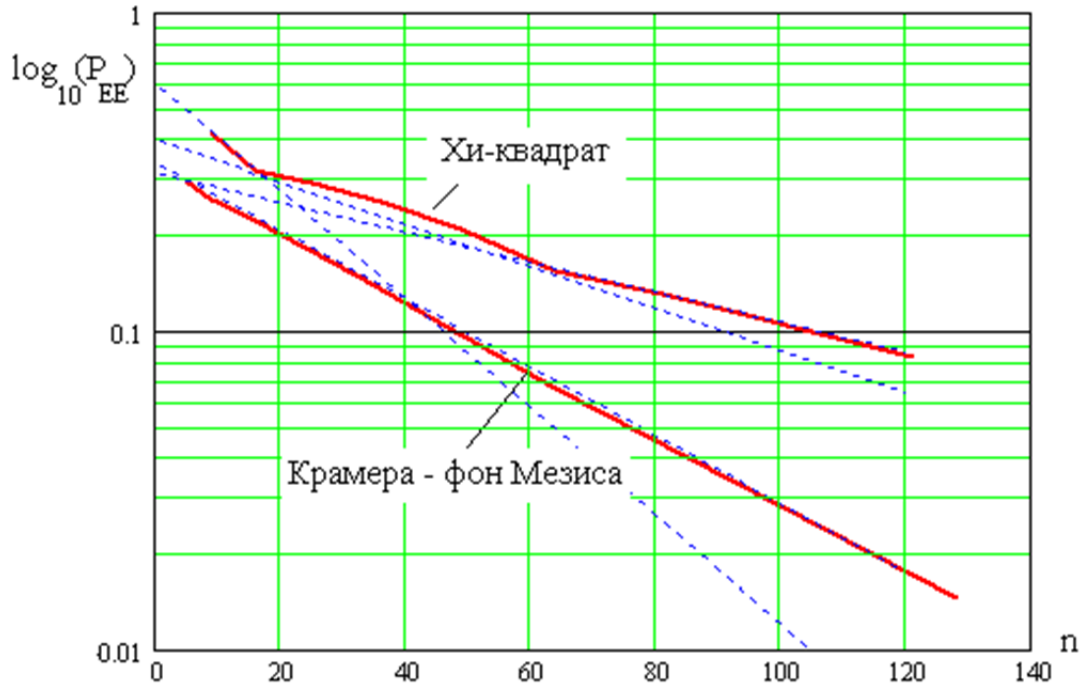


Рис. 3. Влияние объема тестовой выборки на значение равной вероятности ошибок в зависимости от объема тестовой выборки для критериев Крамера – фон Мизеса и хи-квадрат критерия

Как видно из рис. 3,  $\log_{10}(P_{EE}(n))$  является линейной функцией:

$$P_{EE}(n) = 10^{-0,47-0,0107 \cdot n} \text{ при } n = 1, 2, \dots, \infty. \tag{7}$$

Аналогичную зависимость можно построить и для равных вероятностей ошибок критерия хи-квадрат [7, 8]. Из теории известно, что критерий хи-квадрат должен описываться распределением Пирсона:

$$p(\chi^2, m) = \frac{1}{2^{\frac{m}{2}} \cdot \Gamma\left(\frac{m}{2}\right)} \left\{ x^{\frac{m}{2}-1} \cdot \exp\left(\frac{-x}{2}\right) \right\}, \tag{8}$$

где  $\Gamma\left(\frac{m}{2}\right)$  – гамма функция;  $m$  – число степеней свободы.

В свою очередь число степеней свободы  $m$  рекомендуется выбирать исходя из числа столбцов гистограммы [8]:

$$m = k - 3. \tag{9}$$

Для выбора числа столбцов гистограммы существует множество рекомендаций разных авторов. В частности, по действующим рекомендациям Госстандарта [8] можно выбирать этот параметр, применяя следующие правила:

$$\left\{ \begin{array}{l} k \geq \sqrt{n}; \\ k \geq \frac{n}{5}; \\ k \geq \log_2(n) + 1; \\ k \geq 5 \lg(n); \\ k \geq 5 \lg(n) - 5; \\ \dots \end{array} \right. \tag{10}$$

Для того, чтобы снять неопределенность при выполнении численного эксперимента, мы воспользовались гистограммами с числом столбцов

$$\begin{cases} k = 4 & \text{при } 5 < n \leq 16; \\ k = 6 & \text{при } 16 < n \leq 64; \\ k = 8 & \text{при } 64 < n \leq 121. \end{cases} \quad (11)$$

Результаты численного моделирования отражены в виде ломаной кривой, чье кусочно-линейное приближение выглядит следующим образом:

$$\begin{cases} P_{EE}(n) = 10^{-0,22-0,017 \cdot n} & \text{при } 5 < n \leq 16; \\ P_{EE}(n) = 10^{-0,401-0,0066 \cdot n} & \text{при } 16 < n \leq 64; \\ P_{EE}(n) = 10^{-0,503-0,0042 \cdot n} & \text{при } 64 < n \leq 121. \end{cases} \quad (12)$$

Из рис. 3 видно, что критерий Крамера – фон Мизеса обеспечивает существенно меньшую ошибку принятия решений в сравнении с критерием хи-квадрат Пирсона. С ростом объема тестовой выборки преимущество критерия Крамера – фон Мизеса растет. Также преимущество этого критерия увеличивается с увеличением размерности биометрических данных [9–11].

### Заключение

Основной причиной преимуществ критерия Крамера – фон Мизеса является то, что при прочих равных условиях его шумы квантования имеют большую частоту скачков и меньшую амплитуду каждого скачка (см. рис. 1). Как следствие, шумы квантования сглаживаются критерием Крамера – фон Мизеса лучше, чем те же самые шумы квантования в критерии хи-квадрат Пирсона. На типовой выборке биометрических данных в 20 примеров критерий Крамера – фон Мизеса дает в 1,5 раза меньшую вероятность ошибок, чем критерий хи-квадрат Пирсона. При анализе биометрических данных имеет смысл отказаться от использования классического хи-квадрат критерия Пирсона в пользу более мощного критерия Крамера – фон Мизеса.

### Список литературы

1. Ramírez-Ruiz, J. Keys Generation Using Finger Codes / J. Ramírez-Ruiz, C. Pfeiffer, J. Nolzco-Flores // Advances in Artificial Intelligence – IBERAMIA-SBIA. – 2006 (LNCS 4140). – P. 178–187.
2. Monrose, F. Cryptographic key generation from voice / F. Monrose, M. Reiter, Q. Li, S. Wetzel // Proc. IEEE Symp. on Security and Privacy. – 2001. – 354 с.
3. Hao, F. Crypto with Biometrics Effectively / Feng Hao, Ross Anderson, John Daugman // IEEE TRANSACTIONS ON COMPUTERS. – 2006. – Vol. 55, № 9. – 244 p.
4. Нейросетевая защита персональных биометрических данных / Ю. К. Язов, В. И. Волчихин, А. И. Иванов [и др.]. – М. : Радиотехника, 2012. – 157 с.
5. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа / Б. С. Ахметов, А. И. Иванов, В. А. Фунтиков [и др.]. – Алматы, Казахстан : ТОО «Издательство LEM», 2014. – 144 с.
6. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации / Б. С. Ахметов, В. И. Волчихин, А. И. Иванов, А. Ю. Малыгин. – Алматы, Казахстан : КазНТУ им. Сатпаева, 2013. – 152 с.
7. Кобзарь, А. И. Прикладная математическая статистика для инженеров и научных работников / А. И. Кобзарь – М. : ФИЗМАТЛИТ, 2006. – 816 с.
8. ГОСТ Р 50.1.037–2002 Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть I. Критерии типа  $\chi^2$ . – М., 2001. – 140 с.
9. Серикова, Н. И. Эффект снижения размера тестовой выборки за счет перехода к многомерному статистическому анализу биометрических данных / В. И. Волчихин, А. И. Иванов, Н. И. Серикова, Ю. В. Фунтикова // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2015. – № 1. – С. 50–59.
10. Ахметов, Б. Б. Многомерный статистический анализ биометрических данных сетью частных критериев Пирсона / Б. Б. Ахметов, А. И. Иванов, А. В. Безяев, Ю. В. Фунтикова // Вестник Национальной академии наук Республики Казахстан. – 2015. – № 1. – С. 5–11.
11. Быстрый алгоритм оценки высокоразмерной энтропии биометрических образов на малых выборках / Б. Б. Ахметов, А. И. Иванов, А. Ю. Малыгин, А. В. Безяев, А. И. Газин // Труды международного симпозиума Надежность и качество. – 2015. – Т. 2. – С. 283–284.

**Иванов Александр Иванович**

доктор технических наук, доцент,  
начальник лаборатории биометрических  
и нейросетевых технологий,  
Пензенский научно-исследовательский  
электротехнический институт  
(440000, Россия, г. Пенза, ул. Советская, 9)  
E-mail: ivan@pniei.penza.ru

**Газин Алексей Иванович**

кандидат технических наук, доцент,  
кафедра информатики, информационных  
технологий и защиты информации,  
Липецкий государственный педагогический  
университет  
(398020, Россия, г. Липецк, ул. Ленина, 42)  
E-mail: yearn@bk.ru

**Вятчанин Сергей Евгеньевич**

доцент,  
начальник кафедры радио и космической связи,  
Пензенский государственный университет  
(440026, Россия, г. Пенза, ул. Красная, 40)  
E-mail: fvopgu@pnzgu.ru

**Перфилов Константин Александрович**

аспирант,  
Пензенский государственный университет  
(440026, Россия, г. Пенза, ул. Красная, 40)  
E-mail: fvopgu@pnzgu.ru

**Аннотация.** *Актуальность и цели.* Классический статистический критерий хи-квадрат плохо работает на малых тестовых выборках. Статья посвящена исследованию поведения статистического критерия Крамера – фон Мизеса. Целью работы является оценка того, насколько мощность критерия Крамера – фон Мизеса выше мощности критерия хи-квадрат. *Материалы и методы.* Предложено оценивать мощность сравниваемых критериев в точке равновесных ошибок первого и второго рода. Показано, что в логарифмической шкале равной вероятности ошибок мощность критерия Крамера – фон Мизеса описывается прямой линией. Это упрощает вычисления. *Результаты и выводы.* Использование критерия Крамера – фон Мизеса вместо критерия хи-квадрат на выборке из 20 примеров позволяет снизить вероятность ошибок принимаемых решений в полтора раза. Если рассматривать сравниваемые критерии как некоторые нелинейные низкочастотные цифровые фильтры, то критерий Крамера – фон Мизеса оказывается эффективнее критерия хи-квадрат из-за того, что имеет более высокую частоту и меньшую амплитуду скачков шума квантования данных.

**Ключевые слова:** статистический критерий Крамера – фон Мизеса, хи-квадрат критерий Пирсона, подавление шумов квантования.

**Ivanov Aleksandr Ivanovich**

doctor of technical sciences, associate professor,  
head of biometric and neuronal nets technology  
laboratory,  
Penza Scientific Research Electrotechnical Institute  
(440000, 9 Sovetskaja street, Penza, Russia)

**Gazin Aleksey Ivanovich**

candidate of technical sciences, associate professor,  
sub-department of computer sciences, information  
technology and information protection,  
Lipetsk State Pedagogical University  
(398020, 42 Lenina street, Lipetsk, Russia)

**Vjatchanin Sergej Evgen'evich**

associate professor,  
head of sub-department of radio  
and space communications,  
Penza State University  
(440026, 40 Krasnaya street, Penza, Russia)

**Perfilov Konstantin Aleksandrovich**

postgraduate student,  
Penza State University  
(440026, 40 Krasnaya street, Penza, Russia)

**Abstract.** *Background.* Classical statistical criteria chi-square works bad with small text samples. This article is about of researching statistical criteria of Cramer – von Mizes works with small text samples. The propose of this research is compare of applicability statistical criteria of Cramer – von Mizes and statistical criteria chi-square with small text samples. *Materials and methods.* It's suggested to compare the power of this methods in the point of equiprobable type one and type two errors. It's proved that in logarithmic scale equal probability errors of the power criteria of Cramer – von Mizes is straight line, this makes calculations easier. *Results and conclusions.* Using the criterion of the Cramer-von Mizes instead of the chi-square test on a sample of 20 examples to reduce the likelihood of decisions made errors in one and a half times. If we consider the criteria compared some nonlinear low-frequency digital filters, the criterion of Cramer-von Mizes is more effective then chi-square due to the fact that there is a higher frequency and lower amplitude data quantization noise spikes.

**Key words:** Cramer – von Mizes statistical criteria, chi square criteria of Pearson, noise elimination of quantization.

**УДК 519.24; 57.017**

**Сравнение мощности хи-квадрат критерия и критерия Крамера – фон Мизеса для малых тестовых выборок биометрических данных / А. И. Иванов, А. И. Газин, С. Е. Вятчанин, К. А. Перфилов // Надежность и качество сложных систем. – 2016. – № 2 (14). – С. 67–73.**