---

**Банных А.Г.** Энтропийная оценка качества непрерывных биометрических данных малых обучающих выборок // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 5 – 9 (http://пниэи.рф/activity/science/BIT/T10–p5.pdf)

В докладе рассматривается проблема оценки качества непрерывных биометрических данных с учетом их коррелированности. Для дискретных биометрических данных эта проблема решена. Предложено решать задачу путем вычисления энтропии непрерывных биометрических данных после их квантования. Квантовать непрерывные данные предложено исходя из условия обеспечения равных вероятностей ошибок первого и второго рода. Это позволяет делать вычисления однозначными, не зависящими от принятого шага квантования. Фактически предложено осуществлять регуляризацию вычислений путем стабилизации результатов вычисления и исключения таких факторов как число порогов квантования (шага квантования биометрических данных).

**Bannykh A.G.** Entropy estimation of the quality of continuous biometric data of small training samples // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 5 - 9

The report examines the problem of assessing the quality of continuous biometric data taking into account their correlation. For discrete biometric data, this problem is solved. It is proposed to solve the problem by calculating the entropy of continuous biometric data after their quantization. Quantization of data is proposed on the basis of the condition of ensuring equal probabilities of errors of the first and second kind. This allows you to make calculations unambiguous, independent of the quantization step taken. In fact, it is proposed to carry out regularization of calculations by stabilizing the calculation results and eliminating such factors as the number of quantization thresholds (the step of quantizing biometric data).

---

**Елфимов А.В., Безяев А.В.** Сравнение гипотезы нормального распределения и гипотезы бета распределения расстояний Хэмминга для выходных кодов нейросетевых преобразователей // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 10 – 14 (http://пниэи.рф/activity/science/BIT/T10–p10.pdf)

Рассматривается ситуация, когда распределение расстояний Хэмминга для нейронной сети или «нечеткого экстрактора» не является нормальным. Предложено перейти при описании распределений расстояний Хэмминга в нормированную систему координат, где оказывается применимо описание статистик в виде бета распределения. Бета распределения дают возможность учета асимметрии при прогнозировании вероятности ошибок первого и второго рода. Делается вывод о необходимости расширения ГОСТ Р 52633.3 процедурами, построенными на учете асимметрии распределений расстояний Хэмминга.

**Elfimov A.V., Bezyaev A.V.** Comparison of the normal distribution hypothesis and the hypothesis of the Hamming distance beta distribution for output codes of neural network converters // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 10 - 14

The situation is considered when the distribution of Hamming distances for a neural network or "fuzzy extractor" is not normal. It is suggested to go over when describing the distribution of Hamming distances to a normalized coordinate system, where the description of statistics in the form of a beta distribution turns out to be applicable. Beta distributions make it possible to account for asymmetry in predicting the probability of errors of the first and second kind. It is concluded that it is necessary to extend GOST R 52633.3 with procedures based on taking into account the asymmetry of the Hamming distances.

---

**Безяев А.В., Иванов А.И. Корнеев О.В.** Типовая схема защиты нейросетевых архивов биометрических данных не криптографическим хешированием, построенном на линейных рекуррентах подсчета контрольных сумм CRC-4 // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 15 – 18 (http://пниэи.рф/activity/science/BIT/T10–p15.pdf)

Предложена типовая схема защиты таблиц обученной искусственной нейронной сети путем многократного хэширования данных с использованием не криптографической хэш-функции CRC-4. Такое техническое решение позволяет снизить размер программного обеспечения в сравнении с аналогичным техническим решением, построенным на использовании вызова полноценной криптографической функции хэширования. Последнее является важным фактором в случае реализации всех вычислений на специализированном процессоре с низкой разрядностью и малым объемом памяти.

**Bezyaev A.V., Ivanov A.I., Korneev O.V.** Typical scheme of protection of neural network archives of biometric data is not cryptographic hashing built on linear recurrences of CRC-4 checksums calculation // Proceedings of scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 15 - 18

A typical scheme for protecting tables of a trained artificial neural network is proposed by repeatedly hashing data using non-cryptographic hash function CRC-4. This technical solution allows you to reduce the size of the software in comparison with a similar technical solution built on the use of a call to a full cryptographic hash function. The latter is an important factor in the case of realization of all calculations on a specialized processor with low bit capacity and low memory capacity.

---

**Иванова Н.А., Серикова Ю.И.** Синтез предсказателя, оценивающего ошибку вычисления математического ожидания для выборки из 32 примеров биометрического образа // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 19 – 20 (http://пниэи.рф/activity/science/BIT/T10–p19.pdf)

Рассматривается проблема повышения точности вычисления математического ожидания на малых выборках биометрических данных. Рассматривается обычный предсказатель, построенный на априорной информации о нормальном законе распределения значений. Такой предсказатель дает симметричный интервал предсказания, ширина которого на 21.4% оказывается выше, чем суммарная ширина асимметричных левого и правого интервалов предсказания. Предложено вычислять асимметричные интервалы как минимум и максимум подвыборок, полученных отбрасыванием из основной выборки одного опыта.

**Ivanova N.A., Serikova Y.I.** Synthesis of the predictor estimating the error of calculating the mathematical expectation for a sample of 32 examples of the biometric image // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 19 - 20

The problem of increasing the accuracy of computing mathematical expectation on small samples of biometric data is considered. An ordinary predictor based on a priori information about the normal law of distribution of values is considered. Such a predictor gives a symmetric prediction interval, whose width is 21.4% higher than the total width of the asymmetric left and right prediction intervals. It is proposed to calculate asymmetric intervals at least and a maximum of subsamples obtained by dropping one experiment from the main sample.

---

**Качайкин Е.И.** Технические требования к средствам автоматизации экспертного анализа авторства рукописных текстов // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 21 – 23 (http://пниэи.рф/activity/science/BIT/T10–p21.pdf)

Рассматривается задача формирования технического задания на опытно-конструкторскую разработку экспертной системы автоматизированной оценки авторства рукописных текстов. Показано, что этого класса автоматизированные системы должны выполняться в двух исполнениях. Сформулированы основные требования к системам, ориентированным на неподготовленного пользователя не являющегося экспертом-почерковедом. Этот тип систем автоматизации может быть создан в виде бесплатного Интернет ресурса и, скорее всего, не станет полноценным программным продуктом. Второй класс подобных систем должен быть ориентирован на его применении подготовленными экспертами-почерковедами, что позволяет формировать для него большие базы естественных биометрических рукописных образов. Кроме того, этот класс систем может быть ориентирован на привлечение «облачных» вычислительных ресурсов. Отмечается необходимость оценки доверительных вероятностей принимаемых с использованием экспертных систем решений для обоих классов систем.

**Kachaykin E.I.** Technical requirements for automation of expert analysis of authorship of handwritten texts // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 21 - 23

The task of forming a technical task for the experimental design of an expert system for the automated evaluation of the authorship of handwritten texts is considered. It is shown that this class of automated systems should be performed in two versions. The basic requirements for systems oriented to an unprepared user who is not an expert handwriter are formulated. This type of automation systems can be created as a free Internet resource and, most likely, will not become a full-fledged software product. The second class of such systems should be oriented toward its application by trained handwriting experts, which allows it to form large bases of natural biometric handwritten images. In addition, this class of systems can be focused on attracting "cloud" computing resources. It is noted that it is necessary to estimate the confidence probabilities of decisions taken with the use of expert systems for both classes of systems.

---

**Вятчанин С.Е., Иванов А.И**. Симметризация многомерной статистической модели сети квадратичных форм при использовании малого объема исходных биометрических данных образа «Свой» // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 24 – 26 (http://пниэи.рф/activity/science/BIT/T10–p21.pdf)

Рассматривается сеть хи-квадрат функционалов. Показано, что подобные сети квадратичных форм могут быть симметризованы, а после симметризации может быть создана статистическая модель биометрического образа «Свой». Эта модель позволяет предсказать значение порога для каждого из рассматриваемых квадратичных функционалов, обеспечивающего заданную вероятность ошибок первого рода. При вычислении среднего модуля коэффициентов корреляции происходит усреднение ошибок каждого из частных коэффициентов корреляции, что эквивалентно регуляризации решаемой задачи или снижению объема обучающей выборки.

**Vyatchanin S.E., Ivanov A.I.** Symmetrization of the multidimensional statistical model of a network of quadratic forms using a small amount of initial biometric data of the image "Svoi" // Proceedings of the scientific and technical conference of a cluster of Penza enterprises that ensure the SAFETY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 24 - 26

We consider a chi-square network of functionals. It is shown that such networks of quadratic forms can be symmetrized, and after symmetrization a statistical model of the biometric image "Svoi" can be created. This model allows us to predict the threshold value for each of the quadratic functionals under consideration, which provides a given probability of errors of the first kind. In calculating the average modulus of correlation coefficients, the errors of each of the partial correlation coefficients are averaged, which

is equivalent to the regularization of the problem being solved or to a decrease in the volume of the training sample.

---

**Серикова Ю.И., Банных А.Г.** Бинормальная регуляризация оценки числа слабо коррелированных данных биометрического образа «Свой» // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 27 – 30 (http://пниэи.рф/activity/science/BIT/T10–p27.pdf)

Рассматривается задача оценки слабо коррелированных биометрических данных биометрического образа «Свой». Показано, что вершина распределения коэффициентов корреляции имеет провал по сравнению с данными нормального закона распределения значений. Предложено описывать распределение реальных данных смесью двух нормальных законов распределения значений сдвинутых относительно центральной точки. Дан фрагмент программы, осуществляющей, рассматриваемое статистическое приближение. Предложенные вычислительные процедуры дают увеличение предсказанного числа параметров со слабой корреляцией примерно на 10%.

**Serikova Y.I., Bannykh A.G.** Binormal regularization of the estimation of the number of weakly correlated data of the biometric image of "Svoi" // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 27 - 30

The problem of estimating weakly correlated biometric data of the biometric image "Svoi" is considered. It is shown that the peak in the distribution of the correlation coefficients has a dip compared with the data of the normal law of distribution of values. It is proposed to describe the distribution of real data by a mixture of two normal distribution laws shifted relative to the central point. A fragment of the program implementing the statistical approximation under consideration is given. The proposed computational procedures give an increase in the predicted number of parameters with a weak correlation by approximately 10%.

---

**Перфилов К.А.** Сравнение мощности критериев среднего геометрического при их интегральном и интегро-дифференциальном исполнении // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 31 – 34 (http://пниэи.рф/activity/science/BIT/T10–p31.pdf)

В работе показано, что статистический критерий среднего геометрического функций вероятности распределения данных малой выборки оказывается слабее аналогичного критерия, построенного как произведение функции вероятности и плотности распределения функции вероятности. В статье этот факт доказывается для выборок, состоящих из 36 опытов. Численное моделирование показывает, что интегральный вариант критерия среднего геометрического позволяет различать нормальный и равномерный закон распределения значений малой выборки с

равновероятными значениями ошибок первого и второго рода 0.223. Интегро-дифференциальный вариант этого же критерия дает значения $P_{EE}$= 0.045, что в 5 раз лучше. С ростом объема тестовой выборки выигрыш увеличивается.

**Perfilov K.A.** Comparison of the power of the average geometric criteria for their integral and integro-differential execution // Proceedings of the scientific and technical conference of the cluster of Penza enterprises that ensure the SAFETY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 31 - 34

It is shown that the statistical criterion of the average geometric probability distribution function of a small sample is weaker than the analogous criterion constructed as the product of the probability function and the probability distribution density function. In the article this fact is proved for samples consisting of 36 experiments. Numerical modeling shows that the integral variant of the geometric mean criterion makes it possible to distinguish between the normal and uniform law of distribution of values of a small sample with equiprobable values of errors of the first and second kind 0.223. The integro-differential variant of the same criterion gives values of $P_{EE}$ = 0.045, which is 5 times better. With the increase in the volume of the test sample, the winnings increase

---

**Калашников Д.М., Захаров О.С., Ахметов Б.Б., Пащенко Д.В.** Создание среды моделирования «БиоНейроГолос», ориентированной на обучение больших искусственных нейронных сетей алгоритмом ГОСТ Р 52633.5 при выполнении лабораторных работ русскоязычными студентами университетов России, Беларуси и Казахстана // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 35 – 39 (http://пниэи.рф/activity/science/BIT/T10–p35.pdf)

В статье рассматривается вопрос о создании программной среды моделирования «БиоНейроГолос» по аналогии с уже созданной средой моделирования «БиоНейроАвтограф». Отмечается дешевизна микрофонов как средства ввода голосовой биометрии стандартными средствами ОС Windows. Это позволяет ожидать широкого применения, создаваемого программного продукта. Дана проработка фрагментов интерфейса ввода голосовых данных для их последующей нейросетевой обработки. Новое программное средство ориентировано на свободное использование университетами России, Белоруссии и Казахстана при преподавании дисциплин, связанных с нейросетевой обработкой биометрических данных.

**Kalashnikov D.M., Zakharov O.S., Akhmetov B.B., Pashchenko D.V.** Creation of modeling environment "BioNeyroGlos", focused on training large artificial neural networks by the GOST R 52633.5 algorithm in the laboratory work of Russian-speaking students of Russian, Belarusian and Kazakh universities // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 35 - 39

The article considers the question of creating a software environment for modeling "BioNeiroGlos" by analogy with the already created modeling environment "BioNeyroAvtograf." The cheapness of microphones as a means of inputting voice biometrics by standard means of Windows OS is noted. This allows us to expect a wide application, the created software product. The development of fragments of the interface for entering voice data for their subsequent neural network processing is given. The new software is aimed at free use by universities in Russia, Belarus and Kazakhstan when teaching disciplines related to neural network processing of biometric data.

---

**Юнин А.П., Корнеев О.В.** Оценка энтропии легко запоминаемых, длинных паролей со смыслом в ASCII кодировке для русского и английского языков // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 40 – 42 (http://пниэи.рф/activity/science/BIT/T10–p40.pdf)

В работе показано, что быстрые алгоритмы вычисления энтропии осмысленных текстов в пространстве расстояний Хэмминга дают значительную методическую ошибку, если вести подсчет расстояний в двоичной системе. Получаются слишком оптимистичные оценки. Методическая ошибка исчезает, если расстояния Хэмминга вычислять в 8-ми битной кодировке по модулю 256. Ошибка в выборе способа вычисления расстояний Хэмминга приводит к эффекту локального хэширования данных, приводящего к завышению значений оценки энтропии.

**Yunin A.P., Korneev O.V.** Estimation of the entropy of easily remembered, long passwords with meaning in ASCII encoding for Russian and English languages // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 40 - 42

The paper shows that fast algorithms for calculating the entropy of meaningful texts in the Hamming distance space give a significant methodological error when counting distances in the binary system. The results are too optimistic. Methodological error disappears if the Hamming distances are calculated in 8-bit encoding modulo 256. An error in choosing the method of calculating Hamming distances leads to the effect of local hashing of data, leading to an overestimation of the values of the entropy estimate.

---

**Безяев А.В.** Оценка выигрыша от использования фрагментов квантовой суперпозиции при корректировке ошибочных состояний нейросетевого преобразователя биометрия-код // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 43 – 46 (http://пниэи.рф/activity/science/BIT/T10–p43.pdf)

Показано, что при корректировке разряда кодов «Свой» путем перебора их возможных состояний нет смысла принимать во внимание все разряды. Более целесообразно выделить только нестабильные разряды кода «Свой» и перебирать только их состояния. Это позволяет снизить затраты вычислительных ресурсов на несколько порядков. Приведена схема безопасного рекурсивного формирования эталонных хэш-остатков кодов, предназначенных для выявления и корректировки малого числа ошибок.

**Bezyaev A.V.** Evaluation of the gain from the use of fragments of quantum superposition in the correction of erroneous states of the neuronet converter biometry-code // Proceedings of the scientific and technical conference of the cluster of Penza enterprises that ensure the SAFETY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 43 - 46

It is shown that when adjusting the discharge of "Svoi" codes by enumeration of their possible states, it makes no sense to take into account all the digits. It is more expedient to select only unstable digits of the code "Svoi" and to sort out only their states. This allows you to reduce the cost of computing resources by several orders of magnitude. The scheme of safe recursive formation of standard hash-remnant codes intended for detection and correction of a small number of errors is given.

---

**Сериков А.В., Иванов А.И.** Перспектива создания нейросетевых идентификаторов уровня слабых корреляционных связей с большим числом сетей и выходных состояний // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 47 – 51 (http://пниэи.рф/activity/science/BIT/T10–p47.pdf)

Рассматривается проблема выявления слабых корреляционных связей малой выборки биометрических параметров. Показано, что ошибка вычисления нулевых значений коэффициентов корреляции оказывается много больше, чем ошибки вычисления коэффициентов корреляции, отличных от нуля. Сделано предположение о том, что нейросетевой анализ двухмерных портретов точек, отображающих состояния пар биометрических данных, будет давать более точные результаты, чем классика. Последнее открывает возможность снижения ошибок вычисления коэффициентов корреляции за счет более сложной нейросетевой обработки данных.

**Serikov A.V., Ivanov A.I.** The prospect of creating neural network identifiers for the level of weak correlation links with a large number of networks and output states // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 47 - 51

The problem of revealing weak correlation links of a small sample of biometric parameters is considered. It is shown that the error in calculating the zero values of the correlation coefficients turns out to be much larger than the errors in calculating the correlation coefficients that are different from zero. The assumption is made that the neural network analysis of two-dimensional portraits of points displaying the states of pairs of biometric data will yield more accurate results than the classics. The latter

opens the possibility of reducing errors in calculating correlation coefficients due to more complex neural network processing of data.

---

**Гончаров С.М., Боршевников А.Е., Половинко А.С.** Генератор синтетических образов электроэнцефалограмм активности головного мозга, используемый для увеличения размеров тестовых и обучающих выборок биометрических данных // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 52 – 57 (http://пниэи.рф/activity/science/BIT/T10–p52.pdf)

Рассматривается задача увеличения размеров баз биометрических образов электроэнцефалограмм путем применения морфинг скрещивания образов-родителей и получения образов-потомков. Отмечается эффективность процедур морфинг скрещивания для биометрических образов электроэнцефалограмм, полученных при предъявлении испытуемому одиночных десятичных цифр 0, 1, 2,…, 9 на экране компьютера. Впервые показана эффективность процедур синтеза искусственных биометрических образов по ГОСТ Р 52633.2 для образов электроэнцефалограмм. Дано обобщение результатов на пары символов и тройки символов.

Goncharov S.M., Borshevnikov A.E., Polovinko A.S. The generator of synthetic images of electroencephalograms of brain activity, used to increase the size of test and training samples of biometric data // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 52 - 57

The problem of increasing the size of the bases of the biometric images of electroencephalograms is considered by applying morphing of parent-parent images and obtaining images of descendants. The effectiveness of morph crossing procedures for biometric images of electroencephalograms obtained by presenting to the subject single decimal digits 0, 1, 2, ..., 9 on the computer screen is noted. For the first time, the efficiency of procedures for synthesizing artificial biometric images according to GOST R 52633.2 for images of electroencephalograms is shown. A generalization of the results to pairs of symbols and a triplet of symbols is given.

---

**Ефимов О.В.** Перспективы широкого использования защищенных биометрических технологий в ответственных гражданских приложениях // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 58 – 59 (http://пниэи.рф/activity/science/BIT/T10–p58.pdf)

Рассматриваются ответственные приложения биометрии. Подчеркивается высокий уровень стандартизации нейросетевой биометрии, обеспеченный усилиями членов ТК 362 «Защита информации». Ставится задача разработки документов, регламентирующих различные аспекты криптографической защиты персональных биометрических данных, размещенных в нейросетевых

контейнерах. Дан перечень ответственных приложений биометрии, где особенно остро стоит проблема стандартизации криптографических механизмов, защищающих биометрию пользователя.

**Efimov O.V.** Prospects for the widespread use of secure biometric technologies in responsible civil applications // Proceedings of the scientific and technical conference of the cluster of Penza enterprises that ensure the SAFETY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 58 - 59

Responsible applications of biometrics are considered. High level of standardization of neural network biometrics, ensured by the efforts of the members of TC 362 "Information Protection", is underlined. The task is to develop documents regulating various aspects of cryptographic protection of personal biometric data located in neural network containers. The list of responsible applications of biometrics is given, where the problem of standardization of cryptographic mechanisms protecting the user's biometrics is especially acute.

---

**Сулавко А.Е, Ковальчук А.С., Семенова З.В., Осипов С.С.** Идентификация функционального состояния водителей транспортных средств с учетом отклонений наблюдаемой вариабельности сердечного ритма // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 60 – 62 (http://пниэи.рф/activity/science/BIT/T10–p60.pdf)

Рассматривается проблема контроля состояния водителя транспортного средства путем анализа биометрических особенностей работы его сердца при прохождении предрейсового контроля. Предложено использовать решающее правило Байеса, многократно примененное к эталонным и проверяемым биометрическим данным. Ошибки принимаемых решений находятся в интервале от 1,6% до 14,7%. Биометрические данные работы сердца планируется объединить с данными теплового изображения лица водителя.

**Sulavko A.E., Kovalchuk A.S., Semenova Z.V., Osipov S.S.** Identification of the functional state of drivers of vehicles taking into account deviations of the observed heart rate variability // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 60 - 62.

The problem of control of the driver's state of a vehicle by analyzing the biometric features of the work of his heart during pre-trip control is considered. It is proposed to use the Bayesian decision rule, repeatedly applied to the reference and verified biometric data. The errors in the decisions made range from 1.6% to 14.7%. Biometric data of the heart work is planned to be combined with the thermal image data of the driver's face.

---

**Ложников П.С., Сулавко А.Е., Толкачева Е.В., Жумажанова С.С.** Распознавание водителей и оценка их функциональных состояний по обычному и тепловому изображениям лица // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 63 – 65 (http://пниэи.рф/activity/science/BIT/T10–p63.pdf)

Рассматривается задача биометрической оценки функционального (психофизического) состояния водителя путем анализа обычного изображения его лица в видимом свете и инфракрасного изображения. Применялись сети функционалов Пирсона, ориентированные на выявление модулей корреляционных связей на уровне значимости 0.3. Так же были исследованы сети хи-модуль функционалов. Оба типа анализируемых сетей сравнивались при реализации 50 и 200 функционалов (нейронов), имеющих разное число входов. Дан график, позволяющий сравнивать данные по приближению равновероятных значений ошибок.

**Lozhnikov P.S., Sulavko A.E., Tolkacheva E.V., Zhumzhanova S.S.** Recognition of drivers and assessment of their functional states by ordinary and thermal images of the face // Proceedings of the scientific and technical conference of the cluster of Penza enterprises that ensure the SAFETY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 63 - 65

The task of biometric evaluation of the functional (psychophysical) state of the driver is considered by analyzing the usual image of his face in visible light and infrared image. The networks of Pearson's functionals were used, aimed at identifying correlation correlation modules at a significance level of 0.3. The networks of chi-moduli of functionals were also investigated. Both types of analyzed networks were compared with the realization of 50 and 200 functionals (neurons) having different number of inputs. A graph is given allowing to compare data on the approximation of equiprobable error values.

---

**Афанасьев А.А.** Непрерывная аутентификация легитимного пользователя сети связи, опирающаяся на использование личностных особенностей низкоскоростного кодирования речевых данных // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 66 – 73 (http://пниэи.рф/activity/science/BIT/T10–p66.pdf)

Рассматриваются средства речевой связи, обеспечивающие высокий уровень сжатия голоса для его цифровой передачи по плохим каналам связи. Показано, что вектора кодовой книги CELP-подобных алгоритмов обработки речи с разной частотой, востребуются при восстановлении речи разных дикторов. Анализируя интенсивность запросов векторов кодовой книги удается построить портрет голосовых особенностей личности говорящего. Это открывает возможность создания систем идентификации личности говорящего на произвольном речевом потоке. Дополнительные технические возможности могут быть реализованы на старом парке технических средств речепреобразования.

**Afanasyev A.A.** Continuous authentication of a legitimate user of the communication network, based on the use of personal characteristics of low-speed coding of speech data // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 66 - 73

The means of voice communication providing a high level of voice compression for its digital transmission over poor communication channels are considered. It is shown that the codebook vectors of CELP-like speech processing algorithms with different frequencies are in demand when speech of different speakers is restored. Analyzing the intensity of requests for codebook vectors, it is possible to construct a portrait of the voice characteristics of the speaker's personality. This opens the possibility of creating systems for identifying the speaker's personality on an arbitrary speech stream. Additional technical capabilities can be realized at the old park of technical means of speech conversion.

---

**Павлов М.А., Секретов М.В.** Обезличивание персональных данных пациентов с использованием «нечетких экстракторов» или нейросетевых преобразователей биометрии в длинный код перед их размещением в облачных хранилищах // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 74 – 77 (http://пниэи.рф/activity/science/BIT/T10–p74.pdf)

Рассматривается задача защиты персональных данных через их обезличивание двумя технологиями: технологией «нечетких экстракторов» и технологией применения нейросетевых преобразователей биометрия-код. Показано, что, приведенные в статье две блок-схемы реализации процесса обезличивания, имеют существенные различия. Подчеркивается, что при обезличивании электронных медицинских документов с пациента нет необходимости брать согласие на обработку его персональных данных. Снижается информационная ценность для третьих лиц баз данных медицинских учреждений.

**Pavlov M.A., Secretsov M.V.** Anonymization of patients' personal data using "fuzzy extractors" or neuronet biometric converters into long code before placing them in cloud storage // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 74 - 77

The problem of protection of personal data through their depersonalization by two technologies is considered: the technology of "fuzzy extractors" and the technology of application of neuronet converters of biometry-code. It is shown that the two block diagrams of the process of depersonalization presented in the article have significant differences. It is emphasized that in the de-identification of electronic medical documents from the patient, there is no need to agree to the processing of his personal data. Information value of third-party databases of medical institutions is reduced.

**Газин А.И., Ахметов Б.Б., Сериков А.В., Серикова Ю.И.** Оценка соотношения методической и случайной составляющих погрешности вычисления коэффициентов корреляции для малых выборок биометрических данных // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 78 – 83 (http://пниэи.рф/activity/science/BIT/T10–p78.pdf)

Показано, что при малых значениях модуля оцениваемого коэффициента корреляции случайная составляющая погрешности оказывается много выше ее методической составляющей. Для корреляционных коэффициентов с большим значением модуля положение меняется, случайная составляющая уменьшается, а методическая погрешность увеличивается. Дано приближение полиномом второй степени методической составляющей погрешности, используемое при ее частичной компенсации. Утверждается, что связи объема выборки с квадратичным корректирующим полиномом хорошо описывается гиперболой степени 1.29.

**Gazin A.I., Akhmetov B.B., Serikov A.V., Serikova Y.I.** Estimation of the ratio of the methodological and random components of the error in calculating the correlation coefficients for small samples of biometric data // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 78 - 83

It is shown that for small values of the modulus of the estimated correlation coefficient, the random component of the error is much higher than its methodological component. For correlation coefficients with a large value of the module, the position changes, the random component decreases, and the methodical error increases. The polynomial of the second degree is approached by the methodological component of the error, used for its partial compensation. It is asserted that the relationship between the sample size and the quadratic correcting polynomial is well described by a hyperbola of degree 1.29.

---

**Малыгина Е.А., Урнев И.В.** Пакет международных стандартов XML программной поддержки для Интернет обработки биометрических данных // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 84 – 87 (http://пниэи.рф/activity/science/BIT/T10–p84.pdf)

Рассматриваются международные биометрические стандарты ISO/IEC JTC1 sc37, ориентированные на применение XML поддержки обработки

биометрических данных. Приведена таблица из 7 таких стандартов, сделан вывод о расширении внимания мирового сообщества к проблеме стандартизации XML поддержки обработки биометрических данных. Сделано предположение о том, что отечественные биометрические стандарты серии ГОСТ Р 52633.xx-20xx должны поддержать, наблюдаемую мировую тенденцию стандартизации XML поддержки обработки биометрических данных.

**Malygina E.A., Urnev I.V.** Package of international standards for XML software support for the Internet processing of biometric data // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 84 - 87

International biometric standards ISO/IEC JTC1 sc37, oriented to the application of XML support for processing biometric data are considered. A table of 7 such standards is given, it is concluded that the world community's attention to the problem of standardizing XML support for processing biometric data is growing. The assumption is made that the domestic biometric standards of the GOST R 52633.xx-20xx series should support the observed worldwide trend of standardizing XML support for processing biometric data.

---

**Чернов П.С., Смирнов И.И., Суровцев Д.А., Майоров А.В., Секретов М.В.** Корпоративный интернет-портал с мобильным доступом, защищенный от сторонних вмешательств шифрованием IP-трафика и поддержкой протоколов биометрической аутентификации пользователя // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 88 – 91 (http://пниэи.рф/activity/science/BIT/T10–p88.pdf)

Показано, что роль биометрической аутентификации личности усиливается при использовании корпоративных интернет-порталов с мобильным доступом, защищенных от сторонних вмешательств шифрованием IP-трафика. Так же роль биометрии растет по мере увеличения числа пользователей корпоративной информационной системы, находящейся на одной из контролируемых территории предприятия. Рассматриваются особенности применения доверенной вычислительной среды USB «БиоТокен» в корпоративной информационной среде предприятия, подключаемой между серийным сканером биометрии и рабочей станцией.

**Chernov P.S., Smirnov I.I., Surovtsev D.A., Mayorov A.V., Secretsov M.V.** Corporate Internet portal with mobile access, protected from third-party interference by encryption of IP traffic and support of protocols for biometric user authentication // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 88 - 91

It is shown that the role of biometric identity authentication is enhanced by using corporate Internet portals with mobile access, protected from third-party interference by encryption of IP traffic. The role of biometrics also increases with the increase in the

number of users of the corporate information system located in one of the controlled areas of the enterprise. The peculiarities of using the trusted computing environment USB "Biotoken" in the enterprise corporate information environment, connected between the serial biometric scanner and the workstation are considered.

---

**Акмаев А.Ж.** Об одном подходе к построению масштабируемой скоростной оптимизации криптографического алгоритма ГОСТ Р 34.12-2015 с длиной блока 128 бит за счет использования предвычисленных таблиц // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 92 – 95 (http://пниэи.рф/activity/science/BIT/T10–p92.pdf)

Рассматривается проблема снижения потребления вычислительных ресурсов при реализации криптографического алгоритма ГОСТ Р 34.12-2015 с длиной блока 128 бит. Исследован вопрос оптимизации обмена мощности процессора на память, где хранятся предварительно вычисленные таблицы ускорения вычислений. Актуальность рассматриваемых вопросов увеличивается при снижении разрядности использованных для шифрования процессоров и их потребления. Наиболее сложным случаем является реализация криптографических операций на 4-х битных процессорах FRID идентификационных карт, поддерживающих криптографические протоколы биометрико-нейросетевой аутентификации.

**Akmaev A.Z.** About one approach to the construction of scalable speed optimization of the cryptographic algorithm GOST R 34.12-2015 with a block length of 128 bits due to the use of precomputed tables // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 92 - 95

The problem of reducing the consumption of computing resources in the implementation of the cryptographic algorithm GOST R 34.12-2015 with a block length of 128 bits is considered. The issue of optimization of processor power-to-memory exchange, where the previously computed acceleration calculations tables are stored, is investigated. The relevance of the issues under consideration increases with the decrease in the number of processors used for encryption and their consumption. The most difficult case is the implementation of cryptographic operations on 4-bit FRID processors of identification cards supporting cryptographic protocols of biometric-neural network authentication.

---

**Рубцов Я.Д.** О реализации преобразования Гильберта при имитационном моделировании сигналов управления в каналах связи // Труды научно–технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.** Издательство АО «ПНИЭИ», Пенза–2016, Том 10, с. 96 – 97 (http://пниэи.рф/activity/science/BIT/T10–p96.pdf)

Рассматривается цифровая реализация преобразований Гильберта при восстановлении данных управления, прошедших через плохой канал связи.

Описан численный эксперимент, позволяющий оценить работоспособность нового метода обработки информации. Особое внимание уделяется связи данных в пространстве Фурье образов и в пространстве образов Гильберта. Рассматривается так же вопрос оптимизации вычислений в пространстве образов Гильберта за счет использования симметризации заранее вычисленных квадратных матриц.

**Rubtsov J.D.** On the implementation of the Hilbert transform in the simulation simulation of control signals in communication channels. // Proceedings of the scientific and technical conference of the cluster of Penza enterprises providing SECURITY OF INFORMATION TECHNOLOGIES. Publishing house of JSC "PNIEI", Penza-2016, Volume 10, p. 96 - 97

The digital realization of Hilbert transformations is considered when restoring control data that has passed through a poor communication channel. A numerical experiment is described that makes it possible to evaluate the operability of a new method of processing information. Particular attention is paid to the connection of data in the Fourier space of images and in the space of Hilbert images. We also consider the question of optimizing computations in the space of Hilbert images by using the symmetrization of the pre-computed square matrices.