

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет информационных
технологий и электроники

Специальность 10.05.03 –

Специализация -

Кафедра
«Информационная безопасность
систем и технологий»

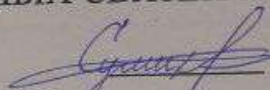
Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

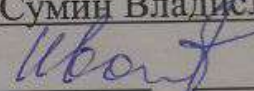
ПРАКТИКУМ ПО ОЦЕНКЕ ЭНТРОПИИ КОДОВ ОТКЛИКОВ НЕЙРОСТЕТИ
НА ПРИМЕРЕ РУКОПИСНОГО ОБРАЗА «ЧУЖОЙ» В ПРОСТРАНСТВЕ
КОРРЕЛЯЦИОННЫХ СВЯЗЕЙ МЕЖДУ РАЗРЯДАМИ

Студент



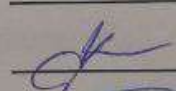
Сумин Владислав Алексеевич

Руководитель



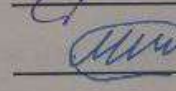
Иванов А.И.

Нормоконтролёр



Егорова Н.А.

Рецензент ведущий инженер АО «ПНИЭИ»

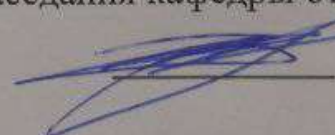


Секретов М.В.

Работа допущена к защите (протокол заседания кафедры от

10.06.22 № 9)

Заведующий кафедрой



С.Л. Зефирова

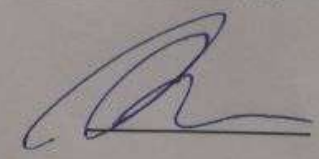
Работа защищена с отметкой

О М Л М Ч О

(протокол заседания ГЭК

от 23.06.22 № 8)

Секретарь ГЭК



А.П. Иванов

Пенза 2022

Оглавление

Термины и определения	3
Введение.....	4
1 Обзор средств тестирования биометрической аутентификации.....	5
2 Разработка алгоритма для вычисления коэффициентов парной корреляции и программная реализация его.....	11
3 Тестирование разработанной программы.....	17
4 Разработка руководства пользователя	26
5 Разработка рекомендаций для проведения практикума.....	29
6 Разработка индивидуальных вариантов выполнения практикума	54
7 Вредные психофизиологические факторы, влияющие на опорно- двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	56
Заключение	58
Список используемых источников.....	59
Приложение А Обязательное Алгоритм программы	61
Приложение Б Справочное Статья, принятая к публикации в сборнике научных статей по материалам Всероссийской научно-технической конференции «Безопасность информационных технологий»	64

Термины и определения

Биометрическая аутентификация – процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путём преобразования этого образа в соответствии с заранее определённым протоколом аутентификации.

Нейросетевой преобразователь – преобразователь, заранее обученный преобразовывать многомерные континуумы примеров биометрического образа «Свой» в почти однозначный выходной код криптографического ключа или длинного пароля доступа по ГОСТ Р 52633.0-2006. После каждого обучения нуждается в быстром автоматическом тестировании.

Биометрический образ «Свой» – биометрический образ человека, параметры которого порождают с высокой вероятностью от 0.92 до 0.95 на выходах обученной нейронной сети код его личного криптографического ключа.

Биометрический образ «Чужой» – случайный биометрический образ, параметры которого порождают на выходах обученной нейронной сети случайный выходной код.

Ошибка второго рода – вероятность ложной идентификации пользователя, отсутствующего в базе данных.

Введение

Как известно больше половины мирового населения имеют аккаунты на одной или нескольких платформах. Как показывает практика, парольная защита доступа к личным интернет ресурсам имеет ряд уязвимостей. Пользователи обычно пользуются короткими, легко подбираемыми паролями. Для повышения безопасности парольной защиты в настоящее время желательно использовать биометрическую аутентификацию.

Биометрические системы доступа в наше время достаточно удобны в отличии от паролей и носителей информации, которые могут быть скомпрометированы третьими лицами. Биометрические системы основаны на личных параметрах человека, которые потерять почти невозможно.

Целью ВКР является разработка практикума по оценке энтропии кодов откликов нейросети на примере рукописного образа «Чужой» в пространстве корреляционных связей между разрядами.

Для достижения данной цели необходимо выполнить следующее:

- обзор средств тестирования биометрической аутентификации;
- разработка алгоритма для вычисления коэффициентов парной корреляции и программная реализация его;
- тестирование разработанной программы;
- разработка руководства пользователя;
- разработка рекомендации для поведения практикума;
- разработка индивидуальных вариантов выполнения практикума.

1 Обзор средств тестирования биометрической аутентификации

Классифицируют два метода биометрической аутентификации:

- статический метод биометрической аутентификации;
- динамический метод биометрической аутентификации.

Статические методы биометрической аутентификации основаны на физиологических характеристиках человека, которые не меняются на протяжении всей его жизни. К такому методу можно отнести радужную оболочку глаза, отпечаток пальца.

Основными плюсами данного метода является:

- неотделимость, идентификатор нельзя забыть, потерять или передать третьим лицам;
- воссоздать или подделать идентификатор пользователя будет довольно сложно;
- процесс аутентификации происходит довольно быстро и полностью автоматизирован.

Так же у статистического метода есть ряд минусов:

- биометрические сканеры многих систем дорогие и не многие смогут позволить себе приобретение таких систем;
- могут возникнуть ситуации, когда идентификатор пользователя поврежден или недоступен для считывания;
- необходимость выполнения определенных условий окружающей среды для биометрической аутентификации.

Метод аутентификации по отпечатку пальца самая распространенная технология, которая основана на уникальных папиллярных узлах на пальцах рук человека. Полученный образ отпечатка пальца преобразуется в цифровой код и сравнивается с ранее введенными цифровыми кодами.

Плюсы распознавания по отпечатку пальца:

- легкость в использовании;

- удобство и надежность.

Минусы распознавания по отпечатку пальца:

- деформации папиллярного рисунка может повлиять на распознавание.

Динамические методы основаны на поведенческих характеристиках людей. К ним можно отнести распознавание по голосу или по подписи.

Плюсы поведенческой биометрии:

- у каждого пользователя есть свой набор анализируемых поведенческих характеристик;
- при аутентификации не требуется смена пользовательского сценария;
- повышенная точность в многофакторной аутентификации.

Минусы поведенческой биометрии:

- неточность возникнуть из-за того, что поведение пользователя непостоянно и от определенной жизненной ситуации усталости, плохого самочувствия может меняться;
- требует большого количества личной информации для определения стандартного поведения пользователя.

Если взять поведенческий метод распознавания по подписи, то в таком методе аутентификация использует два изображения. Он сравнивает полученное изображение с уже имевшимся в системе и тем самым пропускает или отклоняет попытку авторизации. В момент регистрации пользователь должен несколько раз расписаться для сбора данных, после чего алгоритмы извлекают уникальные характеристики пользователя, которые в дальнейшем служат для распознавания образа «Свой», «Чужой».

Плюсы распознавания по подписи:

- практически невозможно подделать;
- быстро и безопасно.

Минусы распознавания по подписи:

- высокая вероятность ошибок распознавания.

Проведя анализ методов аутентификации статистических и динамических образов пользователей можно сделать следующие выводы.

Биометрическое сканирование статистических образов характеризует точность и практически безотказная работа благодаря не допускающим никаких отклонений алгоритмам распознавания. Благодаря отчетливости использования биометрические методы аутентификации зарекомендовали себя и совершенствуются и дополняются не так часто в связи с тем, что каждый из методов по-своему универсален и возможностей обойти его не так просто.

Биометрическое сканирование динамических образов характеризует объемность и некоторая трудность в работе, из-за гибких алгоритмов распознавания. Благодаря высокой степени защищенности, система может отказать настоящему пользователю в 40 % случаев и имеет некоторые ограничения по использованию. Это происходит из-за того, что не всем пользователям подходит динамическая процедура аутентификации. Подобное исходит из психофизического состояния человека на момент регистрации в системе с последующей идентификацией и аутентификацией в ней.

Все эти методы позволяют создать уникальный замок. Это служит гарантией того что опыт полученный злоумышленником при взломах будет бесполезен.

Все биометрические технологии строятся на сканировании биометрических образов человека и извлечении из них контролируемых параметров. Основной задачей биометрической аутентификации является предоставить доступ носителю образа «Свой» к его информационному ресурсу, преобразовав биометрические параметры в разряды кода ключа доступа. Второй задачей биометрической аутентификации является преобразование случайных параметров случайного образа «Чужой» в случайные разряды случайного кода. Преобразование непрерывных биометрических параметров в дискретные бинарные состояния в «нечетких экстракторах» осуществляется пороговыми функциями бинарного квантования [6].

Простейшие бинарные квантователи выполняют сравнение анализируемых данных со значением единственного порога. Квантователь может давать скачок из состояния «0» в состояние «1» при переходе возрастающей переменной через порог. Возможно использование инверсных квантователей, которые при переходе возрастающей переменной через порог дают инверсное изменение состояний из «1» в «0». Настройка каждого квантователя осуществляется выбором его типа и выбором порога квантования. Целью настройки квантователей является как можно большее снижение энтропии разрядов кода «Свой» при как можно большем увеличении энтропии состояний разрядов кода «Чужой» [6].

Настройка считается идеальной тогда, когда значение энтропии «Свой» равно нулю. В этом случае ошибка первого рода (отказ в доступе «Своему») практически невозможна.

Основным средством тестирования биометрической аутентификации в данной работе выступает среда моделирования «БиоНейроАвтограф». Она позволяет преобразовывать рукописные образы в динамические символьные пароли.

Так как программа общедоступна, данные лежат в открытом хранении в директории DATA. В ней содержатся файлы:

- 3sigma.txt (содержит информацию о факте попадания биометрических);сданных каждого из 416 параметров в его допустимый интервал ± 3);
- mean.txt (содержит запись среднего значения каждого из 416 контролируемых биометрических параметров);
- mera.txt (содержит меры Хэмминга между кодом «trainKey» и кодом «trainKey», полученные при инициализации режима «проверить»);
- params.txt (содержит 416 биометрических параметров, учитываемых нейронной сетью);

- stdev.txt (содержит 416 стандартных отклонений биометрических параметров, учитываемых нейронной сетью);
- testKeys.txt (содержит данные о коде длиной 256 бит, полученном на выходах нейронной сети при предыдущих проверках);
- trainKey.txt (содержит данные о коде длиной 256 бит, использованном при обучении искусственной нейронной сети);
- weights.txt (содержит данные о 24 весах 256 нейронов преобразователя биометрия-код, полученных в результате последнего обучения).

В программе используется эмулятор искусственной нейронной сети, имеющей множество выходов. Число выходов искусственной нейронной сети определяется длиной порождаемого ею биометрического ключа. Это исключает взлом программы через обнаружение и подмену последнего бита решающего правила. Программа имеет многобитовое решающее правило, сочетание значений бит которого уникально и злоумышленнику неизвестно.

Преимуществом нейросетевых биометрических хранителей паролей является то, что сам ключ в них не хранится, не хранятся также тайные рукописные биометрические образы. После обучения сети вся эта информация удаляется. Восстановить конфиденциальные данные по структуре связей нейросети и величине её весовых коэффициентов практически невозможно.

Обучение нейросетевого преобразователя происходит в автоматическом режиме по ГОСТ Р 52633.5-2011 [2]. Для обучения нейросетевого преобразователя биометрический код использует от 8 до 20 примеров образа «Свой» и не менее 256 примеров образа «Чужой».

Так как биометрические образы могут быть подвержены к атакам подбора, основным требованием является вычисление вероятности ошибок второго рода и выполнение процедур тестирования.

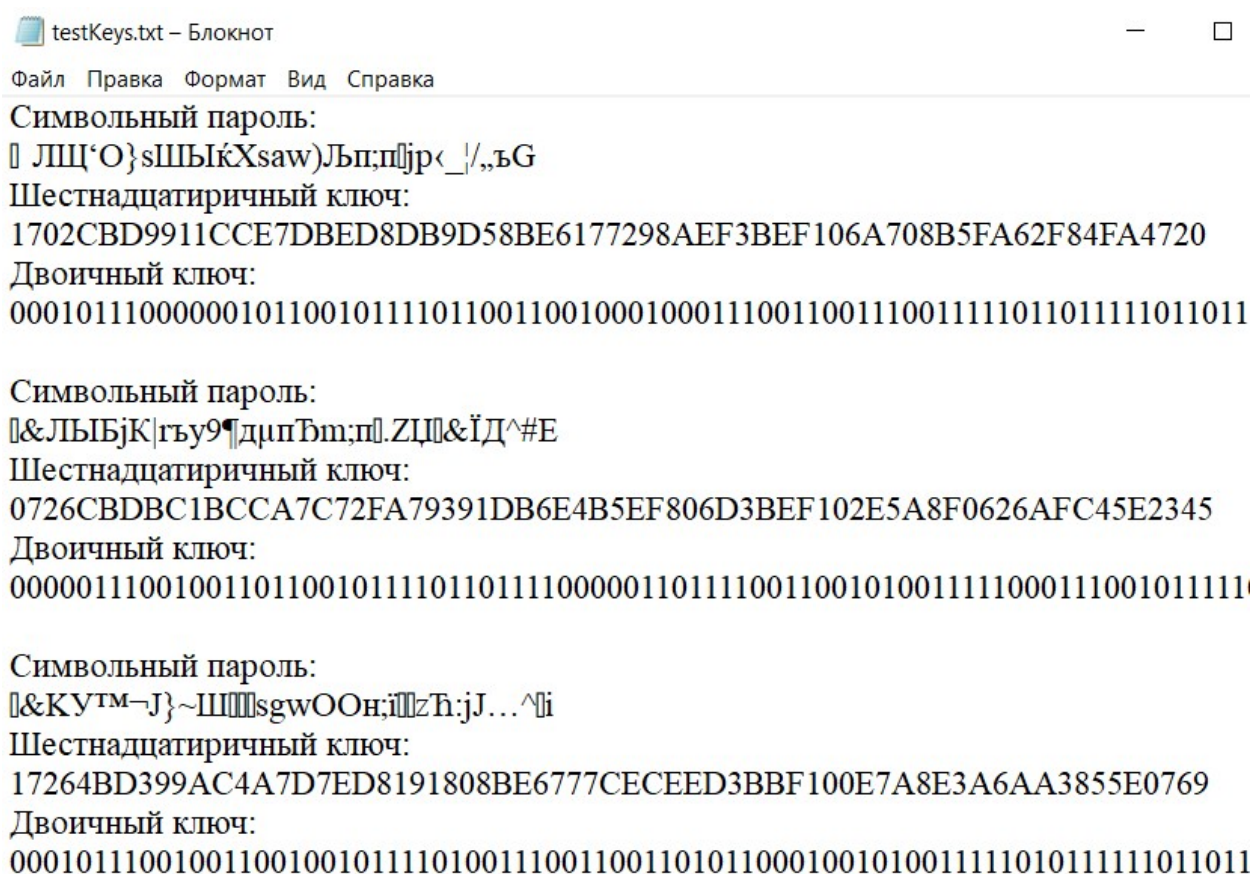
Ошибка второго рода должна оцениваться либо по международным рекомендациям стандарта ГОСТ Р ИСО/МЭК 19795-1-2007, либо ГОСТ 3 52633.3-2011.

Если производить оценку по ГОСТ Р ИСО/МЭК 19795-1-2007 [3], то придется использовать тестовые базы с объемом тестовых образов «Чужой» в 30 раз больше, чем обратная величина предполагаемой стойкости к атакам подбора. Так, если будет тестироваться защита образа с вероятностью ошибок в 0.0000001, размер тестовой базы должен составлять более 30 миллионов образов «Чужой». Это является значительным юридическим барьером для выполнения лабораторных работ по биометрии для университетов. Во всех странах сбор, хранение и использовать большие базы биометрических образов ЗАПРЕЩЕНО. Именно по этой причине постоянно пишут СОГЛАСИЯ на обработку своих персональных данных.

Решить проблему возможно, если воспользоваться отечественным стандартом по быстрому тестированию на малых выборках. ГОСТ Р 52633.3-2011 [4]. Этот стандарт требует перехода от анализа обычных кодов к расстояниям Хэмминга между ними.

2 Разработка алгоритма для вычисления коэффициентов парной корреляции и программная реализация его

Как известно среда моделирования «БиоНейроАвтограф» общедоступна, это позволяет ей хранить биометрические данные в открытом виде. При автоматическом обучении нейросетевого преобразователя программа выводит данные о коде длиной 256 бит, полученных на выходах нейронной сети, в файл testKeys.txt хранящийся в папке Data. Данные представлены на рисунке 1.



```
testKeys.txt – Блокнот
Файл  Правка  Формат  Вид  Справка
Символьный пароль:
ЛЩ‘О}sШЫkXsaw)Льп;пjр<_/,ъG
Шестнадцатиричный ключ:
1702CBD9911CCE7DBED8DB9D58BE6177298AEF3BEF106A708B5FA62F84FA4720
Двоичный ключ:
0001011100000010110010111101100110010001000111001100111001111101101111011011

Символьный пароль:
&ЛЫБjK|гъу9¶дпЪm;п.ЗЦ&ЇД^#Е
Шестнадцатиричный ключ:
0726CBDBC1BCCA7C72FA79391DB6E4B5EF806D3BEF102E5A8F0626AFC45E2345
Двоичный ключ:
00000111001001101100101111011011110000011011110011001010011111000111001011111

Символьный пароль:
&КУ™~J}~ШsgwOOн;иzЪ;jJ...^и
Шестнадцатиричный ключ:
17264BD399AC4A7D7ED8191808BE6777CECEED3BBF100E7A8E3A6AA3855E0769
Двоичный ключ:
0001011100100110010010111101001110011001101011000100101001111101011111011011
```

Рисунок 1 - Хранимые данные в testKeys.txt

Для удобства исследования связи разрядов стоит выделить двоичный ключ каждого образа и записать в отдельный файл.

Для исследования взаимосвязей разрядов образов «Чужой» применяется формула подсчета коэффициентов корреляции Пирсона. Значения коэффициента корреляции варьируются от 0 до ± 1 . Формула (1) показывает связь между величинами, чем больше абсолютное значение, тем выше теснота связи.

$$r_{xy} = \frac{\sum(x_i - \bar{X}) * (y_i - \bar{Y})}{\sqrt{\sum(x_i - \bar{X})^2 * (y_i - \bar{Y})^2}}, \quad (1)$$

где r_{xy} – коэффициент корреляции;

x_i, y_i – значения переменных;

$\bar{X}, \bar{Y}$ – среднее выборочное.

Так как данные имеют бинарный вид и имеют только две границы 0 и 1, следует построить четырехклеточную таблицу сопряженности:

Таблица 1 – Сопряженность разрядов

Границы	Обозначения
00	a
01	b
10	c
11	d

Благодаря таблице 1 стало допустимо применение формулы (1) для подсчета связи между двумя величинами образа «Чужой». Для упрощения расчетов можно применить формулу (2).

$$\varphi = \frac{ad - bc}{\sqrt{(a+b) * (c+d) * (a+c) * (b+d)}} \quad (2)$$

Формула (2) может быть применима в том случае, если данные представлены в четырехклеточной таблице сопряженности. Иначе говоря, формула (2) подобна формуле (1), но использование ее ограничено.

Был разработан алгоритм калькулятора для вычисления коэффициентов корреляции, представленный в приложении А.

В силу того, что корреляционный калькулятор должен давать доступ к большим массивам данных, было принято решение включить в экранную форму два скроллинга для отображения массива коэффициентов корреляции и расстояний Хэмминга.

Расстояние Хэмминга вычисляется путем сравнения бинарных видов одинаковой длины исследуемых пар ключей. Результатом вычисления является количество отличающих позиций.

Калькулятор коэффициентов корреляции был разработан на языке C++. Его экранная форма, представлена на рисунке 2.

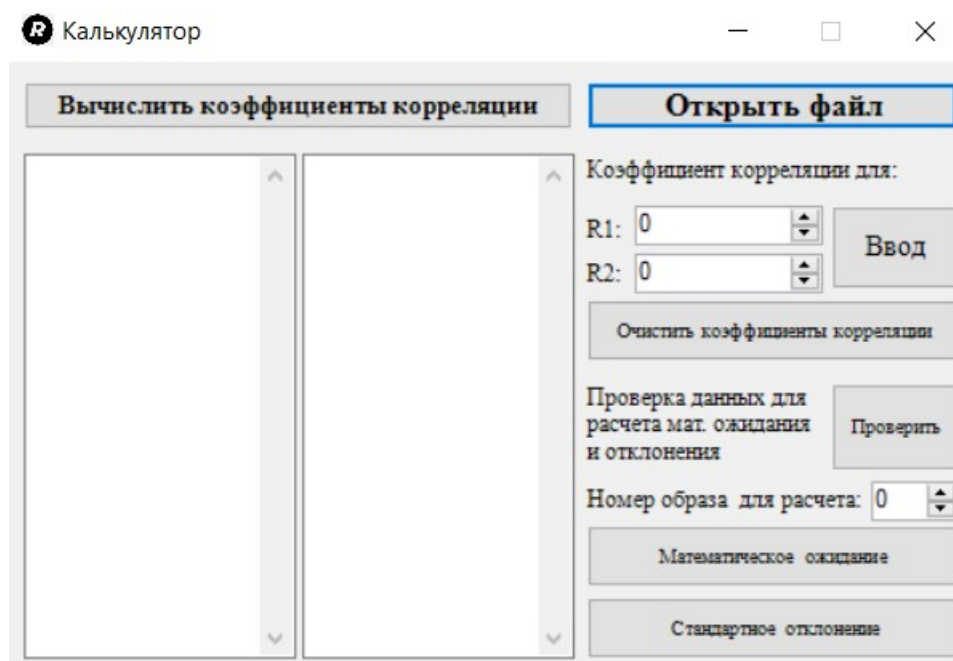


Рисунок 2- Экранная форма разработанного калькулятора

Так как данный калькулятор создан для работы на малых выборках для всех введенных значений пользователем было поставлено ограничение от 0 до 256.

Если пользователь не открыл отчетный файл программы моделирования «БиоНейроАвтограф», а так же ввел значения превышающие количество вычисленных образов, выводятся на экран ошибки, представленные на рисунках 3 - 6.

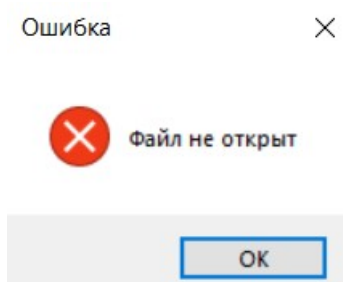


Рисунок 3 - Ошибка показывает, что пользователь не открыл отчетный файл

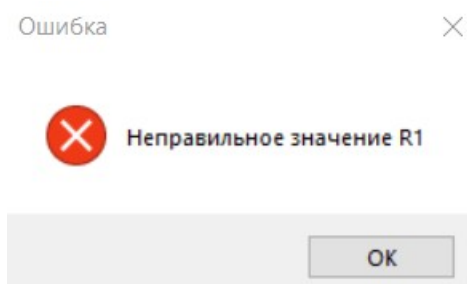


Рисунок 4 - Ошибка показывает, что значение R1 превышает количество обрабатываемых образов

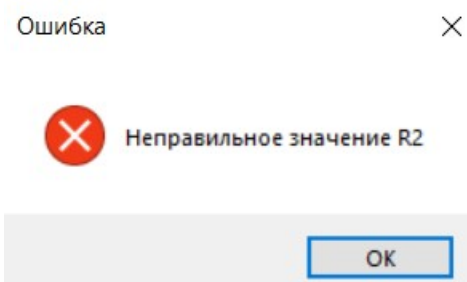


Рисунок 5 - Ошибка показывает, что значение R2 превышает количество обрабатываемых образов

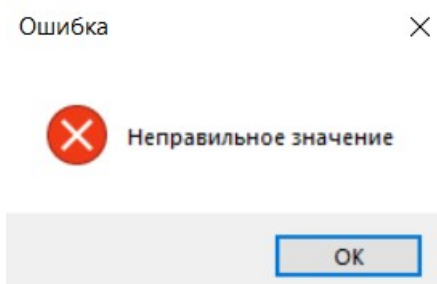


Рисунок 6 - Ошибка показывает, что пользователь в «Номер образа для расчета» ввел значение превышающее количество обрабатываемых образов

Для расчета коэффициентов корреляции и расстояний Хэмминга используется экранная форма, представленная на рисунке 7.

R(0,1) = 0.506	^	H(0,1) = 63	^
R(0,2) = 0.529		H(0,2) = 60	
R(0,3) = 0.570		H(0,3) = 55	
R(0,4) = 0.471		H(0,4) = 68	
R(0,5) = 0.333		H(0,5) = 86	
R(0,6) = 0.387		H(0,6) = 79	
R(0,7) = 0.384		H(0,7) = 79	
R(0,8) = 0.348		H(0,8) = 83	
R(0,9) = 0.522		H(0,9) = 61	
R(0,10) = 0.205		H(0,10) = 102	
R(0,11) = 0.380		H(0,11) = 80	
R(0,12) = 0.493		H(0,12) = 65	
R(0,13) = 0.436		H(0,13) = 73	
R(0,14) = 0.506		H(0,14) = 63	
R(0,15) = 0.570		H(0,15) = 55	
R(0,16) = 0.591		H(0,16) = 52	
R(0,17) = 0.523		H(0,17) = 61	
R(0,18) = 0.741		H(0,18) = 33	
R(0,19) = 0.266	v	H(0,19) = 94	v

Рисунок 7 - Экранная форма для расчета коэффициентов корреляции и расстояний Хэмминга

Коэффициенты корреляции отображаются с тремя десятичными цифрами, а расстояния Хэмминга целые числа, находящиеся на интервале от 0 до 256.

После чего данные полученные в ходе расчета заносятся в таблицу 2.

Таблица 2 – Результаты работы программы

Сравниваемые образы	R	H
0,1	0.506	63
0,2	0.529	60
0,3	0.570	5
0,4	0.471	68
0,5	0.333	86

Для удобства нахождения нужного образа используется экранная форма, представленная на рисунке 8.

Коэффициент корреляции для:

R1:

R2:

Рисунок 8 - Экранная форма для нахождения нужного образа

Результат выполнения записывается в экранную форму, представленную на рисунке 9.

Рисунок 9 - Результат выполнения

Аналогичным образом выводится на экран математическое ожидание и стандартное отклонение при использовании экранной формы представленной на рисунке 10.

Рисунок 10 - Экранная форма для расчета мат. ожидания и отклонения

Математическое ожидание вычисляется по формуле (3), а стандартное отклонение по формуле (4).

$$E = \frac{\sum x_i}{n}, \quad (3)$$

где x_i – каждое наблюдаемое значение признака;

N – количество наблюдений(объем выборки).

$$\sigma = \sqrt{\frac{\sum (x_i - X)^2}{n-1}}, \quad (4)$$

где x_i – каждое наблюдаемое значение признака;

X – среднее арифметическое;

N – количество наблюдений(объем выборки).

3 Тестирование разработанной программы

Для автоматического нахождения отчетного файла разработанная программа была перемещена в корневую папку среды моделирования «БиоНейроАвтограф». Результат показан на рисунке 11.

Data	27.04.2022 18:11	Папка с файлами	
Manual.files	27.04.2022 15:00	Папка с файлами	
Приложение1_БиоРынок	27.04.2022 15:00	Папка с файлами	
bnc32.dll	27.08.2014 15:58	Расширение при...	152 КБ
Manual.htm	21.01.2013 16:26	Microsoft Edge HT...	35 КБ
БиоНейроАвтограф.exe	27.08.2014 15:58	Приложение	636 КБ
Калькулятор.exe	27.04.2022 18:07	Приложение	227 КБ

Рисунок 11 - Корневая папка «БиоНейроАвтограф»

Для того что бы результаты вычисления корреляционного калькулятора были корректны перед использованием был удален уже существующий файл в среде моделирования testKeys.txt. Результат удаления показан на рисунке 12.

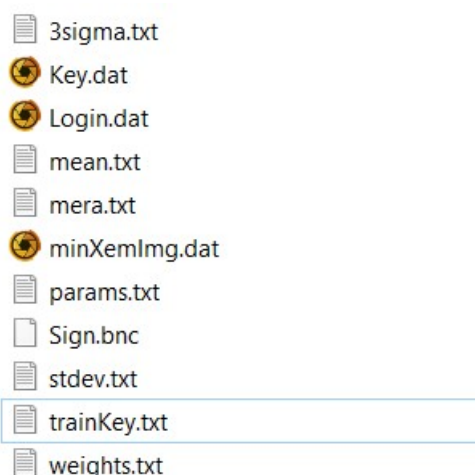


Рисунок 12 - Папка Data среды моделирования «БиоНейроАвтограф»

После чего была запущена среда моделирования в режиме тестирования для примеров одного образа «Чужой». Результат показан на рисунке 13.

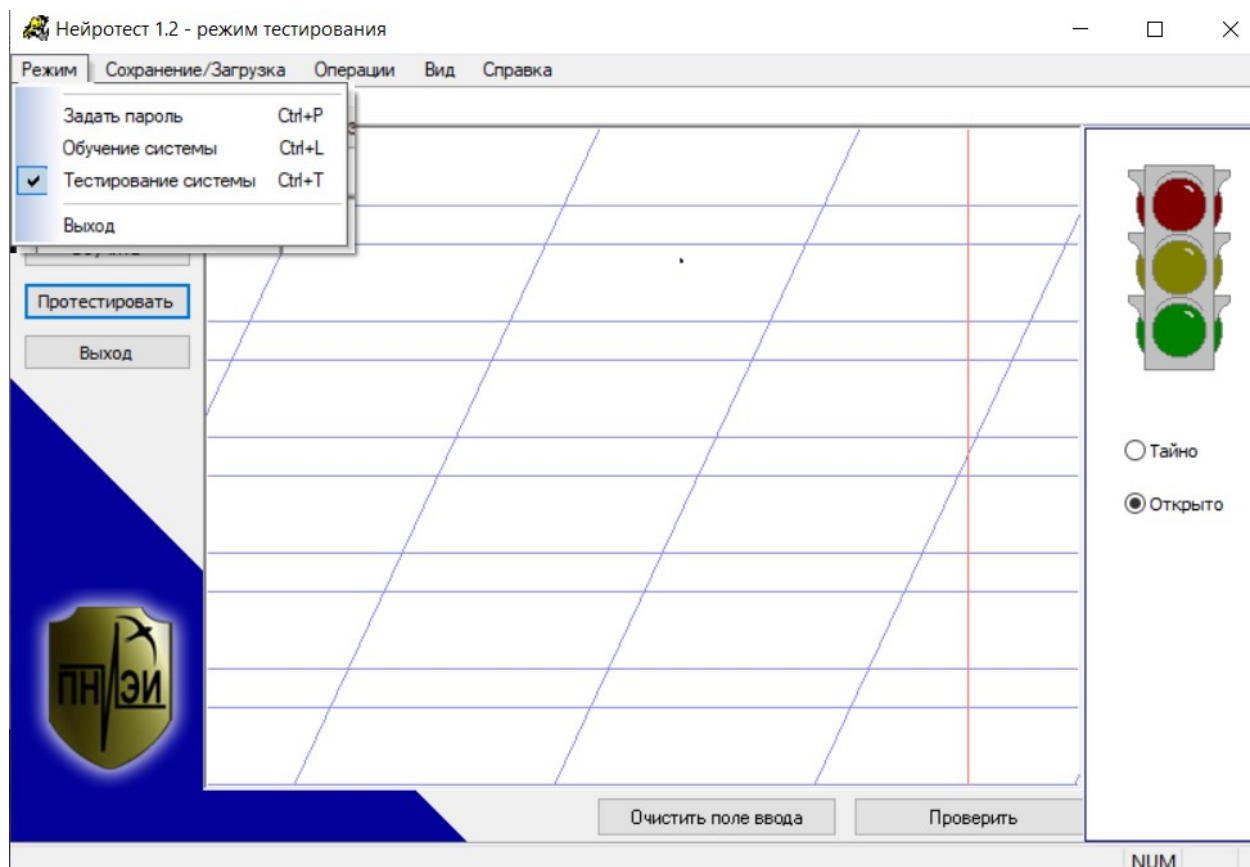


Рисунок 13 - Среда моделирования в режиме тестирования

При этом среда моделирования сформировала новый отчетный файл testKeys.txt, показанный на рисунке 14.

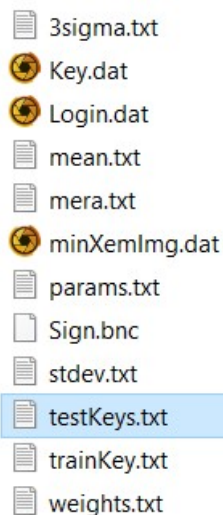


Рисунок 14 - Папка Data среды моделирования «БиоНейроАвтограф»

После чего был запущен корреляционный калькулятор. В начале была произведена проверка на автоматический поиск файла testKeys.txt с помощью

кнопки «Вычислить коэффициенты корреляции». Результат поиска показан на рисунке 15.

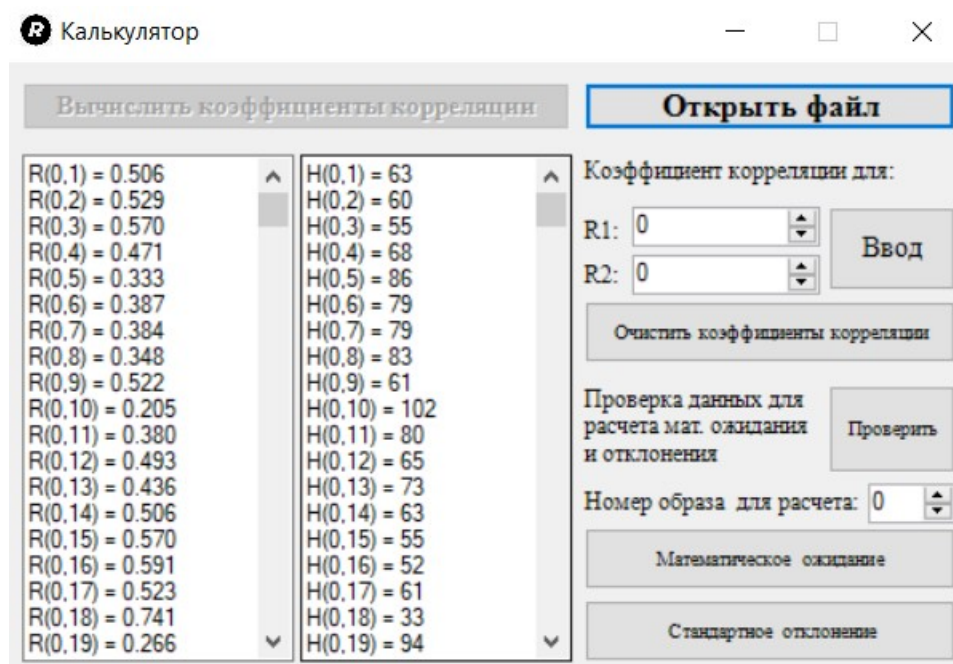


Рисунок 15 - Тестирование кнопки «Вычислить коэффициенты корреляции»

Как видно из рисунка кнопка «Вычислить коэффициенты корреляции» загорелась серым, это означает, что программа успешно нашла файл и обработала его. Так же это можно увидеть по результатам нахождения коэффициента корреляции и расстояний Хэмминга из скроллинга 1 и 2 из рисунка 15.

Далее файл testKeys.txt был перенесен из папки Data, в которой среда моделирования «БиоНейроАвтограф» создает отчетные файлы, в корневую папку программы, где расположен наш корреляционный калькулятор. После чего произведен повторный запуск кнопки «Вычислить коэффициенты корреляции». Результат работы представлен на рисунке 16.

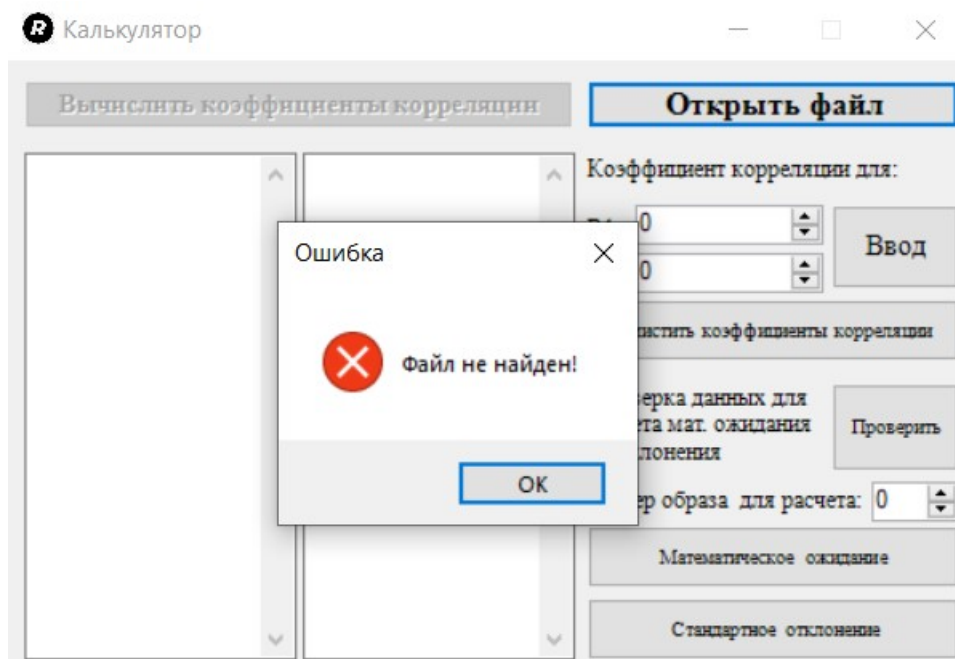


Рисунок 16 - Ошибка открытия файла

Как видно из рисунка корреляционный калькулятор не смог самостоятельно найти файл testKeys.txt. Для этого предусмотрена кнопка «Открыть файл» для ручного прописывания пути к нужному файлу. Результат показан на рисунке 17.

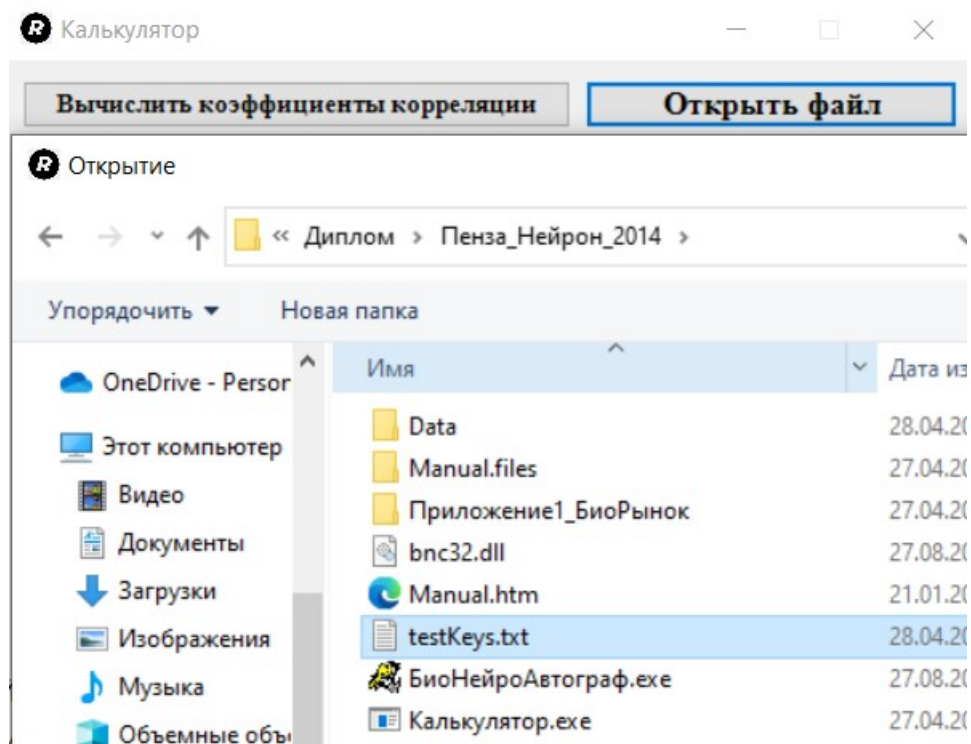


Рисунок 17- Ручного прописывание пути к нужному файлу

После успешного открытия файла нам показываю оповещение, представленное на рисунке 18.

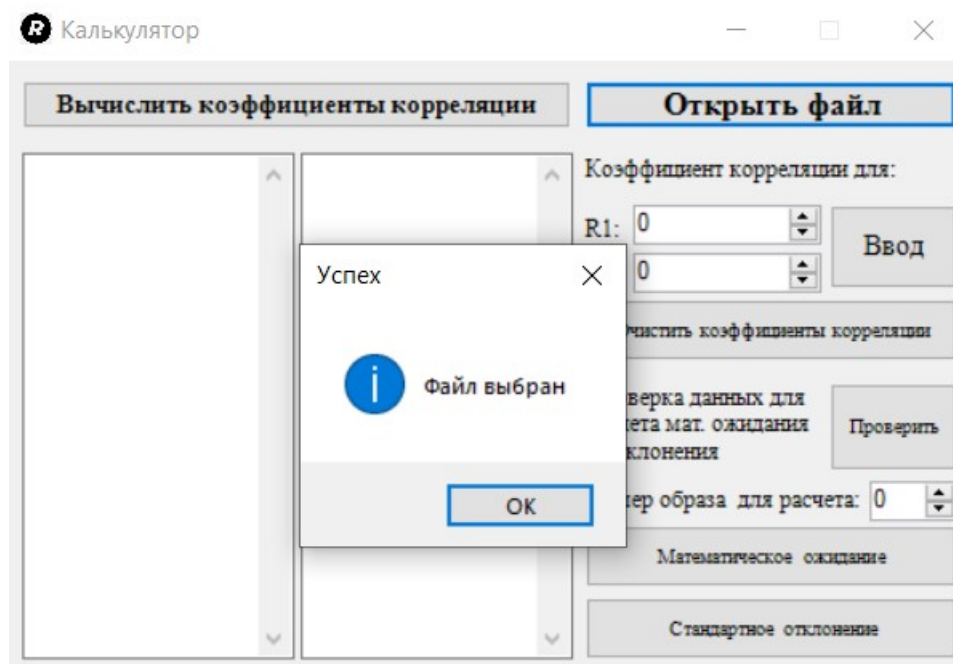


Рисунок 18 - Успешное открытие файла

Далее нам следует нажать кнопку «Вычислить коэффициенты корреляции» для расчета значений для каждого образа. При расчете корреляционный калькулятор создает для каждого образа отдельный файл с его бинарным ключом. Результат показан на рисунке 19.

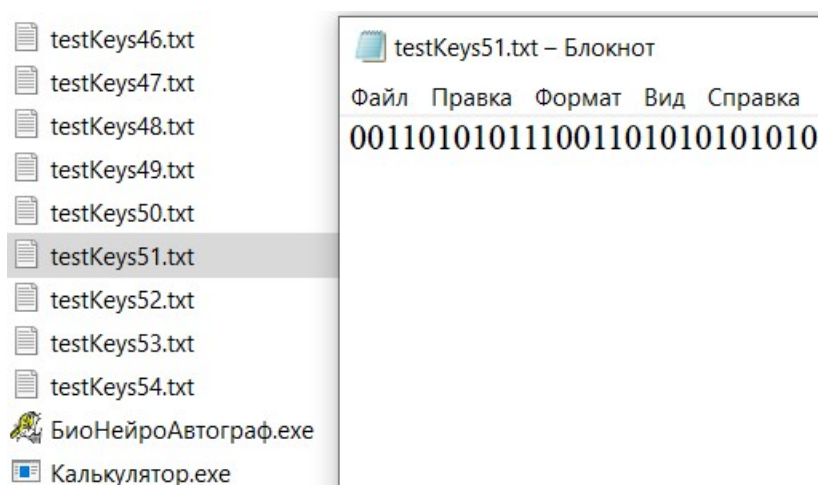


Рисунок 19 - Бинарный ключ

Так же калькулятор создает два файла, в одном расположены коэффициенты парной корреляции, в другом расстояния Хэмминга. Файл

testKeys_R.txt содержит коэффициенты парной корреляции, показанные на рисунке 20.

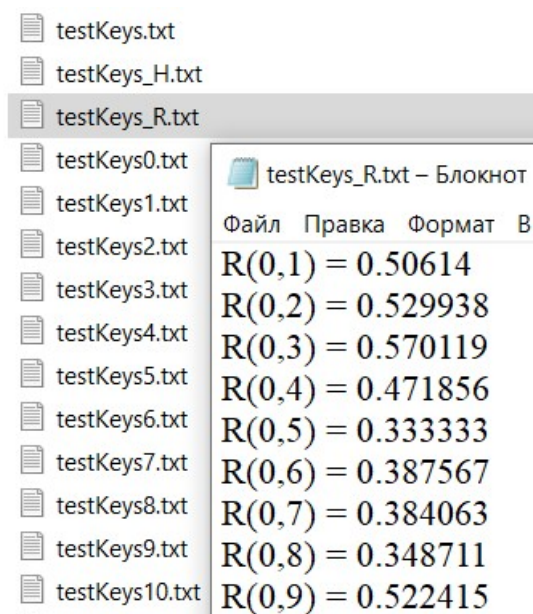


Рисунок 20 - Коэффициенты парной корреляции

Файл testKeys_H.txt содержит расстояния Хэмминга, показанные на рисунке 21.

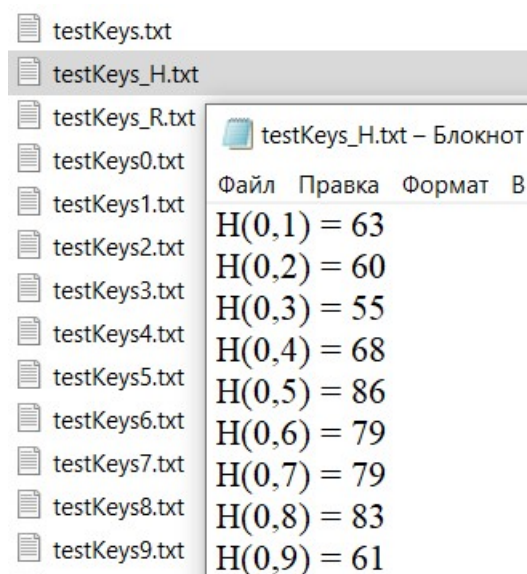


Рисунок 21 - Расстояния Хэмминга

Была произведена проверка нахождения коэффициента корреляции и расстояния Хэмминга между образами 3 и 6. Результат представлен на рисунке 22.

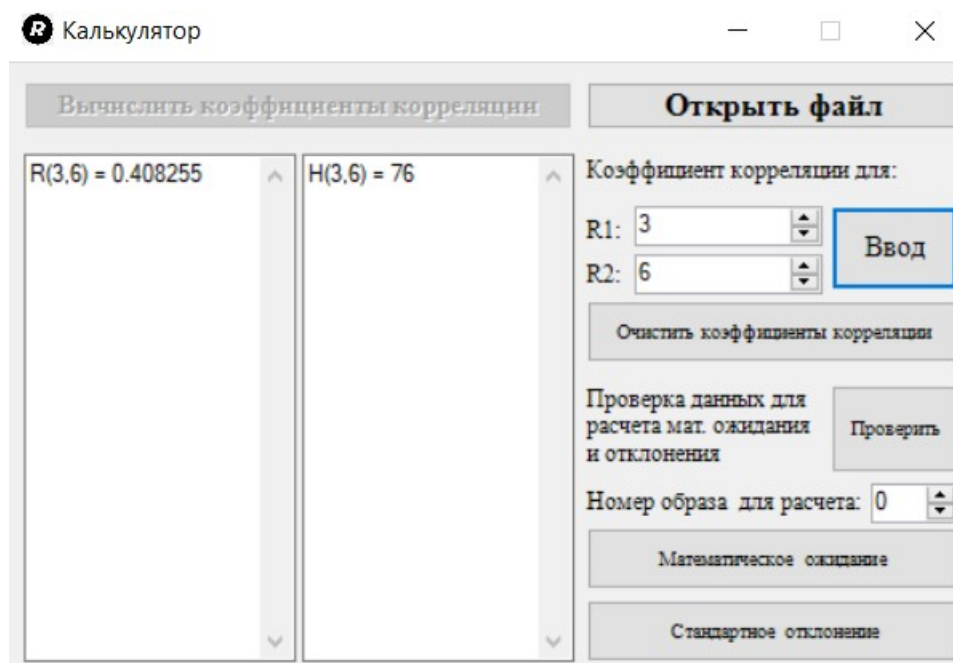


Рисунок 22 - Коэффициент корреляции и расстояние Хэмминга между образами 3 и 6

Прежде чем производить вычисления математического ожидания и стандартного отклонения была произведена проверка на дублирование данных с помощью нажатия на кнопку «Проверить». Результат представлен на рисунке 23.

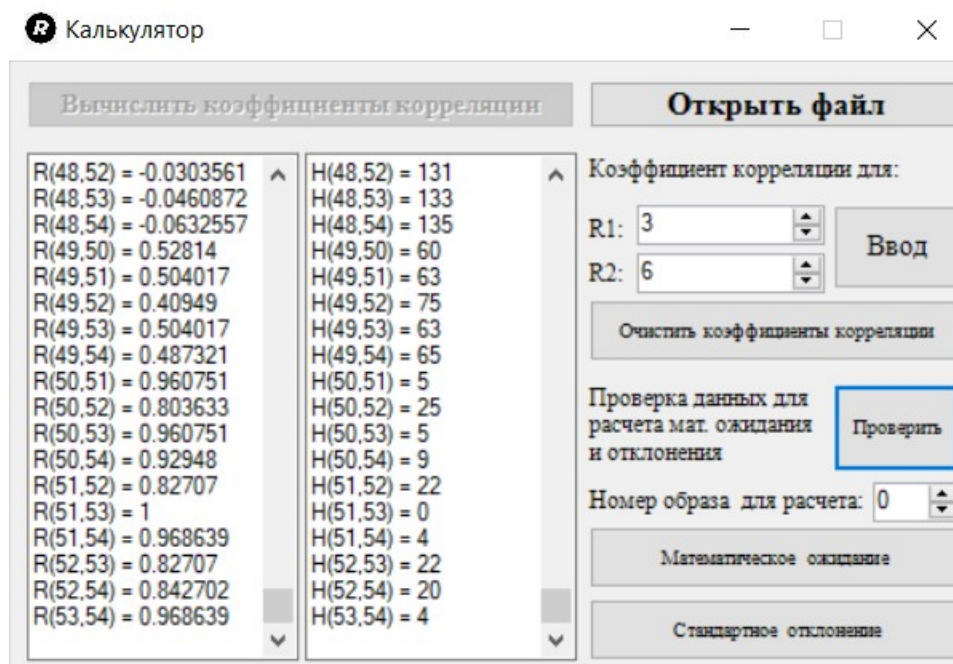


Рисунок 23 - Проверка данных на дублирование

После успешной проверки на дублирование был произведен расчет математического ожидания для образа 3, представленный на рисунке 24.

The screenshot shows a window titled "Калькулятор" (Calculator) with a standard Windows interface. The window is divided into several sections. On the left, there are two large text areas. The first area displays "M(3) = 0,212305" and the second area displays "M(3) = 101,000000". Above these areas is a button labeled "Вычислить коэффициенты корреляции". To the right of these areas is a section titled "Открыть файл". Below this, there are input fields for "R1:" (value 3) and "R2:" (value 6), followed by a "Ввод" (Input) button. Below the input fields is a button labeled "Очистить коэффициенты корреляции". Further down is a section titled "Проверка данных для расчета мат. ожидания и отклонения" with a "Проверить" (Check) button. Below this is a label "Номер образа для расчета:" followed by a dropdown menu showing the value 3. At the bottom, there are two buttons: "Математическое ожидание" (Mathematical expectation) and "Стандартное отклонение" (Standard deviation). The "Математическое ожидание" button is highlighted with a blue border.

Рисунок 24 - Математическое ожидание

Затем была произведен расчет стандартного отклонения для образа 3, представленный на рисунке 25.

The screenshot shows the same "Калькулятор" (Calculator) window as in Figure 24. The left text areas now display "с(3) = 0,286744" and "с(3) = 36,760920". The "Математическое ожидание" button is no longer highlighted, and the "Стандартное отклонение" (Standard deviation) button is highlighted with a blue border. All other elements, including the "Открыть файл" section, input fields, and buttons, remain the same as in the previous screenshot.

Рисунок 25 - Стандартное отклонение

После работы была произведена очистка всех созданных файлов калькулятора с помощью кнопки «Очистить коэффициенты корреляции». Результат очистки представлен на рисунке 26.

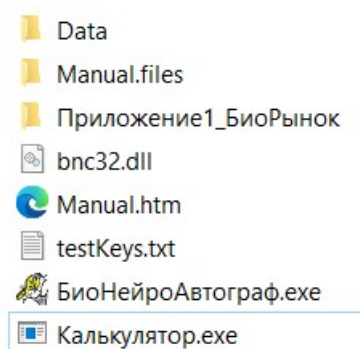


Рисунок 26 - Результат после очистки коэффициентов корреляции

На основе произведенного тестирования было установлена, что программа работает корректно. Недочетов в работе калькулятора установлено не было.

4 Разработка руководства пользователя

Информация о программе:

Корреляционный калькулятор – программное средство, позволяющее обрабатывать длинный символьные пароли среды моделирования «БиоНейроАвтограф» и рассчитывать коэффициенты парной корреляции, расстояния Хэмминга, математическое ожидание и стандартное отклонение для каждого образа.

Преимущество данного корреляционного калькулятора является возможность обработки отчетных файлов среды моделирования «БиоНейроАвтограф». Так как отчетный файл testKeys.txt специфичен и не читается обычными средствами автоматизации вычислений, его приходилось редактировать и обрабатывать данные в ручную, что приводила к большим затратам времени и возможностью допустить ошибки, которые давали бы недостоверную оценку.

Системные требования:

Данная программа работает на всех платформах семейства Windows.

Объем программы: 227 КБ.

Данная программа может быть скопированная в любую папку, но для автоматического нахождения отчетных файлов ее следует скопировать в папку с БиоНейроАвтограф.exe.

Экранная форма:

Экранная форма корреляционного калькулятора представлена на рисунке 27.

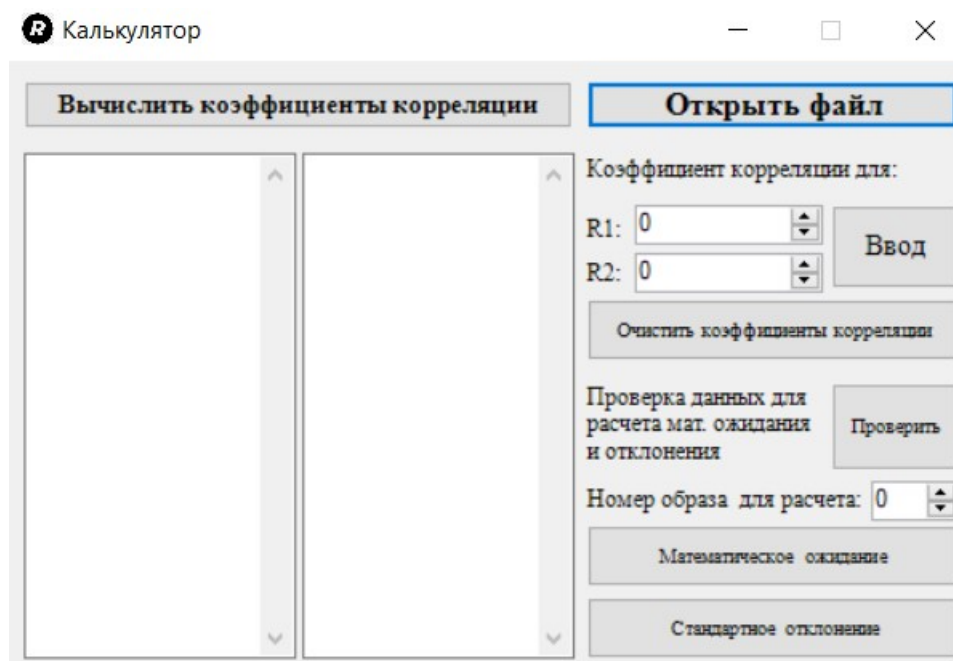


Рисунок 27 - Экранная форма корреляционного калькулятора

Кнопка «Вычислить коэффициенты корреляции» вычисляет коэффициенты парной корреляции и выводит полученные значения на скроллинг.

Кнопка «Открыть файл» открывает выбранный файл пользователем.

Кнопка «Ввод» выводит на скроллинг значения коэффициентов парной корреляции для выбранных образов пользователем.

Кнопка «Проверить» служит для вывода на экран всех коэффициентов парной корреляции.

Кнопка «Математическое ожидание» рассчитывает математическое ожидание для выбранного образа.

Кнопка «Стандартное отклонение» рассчитывает стандартное отклонение для выбранного образа.

Кнопка «Очистить коэффициенты корреляции» служит для удаления коэффициентов корреляции, математических ожиданий и стандартных отклонений.

Левый скроллинг выводит математические вычисления, включающие в себя работы с коэффициентами корреляции.

Правый скроллинг выводит математические вычисления, включающие в себя робы с расстояниями Хэмминга.

Удаление программы:

Для удаления корреляционного калькулятора необходимо удалить все созданные файлы (testKeys1-256.txt, testKeys_R.txt, testKeys_H.txt). Удаление можно выполнить самостоятельно, с помощью перехода в рабочую папку калькулятора, или автоматически, с помощью кнопки «Очистить коэффициенты корреляции».

5 Разработка рекомендаций для проведения практикума

Каждый студент выполняет практику по «Оценки энтропии кодов откликов нейросети на примере рукописного образа «Чужой» в пространстве корреляционных связей между разрядами» на персональном компьютере с установленной операционной системой Windows 7 и выше.

На выполнение данной практической работы должно быть выделено не более двух академических часов.

Перед началом выполнения практической работы студент должен освоить общие положения обучения искусственных нейросетевых сетей.

Пример выполнения практической работы:

Так как среда моделирования записывает все образы в один отчетный файл testKeys.txt, перед началом работы нужно удалить этот файл. Данный файл будет находиться в папке Data\<Имя пользователя>, как показано на рисунке 28.

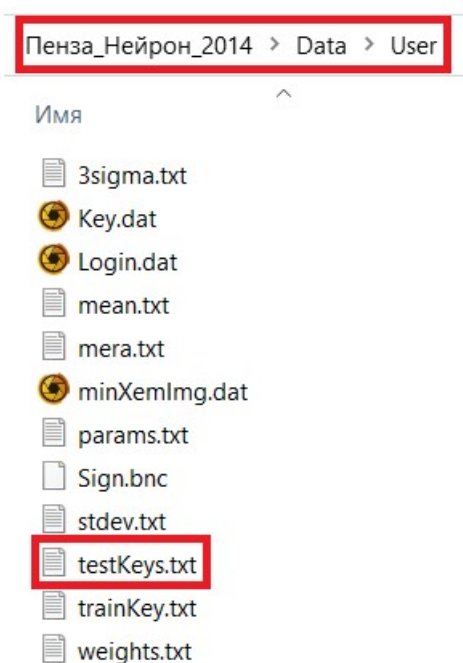


Рисунок 28 - Рабочая папка

Затем запустите среду моделирование «БиоНейроАвтограф» и задайте пароль. В поле «Пользователь» ввести свою фамилию либо имя (для

автоматического нахождения отчетного файла указать User), как показано на рисунке 29.

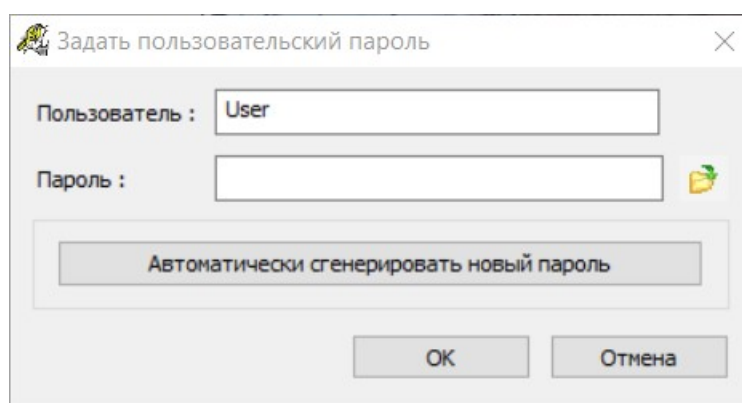


Рисунок 29 - Пользовательский пароль

После создания пароля следует обучить систему. За обучение системы отвечает кнопка «Обучить» в окне программы. В появившемся диалоговом окне необходимо ввести нужное количество образов символа по варианту задания. Диалоговое окно представлено на рисунке 30.

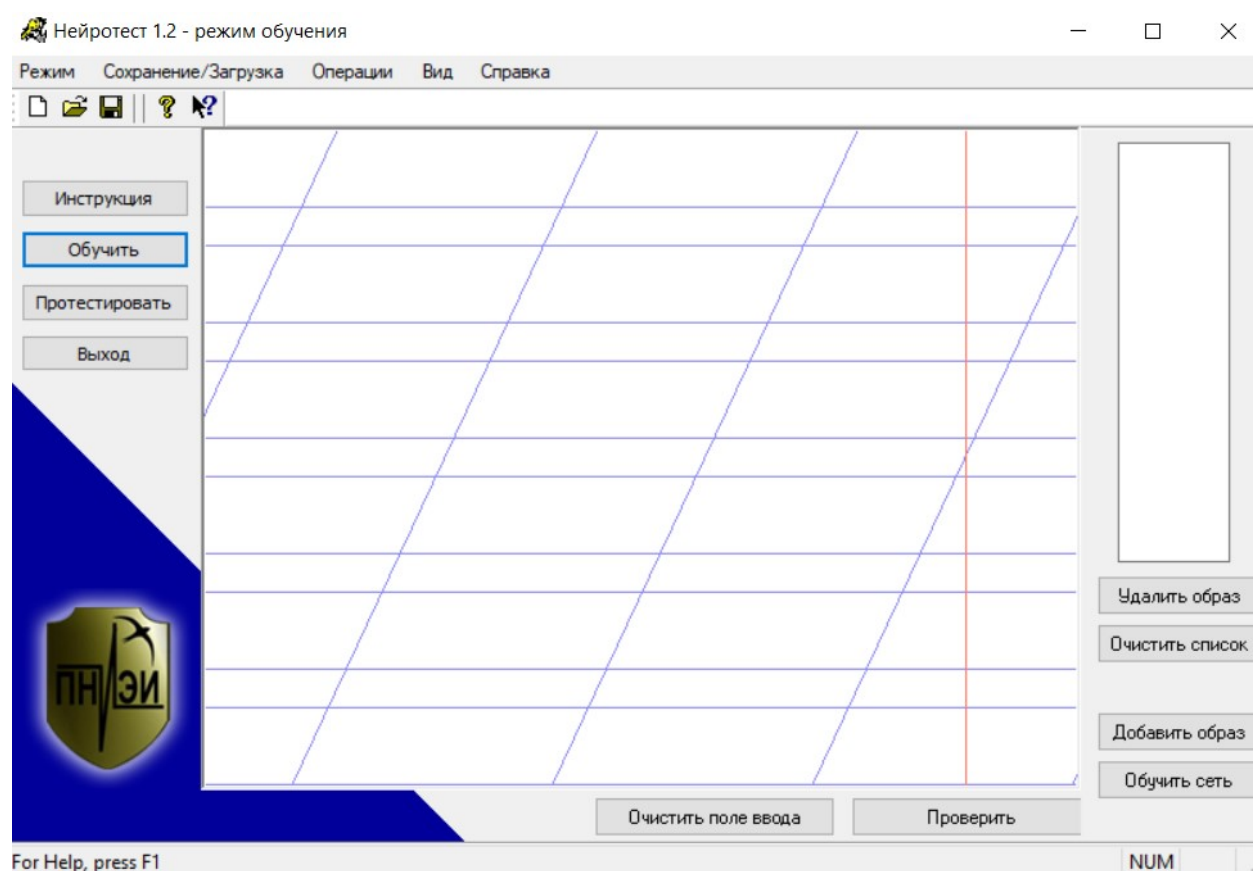


Рисунок 30 - Диалоговое окно режима обучения

Затем перейдите в тестовый режим «Протестировать» для примеров одного образа «Чужой». Для этого нужно перейти в «Режим», а затем нажать «Тестирование системы», либо с помощью клавиш CTRL+T, как показано на рисунке 31.

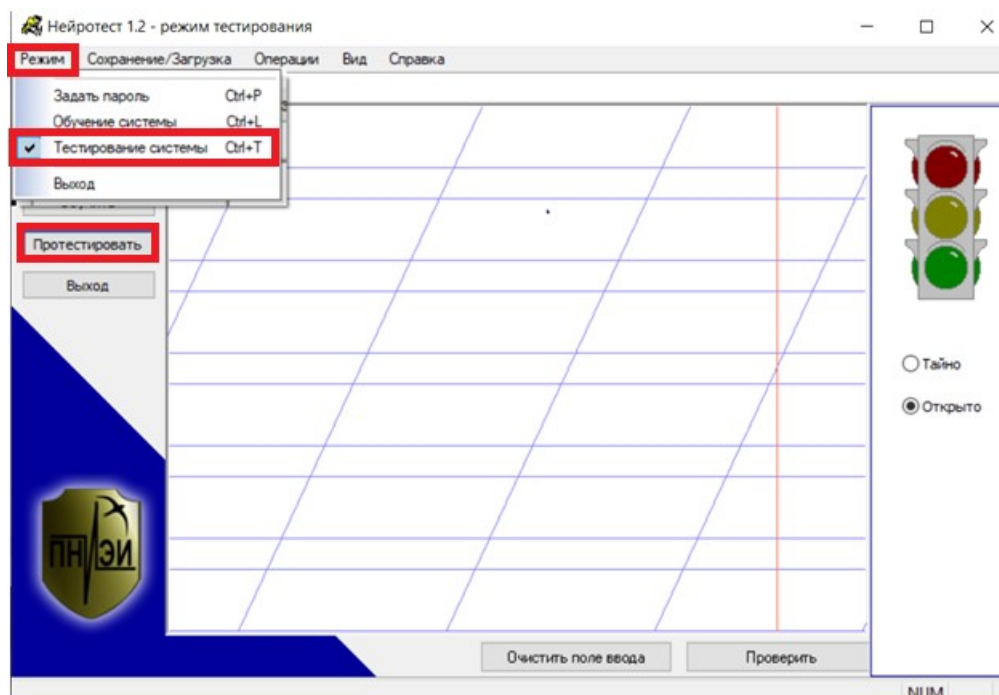


Рисунок 31 - Режим тестирования среды моделирования «БиоНейроАвтограф»

После чего произвести ввод нужного количества одного образа «Чужой». Убедиться, что файл testKeys.txt успешно создан.

Далее запустить файл Калькулятор.exe и выполнить нахождение коэффициентов парной корреляции с помощью кнопки «Вычислить коэффициенты корреляции», как показано на рисунке 32.

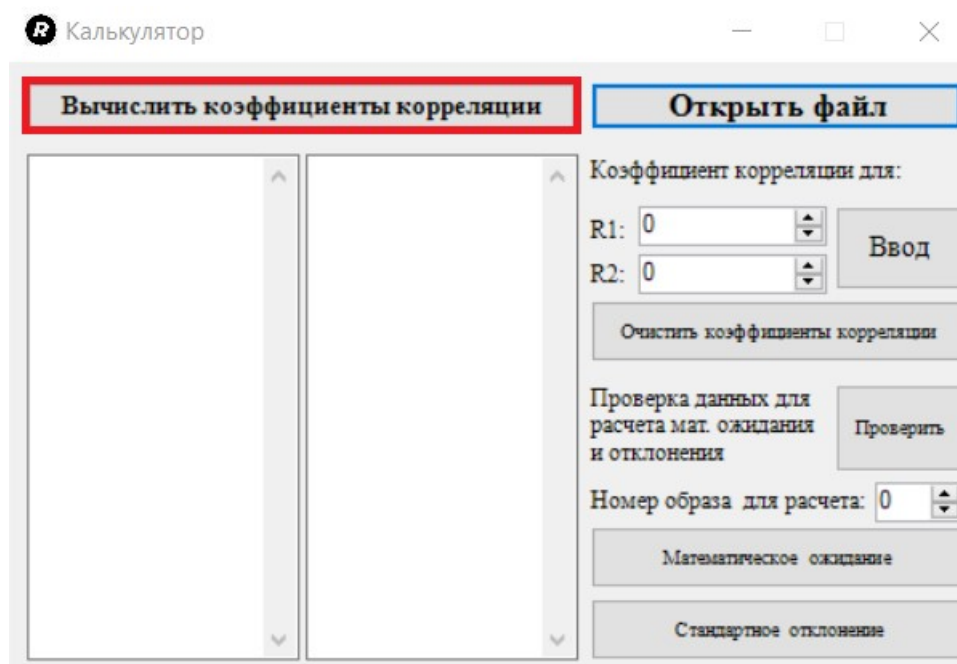


Рисунок 32 - Нахождение коэффициентов парной корреляции с помощью кнопки «Вычислить коэффициенты корреляции»

Если калькулятор выдал ошибку «Файл не найден», то следует открыть его самостоятельно с помощью кнопки «Открыть файл» из рисунка 33.

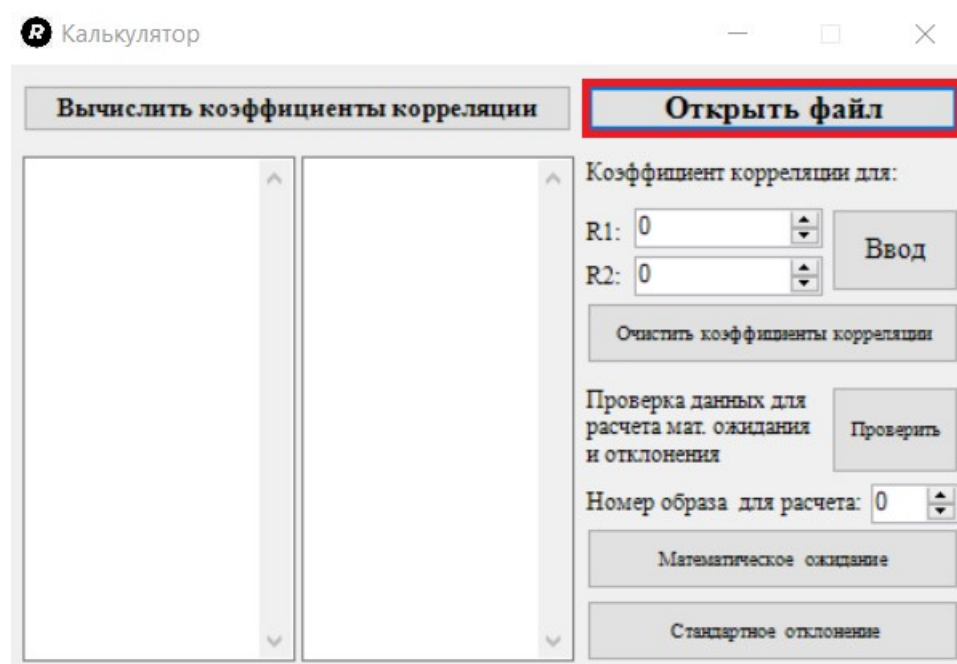


Рисунок 33 - Прописывания пути к файлу

После успешного нахождения коэффициентов парной корреляции вычислите математическое ожидание и стандартное отклонения для нужного

образа из варианта задания. Это можно сделать с помощью ввода нужного образа в колонку «Номер образа для расчета», показанного на рисунке 34.

Рисунок 34 - Номер образа для расчета

Далее запустите Mathcad и вычислите ошибку 2 рода с помощью формулы (5).

$$P = \frac{1}{\sigma \sqrt{2 \cdot \pi}} \int_{-\infty}^1 \exp \left(\frac{-(u-E)^2}{2 \cdot \sigma^2} \right) du, \quad (5)$$

где P – ошибка второго рода;

E – математическое ожидание;

σ – стандартное отклонение.

Затем с помощью формулы (6) находим энтропию.

$$-\log_2(P) \quad (6)$$

В качестве примера был взят образ 3 со значениями $E=0,212305$, $\sigma=0,285400$. Результаты вычисления калькулятора представлены на рисунках 35 – 36.

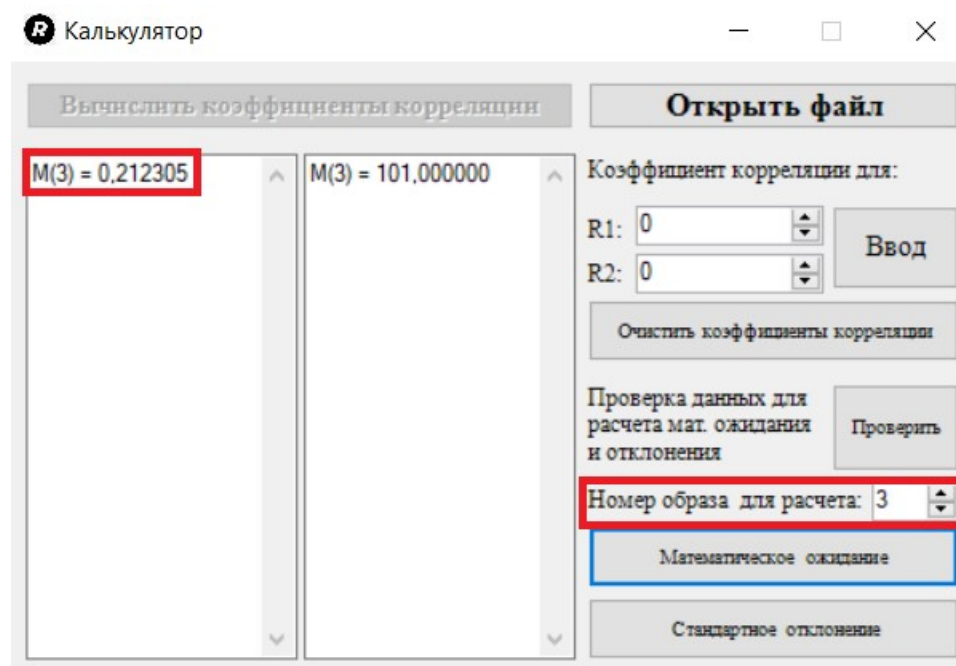


Рисунок 35 - Результат вычисления математического ожидания

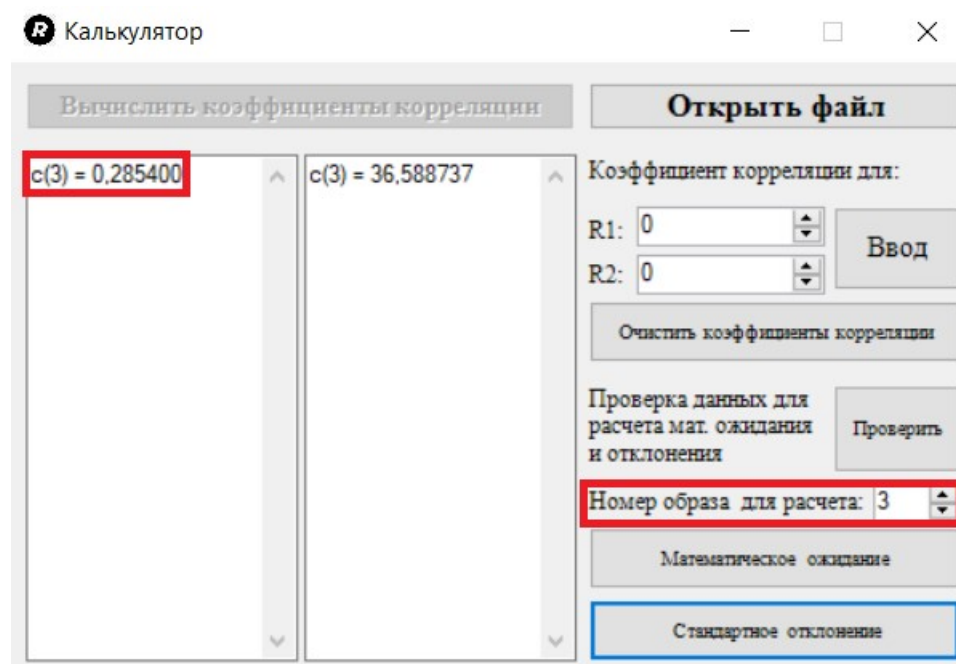


Рисунок 36 - Результат вычисления стандартного отклонения

Полученные значения были присвоены переменным и введены формулы (5) и (6). Результат показан на рисунке 37.

$$\begin{aligned}
 c &:= .285400 \\
 E &:= .212305 \\
 p &:= \frac{1}{c \cdot \sqrt{2 \cdot \pi}} \cdot \int_{-\infty}^1 \exp\left(\frac{-(x-E)^2}{2 \cdot c^2}\right) dx = 0.997 \\
 -\log(p, 2) &= 0.004
 \end{aligned}$$

Рисунок 37 - Результаты расчета в Mathcad

На основе полученных результатов делается вывод о стойкости к атакам подбора и оформляется отчет о проделанной работе.

Пример отчета о проделанной работе должен выглядеть следующем образом:

1. Была скопирована папка «Пенза Нейрон 2014» на рабочий стол компьютера.
2. После открытия папки был произведен запуск «БиоНейроАвтографа». Появилось диалоговое окно, представленное на рисунке 38.

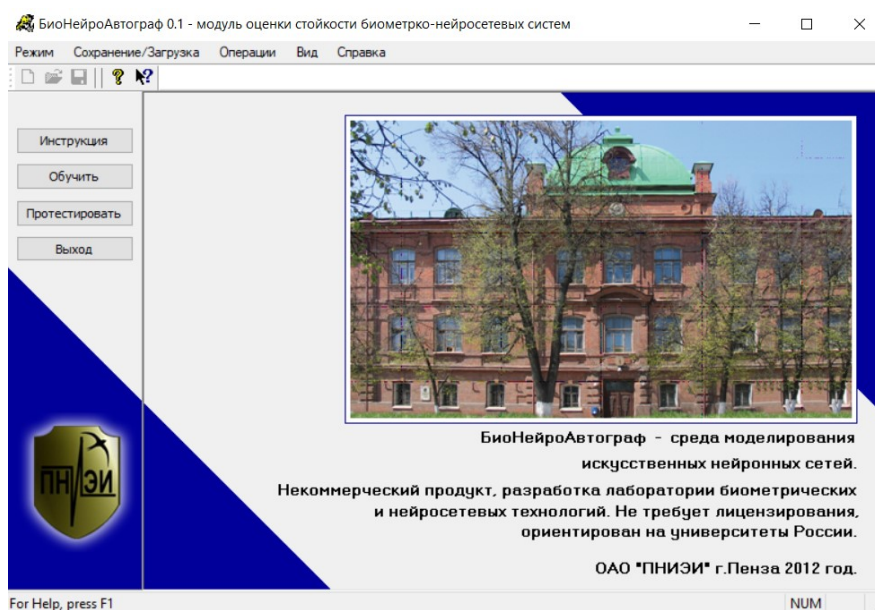


Рисунок 38 - Диалоговое окно программы «БиоНейроАвтограф»

3. После чего в меню пуск был выбран «Режим», представленный на рисунке 39.

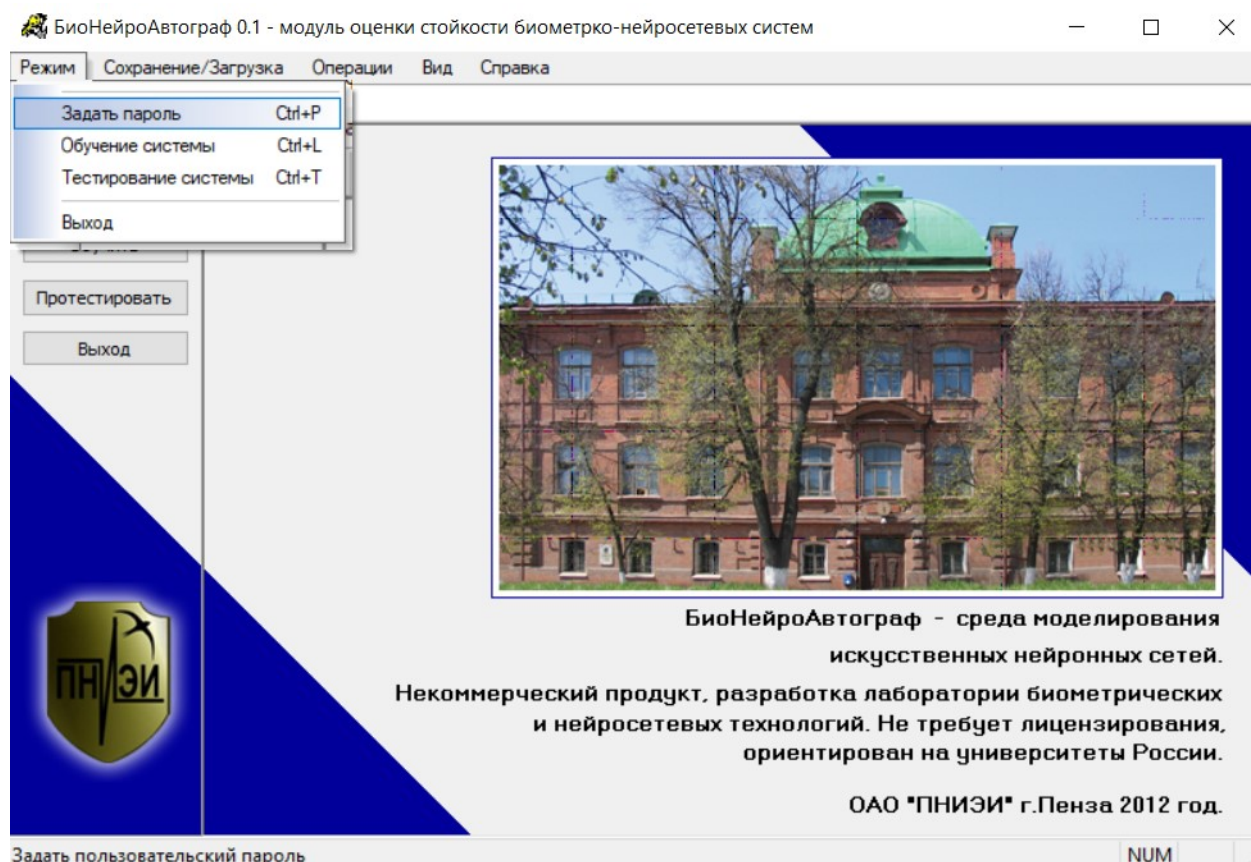


Рисунок 39 - Пункт меню «Режим»

4. После чего было выбрано «Задать пароль»
5. В появившейся форме было введено имя пользователя User, представленное на рисунке 40.

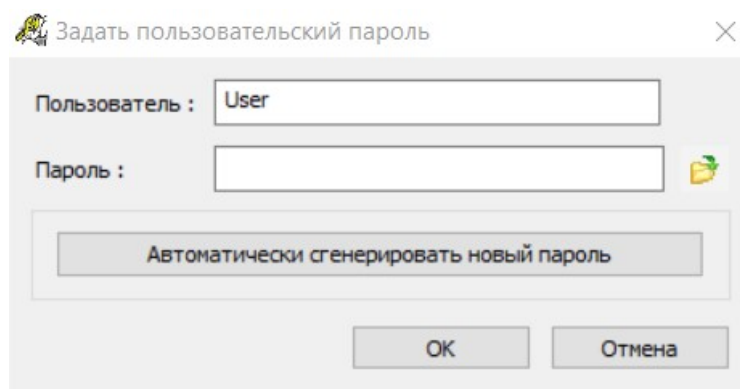


Рисунок 40 - Создание нового пользователя

6. Далее была заполнена графа «Пароль». После успешного заполнения была нажата клавиша «ОК».

7. В появившемся диалоговом окне была нажата клавиша «ДА». Диалоговое окно представлено на рисунке 41.

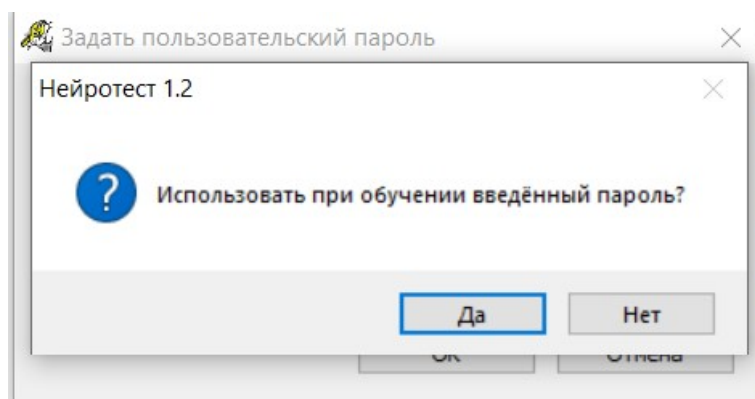


Рисунок 41 - Диалоговое окно

8. После успешного сохранения пользовательских данных появилось сообщение, представленное на рисунке 42.

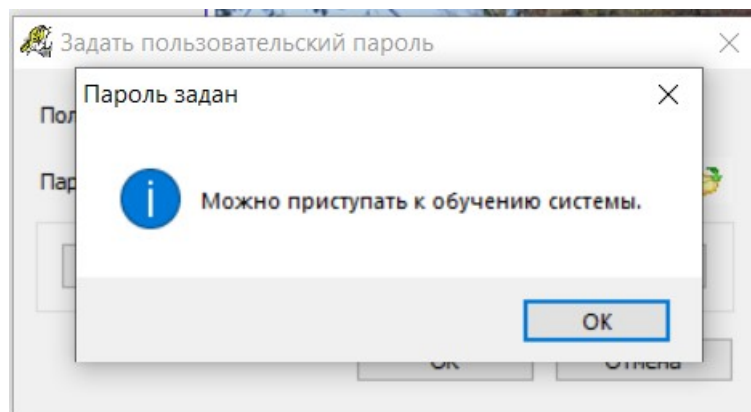


Рисунок 42 - Сообщение

9. После успешного создания пользователя была нажата кнопка «Обучить».

10. В поле ввода был введен рукописный символ «а». После того как символ был введен была нажата кнопка «Добавить образ». Обучение системы представлено на рисунке 43.

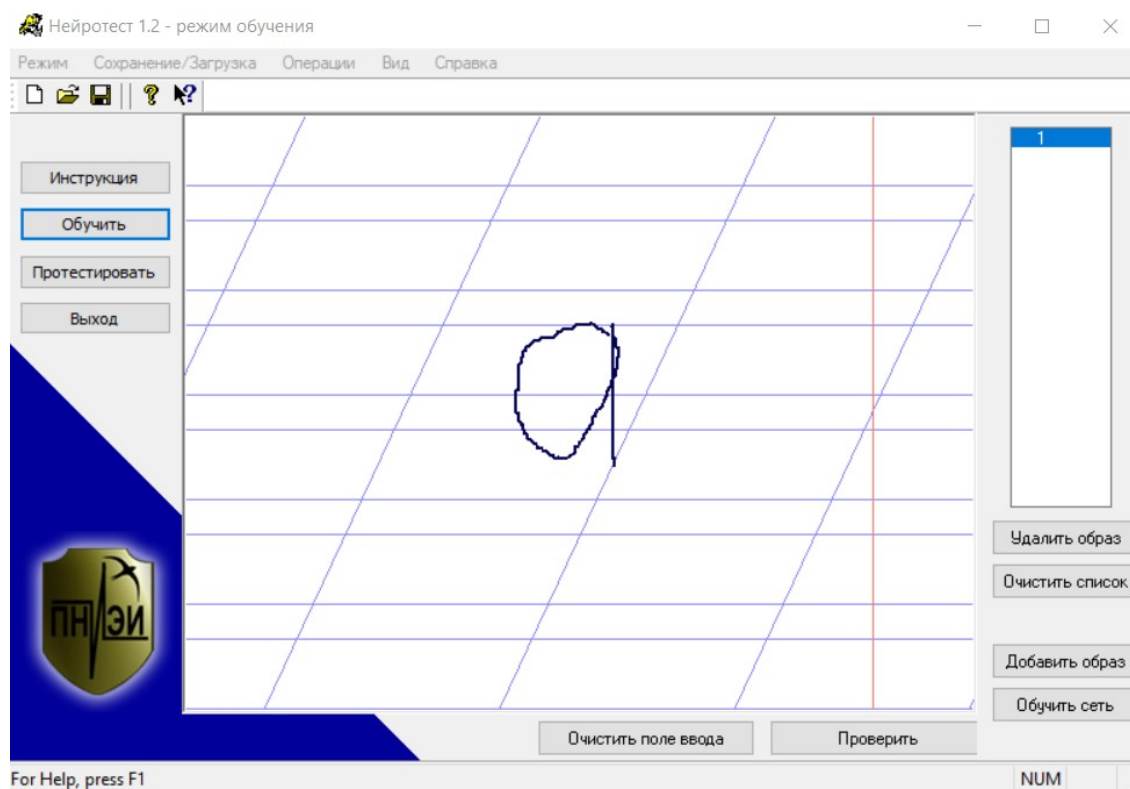


Рисунок 43 - Обучение системы

11. После чего было добавлено 8 образов рукописного символа «а». Результат представлен на рисунке 44.

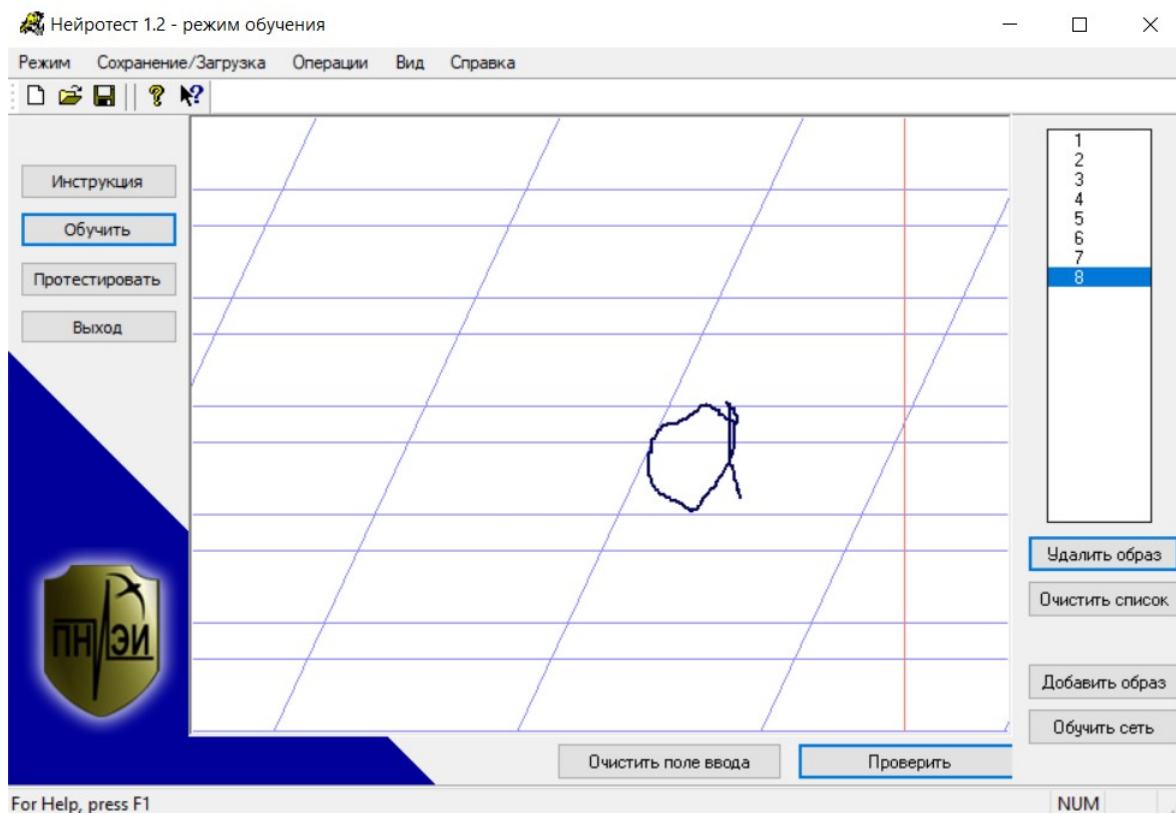


Рисунок 44 - Результат добавления образов символа «а»

12. После ввода достаточного количества примером была нажата кнопка «Обучить сеть». После обучения сети появилось диалоговое окно с результатом обучения, представленное на рисунке 45.

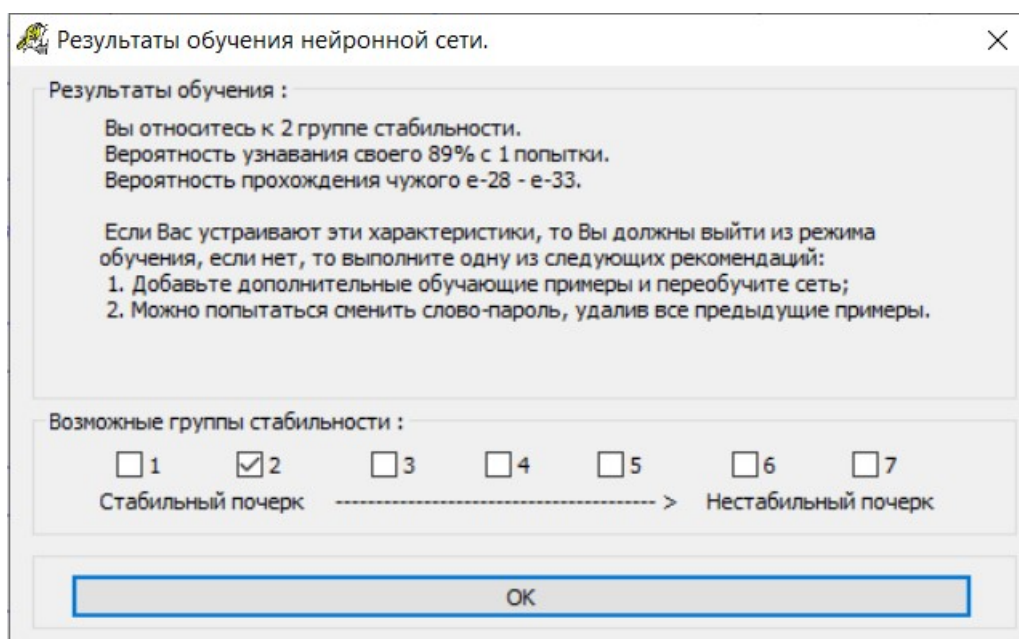


Рисунок 45 - Результат обучения

13. После чего была произведена проверка качества обучения. Для проверка качества был введен контрольный рукописный образ «а» и нажата кнопка «Проверить». Результат проверки представлен на рисунке 46.

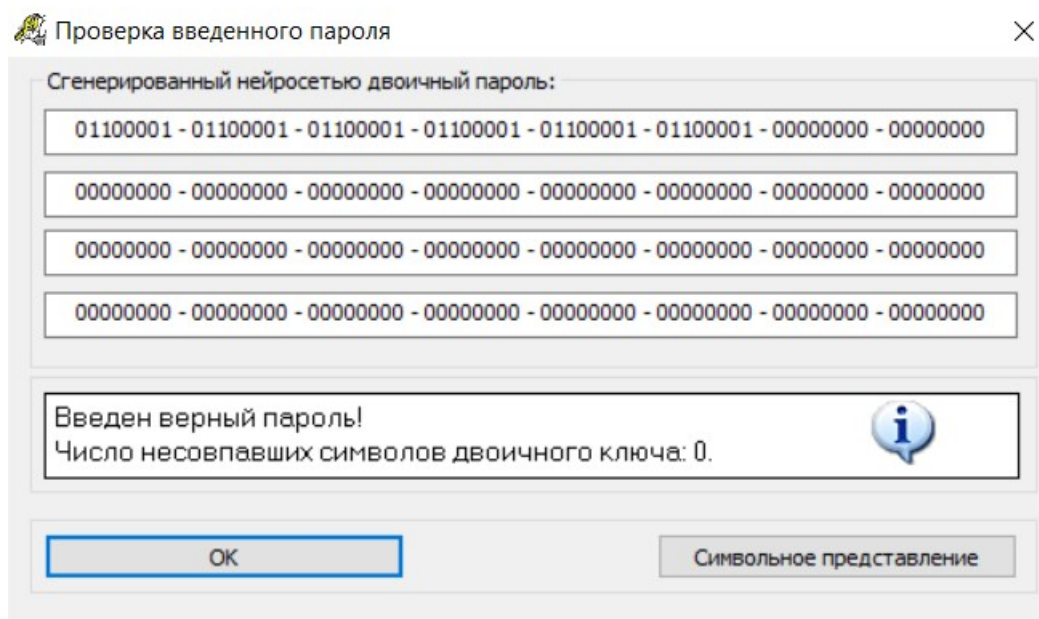


Рисунок 46 - Результат проверки качества обучения

14. После чего перешли в режим тестирования, нажав кнопку «Протестировать». Далее мы произвели проверку с распознаванием в образе «Чужой» образ «Свой» введя 50 раз символ «в». Ни одна проверка не прошла, результат представлен на рисунке 47.

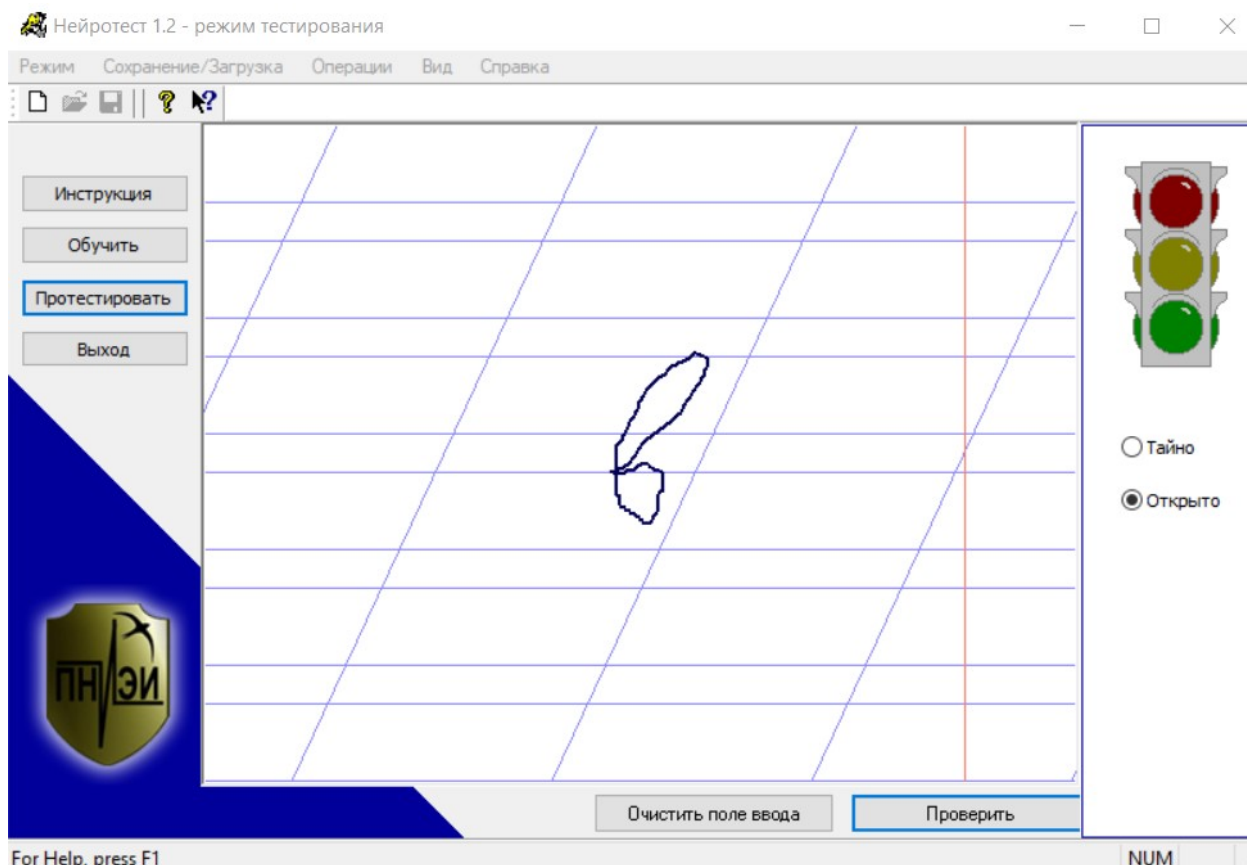


Рисунок 47 - Проверка

15. После чего был произведен запуск программы «Калькулятор».

16. В появившейся экранной форме с помощью кнопки «Открыть файл» был выбран отчетный файл testKeys.txt, находящийся в Data\User\testKeys.txt. Результат представлен на рисунке 48.

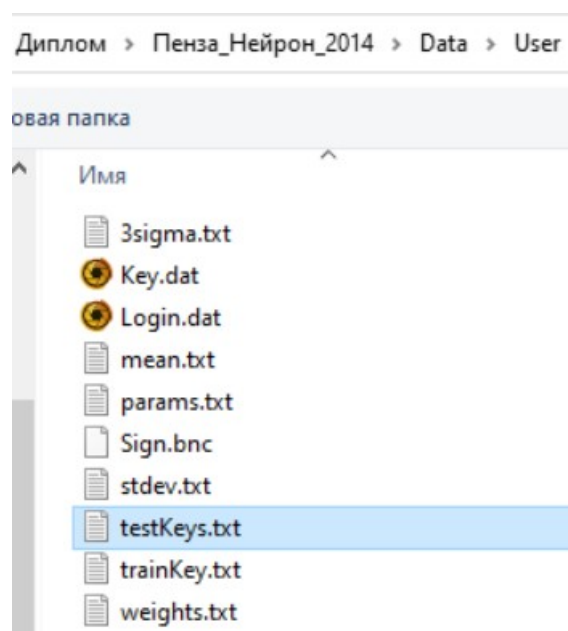


Рисунок 48 - Путь к файлу testKeys.txt

17. После чего был произведен расчет коэффициентов корреляции с помощью кнопки «Вычислить коэффициенты корреляции». Результат вычисления представлен в таблице 3.

Таблица 3 – Полученные результаты

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(0,1)	-0.494	192	R(0,22)	-0.412	182	R(0,43)	-0.487	191
R(0,2)	-0.492	192	R(0,23)	-0.461	188	R(0,44)	-0.469	189
R(0,3)	-0.358	175	R(0,24)	-0.388	179	R(0,45)	-0.530	197
R(0,4)	-0.422	183	R(0,25)	-0.594	205	R(0,46)	-0.322	170
R(0,5)	-0.376	177	R(0,26)	-0.483	191	R(0,47)	-0.452	187
R(0,6)	-0.394	179	R(0,27)	-0.427	184	R(0,48)	-0.268	163
R(0,7)	-0.245	159	R(0,28)	-0.506	194	R(0,49)	-0.376	177
R(0,8)	-0.343	173	R(0,29)	-0.522	196	R(1,2)	0.842	20
R(0,9)	-0.268	162	R(0,30)	-0.476	190	R(1,3)	0.707	37
R(0,10)	-0.429	184	R(0,31)	-0.461	188	R(1,4)	0.802	25
R(0,11)	-0.436	185	R(0,32)	-0.464	188	R(1,5)	0.692	39
R(0,12)	-0.468	189	R(0,33)	-0.390	179	R(1,6)	0.662	43
R(0,13)	-0.427	184	R(0,34)	-0.299	166	R(1,7)	0.527	61
R(0,14)	-0.373	177	R(0,35)	-0.547	199	R(1,8)	0.755	31
R(0,15)	-0.392	178	R(0,36)	-0.501	193	R(1,9)	0.519	62
R(0,16)	-0.422	183	R(0,37)	-0.368	176	R(1,10)	0.810	24
R(0,17)	-0.522	196	R(0,38)	-0.205	155	R(1,11)	0.881	15
R(0,18)	-0.579	203	R(0,39)	-0.385	178	R(1,12)	0.865	17
R(0,19)	-0.455	187	R(0,40)	-0.397	180	R(1,13)	0.874	16
R(0,20)	-0.364	175	R(0,41)	-0.508	194	R(1,14)	0.849	19
R(0,21)	-0.408	181	R(0,42)	-0.430	184	R(1,15)	0.596	52

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(1,16)	0.834	21	R(2,13)	0.840	20	R(3,11)	0.730	34
R(1,17)	0.795	26	R(2,14)	0.769	29	R(3,12)	0.746	32
R(1,18)	0.802	25	R(2,15)	0.629	48	R(3,13)	0.738	33
R(1,19)	0.881	15	R(2,16)	0.802	25	R(3,14)	0.762	30
R(1,20)	0.647	45	R(2,17)	0.840	20	R(3,15)	0.730	35
R(1,21)	0.724	35	R(2,18)	0.833	21	R(3,16)	0.762	30
R(1,22)	0.857	18	R(2,19)	0.818	23	R(3,17)	0.706	37
R(1,23)	0.826	22	R(2,20)	0.680	41	R(3,18)	0.667	42
R(1,24)	0.754	31	R(2,21)	0.772	29	R(3,19)	0.779	28
R(1,25)	0.787	27	R(2,22)	0.840	20	R(3,20)	0.765	30
R(1,26)	0.802	25	R(2,23)	0.857	18	R(3,21)	0.827	22
R(1,27)	0.842	20	R(2,24)	0.753	31	R(3,22)	0.802	25
R(1,28)	0.827	22	R(2,25)	0.752	31	R(3,23)	0.707	37
R(1,29)	0.842	20	R(2,26)	0.832	21	R(3,24)	0.794	26
R(1,30)	0.826	22	R(2,27)	0.808	24	R(3,25)	0.603	50
R(1,31)	0.921	10	R(2,28)	0.872	16	R(3,26)	0.778	28
R(1,32)	0.858	18	R(2,29)	0.888	14	R(3,27)	0.754	31
R(1,33)	0.786	27	R(2,30)	0.888	14	R(3,28)	0.770	29
R(1,34)	0.660	44	R(2,31)	0.841	20	R(3,29)	0.722	35
R(1,35)	0.834	21	R(2,32)	0.796	26	R(3,30)	0.817	23
R(1,36)	0.865	17	R(2,33)	0.786	27	R(3,31)	0.723	35
R(1,37)	0.779	28	R(2,34)	0.615	50	R(3,32)	0.677	41
R(1,38)	0.615	49	R(2,35)	0.832	21	R(3,33)	0.778	28
R(1,39)	0.717	36	R(2,36)	0.849	19	R(3,34)	0.794	27
R(1,40)	0.747	32	R(2,37)	0.763	30	R(3,35)	0.730	34
R(1,41)	0.873	16	R(2,38)	0.615	49	R(3,36)	0.715	36
R(1,42)	0.794	26	R(2,39)	0.733	34	R(3,37)	0.834	21
R(1,43)	0.740	33	R(2,40)	0.793	26	R(3,38)	0.796	26
R(1,44)	0.723	35	R(2,41)	0.825	22	R(3,39)	0.819	23
R(1,45)	0.723	35	R(2,42)	0.857	18	R(3,40)	0.770	29
R(1,46)	0.685	40	R(2,43)	0.740	33	R(3,41)	0.754	31
R(1,47)	0.802	25	R(2,44)	0.738	33	R(3,42)	0.786	27
R(1,48)	0.662	43	R(2,45)	0.784	27	R(3,43)	0.795	26
R(1,49)	0.660	43	R(2,46)	0.717	36	R(3,44)	0.778	28
R(2,3)	0.770	29	R(2,47)	0.880	15	R(3,45)	0.635	46
R(2,4)	0.881	15	R(2,48)	0.662	43	R(3,46)	0.851	19
R(2,5)	0.771	29	R(2,49)	0.676	41	R(3,47)	0.778	28
R(2,6)	0.678	41	R(3,4)	0.857	18	R(3,48)	0.780	28
R(2,7)	0.577	55	R(3,5)	0.842	20	R(3,49)	0.794	26
R(2,8)	0.738	33	R(3,6)	0.780	28	R(4,5)	0.810	24
R(2,9)	0.552	58	R(3,7)	0.772	30	R(4,6)	0.717	36
R(2,10)	0.841	20	R(3,8)	0.826	22	R(4,7)	0.677	42
R(2,11)	0.816	23	R(3,9)	0.716	37	R(4,8)	0.826	22
R(2,12)	0.833	21	R(3,10)	0.849	19	R(4,9)	0.606	51

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(4,10)	0.865	17	R(5,10)	0.802	25	R(6,11)	0.655	44
R(4,11)	0.825	22	R(5,11)	0.731	34	R(6,12)	0.670	42
R(4,12)	0.825	22	R(5,12)	0.715	36	R(6,13)	0.679	41
R(4,13)	0.817	23	R(5,13)	0.771	29	R(6,14)	0.717	36
R(4,14)	0.778	28	R(5,14)	0.763	30	R(6,15)	0.821	23
R(4,15)	0.698	39	R(5,15)	0.650	45	R(6,16)	0.670	42
R(4,16)	0.826	22	R(5,16)	0.763	30	R(6,17)	0.632	47
R(4,17)	0.786	27	R(5,17)	0.724	35	R(6,18)	0.591	52
R(4,18)	0.778	28	R(5,18)	0.652	44	R(6,19)	0.685	40
R(4,19)	0.858	18	R(5,19)	0.732	34	R(6,20)	0.874	16
R(4,20)	0.718	36	R(5,20)	0.749	32	R(6,21)	0.780	28
R(4,21)	0.827	22	R(5,21)	0.811	24	R(6,22)	0.726	35
R(4,22)	0.865	17	R(5,22)	0.787	27	R(6,23)	0.631	47
R(4,23)	0.833	21	R(5,23)	0.739	33	R(6,24)	0.702	38
R(4,24)	0.794	26	R(5,24)	0.747	32	R(6,25)	0.561	56
R(4,25)	0.714	36	R(5,25)	0.620	48	R(6,26)	0.671	42
R(4,26)	0.841	20	R(5,26)	0.763	30	R(6,27)	0.679	41
R(4,27)	0.833	21	R(5,27)	0.739	33	R(6,28)	0.696	39
R(4,28)	0.850	19	R(5,28)	0.740	33	R(6,29)	0.648	45
R(4,29)	0.834	21	R(5,29)	0.724	35	R(6,30)	0.726	35
R(4,30)	0.881	15	R(5,30)	0.771	29	R(6,31)	0.646	45
R(4,31)	0.818	23	R(5,31)	0.707	37	R(6,32)	0.584	53
R(4,32)	0.788	27	R(5,32)	0.677	41	R(6,33)	0.670	42
R(4,33)	0.826	22	R(5,33)	0.747	32	R(6,34)	0.791	27
R(4,34)	0.700	39	R(5,34)	0.746	33	R(6,35)	0.671	42
R(4,35)	0.825	22	R(5,35)	0.731	34	R(6,36)	0.638	46
R(4,36)	0.826	22	R(5,36)	0.684	40	R(6,37)	0.741	33
R(4,37)	0.818	23	R(5,37)	0.787	27	R(6,38)	0.701	38
R(4,38)	0.701	38	R(5,38)	0.733	34	R(6,39)	0.819	23
R(4,39)	0.788	27	R(5,39)	0.803	25	R(6,40)	0.725	35
R(4,40)	0.849	19	R(5,40)	0.802	25	R(6,41)	0.678	41
R(4,41)	0.849	19	R(5,41)	0.739	33	R(6,42)	0.709	37
R(4,42)	0.865	17	R(5,42)	0.834	21	R(6,43)	0.827	22
R(4,43)	0.779	28	R(5,43)	0.748	32	R(6,44)	0.796	26
R(4,44)	0.778	28	R(5,44)	0.747	32	R(6,45)	0.592	52
R(4,45)	0.730	34	R(5,45)	0.700	38	R(6,46)	0.788	27
R(4,46)	0.788	27	R(5,46)	0.835	21	R(6,47)	0.686	40
R(4,47)	0.873	16	R(5,47)	0.794	26	R(6,48)	0.764	30
R(4,48)	0.717	36	R(5,48)	0.764	30	R(6,49)	0.843	20
R(4,49)	0.715	36	R(5,49)	0.763	30	R(7,8)	0.724	36
R(5,6)	0.764	30	R(6,7)	0.783	28	R(7,9)	0.835	21
R(5,7)	0.660	44	R(6,8)	0.717	36	R(7,10)	0.686	41
R(5,8)	0.794	26	R(6,9)	0.822	23	R(7,11)	0.554	58
R(5,9)	0.667	43	R(6,10)	0.788	27	R(7,12)	0.568	56

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(7,13)	0.563	57	R(8,16)	0.778	28	R(9,20)	0.759	31
R(7,14)	0.631	48	R(8,17)	0.674	41	R(9,21)	0.682	41
R(7,15)	0.804	25	R(8,18)	0.651	44	R(9,22)	0.584	54
R(7,16)	0.599	52	R(8,19)	0.779	28	R(9,23)	0.488	66
R(7,17)	0.533	61	R(8,20)	0.750	32	R(9,24)	0.624	49
R(7,18)	0.505	64	R(8,21)	0.811	24	R(9,25)	0.389	79
R(7,19)	0.597	52	R(8,22)	0.817	23	R(9,26)	0.529	61
R(7,20)	0.814	24	R(8,23)	0.707	37	R(9,27)	0.585	54
R(7,21)	0.722	36	R(8,24)	0.825	22	R(9,28)	0.541	60
R(7,22)	0.624	49	R(8,25)	0.603	50	R(9,29)	0.492	66
R(7,23)	0.513	63	R(8,26)	0.746	32	R(9,30)	0.600	52
R(7,24)	0.649	46	R(8,27)	0.802	25	R(9,31)	0.520	62
R(7,25)	0.446	72	R(8,28)	0.722	35	R(9,32)	0.470	68
R(7,26)	0.617	50	R(8,29)	0.706	37	R(9,33)	0.621	49
R(7,27)	0.594	53	R(8,30)	0.770	29	R(9,34)	0.796	26
R(7,28)	0.598	53	R(8,31)	0.754	31	R(9,35)	0.529	61
R(7,29)	0.549	59	R(8,32)	0.709	37	R(9,36)	0.527	61
R(7,30)	0.656	45	R(8,33)	0.841	20	R(9,37)	0.690	40
R(7,31)	0.560	57	R(8,34)	0.826	23	R(9,38)	0.759	31
R(7,32)	0.510	63	R(8,35)	0.730	34	R(9,39)	0.674	42
R(7,33)	0.662	44	R(8,36)	0.746	32	R(9,40)	0.567	56
R(7,34)	0.773	29	R(8,37)	0.866	17	R(9,41)	0.537	60
R(7,35)	0.554	58	R(8,38)	0.827	22	R(9,42)	0.581	54
R(7,36)	0.567	56	R(8,39)	0.788	27	R(9,43)	0.666	43
R(7,37)	0.699	39	R(8,40)	0.754	31	R(9,44)	0.653	45
R(7,38)	0.815	24	R(8,41)	0.770	29	R(9,45)	0.437	73
R(7,39)	0.698	39	R(8,42)	0.786	27	R(9,46)	0.799	26
R(7,40)	0.623	49	R(8,43)	0.716	36	R(9,47)	0.544	59
R(7,41)	0.593	53	R(8,44)	0.731	34	R(9,48)	0.744	33
R(7,42)	0.606	51	R(8,45)	0.603	50	R(9,49)	0.777	29
R(7,43)	0.706	38	R(8,46)	0.851	19	R(10,11)	0.785	27
R(7,44)	0.693	40	R(8,47)	0.762	30	R(10,12)	0.754	31
R(7,45)	0.478	68	R(8,48)	0.812	24	R(10,13)	0.793	26
R(7,46)	0.760	31	R(8,49)	0.794	26	R(10,14)	0.833	21
R(7,47)	0.600	52	R(9,10)	0.677	42	R(10,15)	0.722	36
R(7,48)	0.721	36	R(9,11)	0.529	61	R(10,16)	0.802	25
R(7,49)	0.739	34	R(9,12)	0.512	63	R(10,17)	0.761	30
R(8,9)	0.700	39	R(9,13)	0.538	60	R(10,18)	0.722	35
R(8,10)	0.802	25	R(9,14)	0.623	49	R(10,19)	0.850	19
R(8,11)	0.762	30	R(9,15)	0.734	34	R(10,20)	0.774	29
R(8,12)	0.762	30	R(9,16)	0.543	59	R(10,21)	0.819	23
R(8,13)	0.770	29	R(9,17)	0.476	68	R(10,22)	0.825	22
R(8,14)	0.825	22	R(9,18)	0.449	71	R(10,23)	0.778	28
R(8,15)	0.620	49	R(9,19)	0.557	57	R(10,24)	0.817	23

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(10,25)	0.674	41	R(11,31)	0.912	11	R(12,38)	0.623	48
R(10,26)	0.785	27	R(11,32)	0.852	19	R(12,39)	0.741	33
R(10,27)	0.793	26	R(11,33)	0.857	18	R(12,40)	0.770	29
R(10,28)	0.778	28	R(11,34)	0.656	45	R(12,41)	0.880	15
R(10,29)	0.761	30	R(11,35)	0.872	16	R(12,42)	0.834	21
R(10,30)	0.873	16	R(11,36)	0.905	12	R(12,43)	0.764	30
R(10,31)	0.794	26	R(11,37)	0.756	31	R(12,44)	0.730	34
R(10,32)	0.701	38	R(11,38)	0.623	48	R(12,45)	0.745	32
R(10,33)	0.738	33	R(11,39)	0.725	35	R(12,46)	0.693	39
R(10,34)	0.756	32	R(11,40)	0.785	27	R(12,47)	0.857	18
R(10,35)	0.769	29	R(11,41)	0.896	13	R(12,48)	0.670	42
R(10,36)	0.786	27	R(11,42)	0.850	19	R(12,49)	0.668	42
R(10,37)	0.810	24	R(11,43)	0.780	28	R(13,14)	0.817	23
R(10,38)	0.709	37	R(11,44)	0.698	38	R(13,15)	0.583	54
R(10,39)	0.796	26	R(11,45)	0.760	30	R(13,16)	0.833	21
R(10,40)	0.809	24	R(11,46)	0.694	39	R(13,17)	0.791	26
R(10,41)	0.825	22	R(11,47)	0.841	20	R(13,18)	0.817	23
R(10,42)	0.841	20	R(11,48)	0.686	40	R(13,19)	0.882	15
R(10,43)	0.771	29	R(11,49)	0.668	42	R(13,20)	0.665	43
R(10,44)	0.770	29	R(12,13)	0.896	13	R(13,21)	0.709	37
R(10,45)	0.674	41	R(12,14)	0.777	28	R(13,22)	0.920	10
R(10,46)	0.843	20	R(12,15)	0.621	49	R(13,23)	0.841	20
R(10,47)	0.833	21	R(12,16)	0.825	22	R(13,24)	0.832	21
R(10,48)	0.741	33	R(12,17)	0.833	21	R(13,25)	0.767	29
R(10,49)	0.771	29	R(12,18)	0.841	20	R(13,26)	0.784	27
R(11,12)	0.872	16	R(12,19)	0.842	20	R(13,27)	0.888	14
R(11,13)	0.928	9	R(12,20)	0.687	40	R(13,28)	0.839	20
R(11,14)	0.825	22	R(12,21)	0.716	36	R(13,29)	0.871	16
R(11,15)	0.590	53	R(12,22)	0.896	13	R(13,30)	0.808	24
R(11,16)	0.889	14	R(12,23)	0.849	19	R(13,31)	0.905	12
R(11,17)	0.832	21	R(12,24)	0.777	28	R(13,32)	0.828	22
R(11,18)	0.825	22	R(12,25)	0.793	26	R(13,33)	0.881	15
R(11,19)	0.890	14	R(12,26)	0.809	24	R(13,34)	0.664	44
R(11,20)	0.656	44	R(12,27)	0.848	19	R(13,35)	0.832	21
R(11,21)	0.732	34	R(12,28)	0.865	17	R(13,36)	0.881	15
R(11,22)	0.896	13	R(12,29)	0.881	15	R(13,37)	0.764	30
R(11,23)	0.849	19	R(12,30)	0.817	23	R(13,38)	0.631	47
R(11,24)	0.840	20	R(12,31)	0.912	11	R(13,39)	0.749	32
R(11,25)	0.760	30	R(12,32)	0.819	23	R(13,40)	0.777	28
R(11,26)	0.840	20	R(12,33)	0.873	16	R(13,41)	0.872	16
R(11,27)	0.928	9	R(12,34)	0.638	47	R(13,42)	0.858	18
R(11,28)	0.880	15	R(12,35)	0.841	20	R(13,43)	0.741	33
R(11,29)	0.896	13	R(12,36)	0.857	18	R(13,44)	0.674	41
R(11,30)	0.816	23	R(12,37)	0.771	29	R(13,45)	0.735	33

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(13,46)	0.702	38	R(15,21)	0.728	35	R(16,32)	0.819	23
R(13,47)	0.864	17	R(15,22)	0.629	48	R(16,33)	0.794	26
R(13,48)	0.695	39	R(15,23)	0.581	54	R(16,34)	0.653	45
R(13,49)	0.676	41	R(15,24)	0.606	51	R(16,35)	0.857	18
R(14,15)	0.636	47	R(15,25)	0.514	63	R(16,36)	0.841	20
R(14,16)	0.794	26	R(15,26)	0.669	43	R(16,37)	0.771	29
R(14,17)	0.705	37	R(15,27)	0.599	52	R(16,38)	0.670	42
R(14,18)	0.698	38	R(15,28)	0.649	46	R(16,39)	0.788	27
R(14,19)	0.826	22	R(15,29)	0.600	52	R(16,40)	0.849	19
R(14,20)	0.719	36	R(15,30)	0.724	36	R(16,41)	0.865	17
R(14,21)	0.764	30	R(15,31)	0.612	50	R(16,42)	0.881	15
R(14,22)	0.833	21	R(15,32)	0.532	60	R(16,43)	0.779	28
R(14,23)	0.738	33	R(15,33)	0.588	53	R(16,44)	0.762	30
R(14,24)	0.809	24	R(15,34)	0.687	40	R(16,45)	0.794	26
R(14,25)	0.665	42	R(15,35)	0.606	51	R(16,46)	0.725	35
R(14,26)	0.729	34	R(15,36)	0.588	53	R(16,47)	0.841	20
R(14,27)	0.833	21	R(15,37)	0.658	44	R(16,48)	0.733	34
R(14,28)	0.737	33	R(15,38)	0.664	43	R(16,49)	0.684	40
R(14,29)	0.737	33	R(15,39)	0.751	32	R(17,18)	0.865	17
R(14,30)	0.769	29	R(15,40)	0.691	40	R(17,19)	0.787	27
R(14,31)	0.817	23	R(15,41)	0.629	48	R(17,20)	0.681	41
R(14,32)	0.756	31	R(15,42)	0.643	46	R(17,21)	0.757	31
R(14,33)	0.778	28	R(15,43)	0.775	29	R(17,22)	0.776	28
R(14,34)	0.749	33	R(15,44)	0.761	31	R(17,23)	0.825	22
R(14,35)	0.745	32	R(15,45)	0.545	59	R(17,24)	0.720	35
R(14,36)	0.794	26	R(15,46)	0.688	40	R(17,25)	0.799	25
R(14,37)	0.803	25	R(15,47)	0.652	45	R(17,26)	0.896	13
R(14,38)	0.717	36	R(15,48)	0.664	43	R(17,27)	0.775	28
R(14,39)	0.756	31	R(15,49)	0.729	35	R(17,28)	0.903	12
R(14,40)	0.722	35	R(16,17)	0.866	17	R(17,29)	0.887	14
R(14,41)	0.817	23	R(16,18)	0.794	26	R(17,30)	0.840	20
R(14,42)	0.770	29	R(16,19)	0.858	18	R(17,31)	0.825	22
R(14,43)	0.716	36	R(16,20)	0.718	36	R(17,32)	0.798	26
R(14,44)	0.683	40	R(16,21)	0.811	24	R(17,33)	0.738	33
R(14,45)	0.617	48	R(16,22)	0.849	19	R(17,34)	0.539	60
R(14,46)	0.804	25	R(16,23)	0.833	21	R(17,35)	0.848	19
R(14,47)	0.761	30	R(16,24)	0.762	30	R(17,36)	0.818	23
R(14,48)	0.781	28	R(16,25)	0.730	34	R(17,37)	0.685	40
R(14,49)	0.747	32	R(16,26)	0.905	12	R(17,38)	0.537	59
R(15,16)	0.635	47	R(16,27)	0.849	19	R(17,39)	0.718	36
R(15,17)	0.600	52	R(16,28)	0.882	15	R(17,40)	0.825	22
R(15,18)	0.542	59	R(16,29)	0.850	19	R(17,41)	0.808	24
R(15,19)	0.634	47	R(16,30)	0.833	21	R(17,42)	0.826	22
R(15,20)	0.820	23	R(16,31)	0.865	17	R(17,43)	0.773	29

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(17,44)	0.770	29	R(19,27)	0.882	15	R(20,42)	0.757	31
R(17,45)	0.863	17	R(19,28)	0.836	21	R(20,43)	0.843	20
R(17,46)	0.655	44	R(19,29)	0.819	23	R(20,44)	0.860	18
R(17,47)	0.833	21	R(19,30)	0.850	19	R(20,45)	0.626	48
R(17,48)	0.616	49	R(19,31)	0.865	17	R(20,46)	0.788	27
R(17,49)	0.628	47	R(19,32)	0.803	25	R(20,47)	0.735	34
R(18,19)	0.763	30	R(19,33)	0.826	22	R(20,48)	0.796	26
R(18,20)	0.593	52	R(19,34)	0.714	37	R(20,49)	0.796	26
R(18,21)	0.653	44	R(19,35)	0.858	18	R(21,22)	0.772	29
R(18,22)	0.785	27	R(19,36)	0.889	14	R(21,23)	0.740	33
R(18,23)	0.833	21	R(19,37)	0.787	27	R(21,24)	0.732	34
R(18,24)	0.713	36	R(19,38)	0.654	44	R(21,25)	0.606	50
R(18,25)	0.857	18	R(19,39)	0.740	33	R(21,26)	0.812	24
R(18,26)	0.841	20	R(19,40)	0.771	29	R(21,27)	0.772	29
R(18,27)	0.785	27	R(19,41)	0.866	17	R(21,28)	0.774	29
R(18,28)	0.881	15	R(19,42)	0.802	25	R(21,29)	0.709	37
R(18,29)	0.912	11	R(19,43)	0.763	30	R(21,30)	0.788	27
R(18,30)	0.801	25	R(19,44)	0.700	38	R(21,31)	0.693	39
R(18,31)	0.849	19	R(19,45)	0.716	36	R(21,32)	0.662	43
R(18,32)	0.851	19	R(19,46)	0.740	33	R(21,33)	0.716	36
R(18,33)	0.762	30	R(19,47)	0.810	24	R(21,34)	0.745	33
R(18,34)	0.512	63	R(19,48)	0.717	36	R(21,35)	0.764	30
R(18,35)	0.856	18	R(19,49)	0.716	36	R(21,36)	0.716	36
R(18,36)	0.857	18	R(20,21)	0.843	20	R(21,37)	0.787	27
R(18,37)	0.676	41	R(20,22)	0.696	39	R(21,38)	0.717	36
R(18,38)	0.512	62	R(20,23)	0.663	43	R(21,39)	0.897	13
R(18,39)	0.646	45	R(20,24)	0.656	44	R(21,40)	0.850	19
R(18,40)	0.754	31	R(20,25)	0.563	56	R(21,41)	0.740	33
R(18,41)	0.864	17	R(20,26)	0.720	36	R(21,42)	0.787	27
R(18,42)	0.802	25	R(20,27)	0.665	43	R(21,43)	0.874	16
R(18,43)	0.716	36	R(20,28)	0.714	37	R(21,44)	0.874	16
R(18,44)	0.667	42	R(20,29)	0.650	45	R(21,45)	0.686	40
R(18,45)	0.777	28	R(20,30)	0.743	33	R(21,46)	0.803	25
R(18,46)	0.614	49	R(20,31)	0.648	45	R(21,47)	0.779	28
R(18,47)	0.793	26	R(20,32)	0.553	57	R(21,48)	0.827	22
R(18,48)	0.544	58	R(20,33)	0.687	40	R(21,49)	0.779	28
R(18,49)	0.589	52	R(20,34)	0.759	31	R(22,23)	0.809	24
R(19,20)	0.671	42	R(20,35)	0.688	40	R(22,24)	0.864	17
R(19,21)	0.779	28	R(20,36)	0.640	46	R(22,25)	0.720	35
R(19,22)	0.882	15	R(20,37)	0.773	29	R(22,26)	0.800	25
R(19,23)	0.786	27	R(20,38)	0.718	36	R(22,27)	0.888	14
R(19,24)	0.858	18	R(20,39)	0.835	21	R(22,28)	0.840	20
R(19,25)	0.732	34	R(20,40)	0.774	29	R(22,29)	0.856	18
R(19,26)	0.810	24	R(20,41)	0.680	41	R(22,30)	0.825	22

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(22,31)	0.873	16	R(23,49)	0.597	51	R(25,44)	0.650	44
R(22,32)	0.828	22	R(24,25)	0.632	46	R(25,45)	0.774	28
R(22,33)	0.897	13	R(24,26)	0.744	32	R(25,46)	0.552	57
R(22,34)	0.710	38	R(24,27)	0.880	15	R(25,47)	0.761	30
R(22,35)	0.848	19	R(24,28)	0.768	29	R(25,48)	0.465	68
R(22,36)	0.881	15	R(24,29)	0.768	29	R(25,49)	0.509	62
R(22,37)	0.827	22	R(24,30)	0.785	27	R(26,27)	0.800	25
R(22,38)	0.694	39	R(24,31)	0.801	25	R(26,28)	0.928	9
R(22,39)	0.796	26	R(24,32)	0.773	29	R(26,29)	0.880	15
R(22,40)	0.777	28	R(24,33)	0.857	18	R(26,30)	0.880	15
R(22,41)	0.904	12	R(24,34)	0.766	31	R(26,31)	0.833	21
R(22,42)	0.857	18	R(24,35)	0.792	26	R(26,32)	0.836	21
R(22,43)	0.772	29	R(24,36)	0.857	18	R(26,33)	0.762	30
R(22,44)	0.691	39	R(24,37)	0.756	31	R(26,34)	0.624	49
R(22,45)	0.720	35	R(24,38)	0.702	38	R(26,35)	0.872	16
R(22,46)	0.764	30	R(24,39)	0.725	35	R(26,36)	0.841	20
R(22,47)	0.864	17	R(24,40)	0.690	39	R(26,37)	0.740	33
R(22,48)	0.741	33	R(24,41)	0.800	25	R(26,38)	0.639	46
R(22,49)	0.739	33	R(24,42)	0.770	29	R(26,39)	0.788	27
R(23,24)	0.690	39	R(24,43)	0.732	34	R(26,40)	0.849	19
R(23,25)	0.769	29	R(24,44)	0.651	44	R(26,41)	0.832	21
R(23,26)	0.801	25	R(24,45)	0.632	46	R(26,42)	0.850	19
R(23,27)	0.793	26	R(24,46)	0.788	27	R(26,43)	0.827	22
R(23,28)	0.842	20	R(24,47)	0.745	32	R(26,44)	0.794	26
R(23,29)	0.857	18	R(24,48)	0.734	34	R(26,45)	0.840	20
R(23,30)	0.809	24	R(24,49)	0.763	30	R(26,46)	0.709	37
R(23,31)	0.857	18	R(25,26)	0.744	32	R(26,47)	0.825	22
R(23,32)	0.780	28	R(25,27)	0.703	37	R(26,48)	0.686	40
R(23,33)	0.738	33	R(25,28)	0.782	27	R(26,49)	0.699	38
R(23,34)	0.551	58	R(25,29)	0.831	21	R(27,28)	0.839	20
R(23,35)	0.817	23	R(25,30)	0.720	35	R(27,29)	0.839	20
R(23,36)	0.802	25	R(25,31)	0.785	27	R(27,30)	0.776	28
R(23,37)	0.732	34	R(25,32)	0.790	27	R(27,31)	0.873	16
R(23,38)	0.552	57	R(25,33)	0.682	40	R(27,32)	0.813	24
R(23,39)	0.732	34	R(25,34)	0.453	71	R(27,33)	0.881	15
R(23,40)	0.841	20	R(25,35)	0.776	28	R(27,34)	0.712	38
R(23,41)	0.857	18	R(25,36)	0.762	30	R(27,35)	0.864	17
R(23,42)	0.889	14	R(25,37)	0.629	47	R(27,36)	0.897	13
R(23,43)	0.740	33	R(25,38)	0.465	68	R(27,37)	0.779	28
R(23,44)	0.738	33	R(25,39)	0.615	49	R(27,38)	0.663	43
R(23,45)	0.769	29	R(25,40)	0.722	35	R(27,39)	0.749	32
R(23,46)	0.669	42	R(25,41)	0.816	23	R(27,40)	0.761	30
R(23,47)	0.881	15	R(25,42)	0.739	33	R(27,41)	0.856	18
R(23,48)	0.631	47	R(25,43)	0.686	40	R(27,42)	0.842	20

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(27,43)	0.804	25	R(29,46)	0.655	44	R(32,36)	0.882	15
R(27,44)	0.706	37	R(29,47)	0.865	17	R(32,37)	0.701	38
R(27,45)	0.703	37	R(29,48)	0.600	51	R(32,38)	0.568	55
R(27,46)	0.749	32	R(29,49)	0.660	43	R(32,39)	0.670	42
R(27,47)	0.801	25	R(30,31)	0.857	18	R(32,40)	0.732	34
R(27,48)	0.742	33	R(30,32)	0.812	24	R(32,41)	0.859	18
R(27,49)	0.707	37	R(30,33)	0.770	29	R(32,42)	0.780	28
R(28,29)	0.935	8	R(30,34)	0.694	40	R(32,43)	0.693	39
R(28,30)	0.905	12	R(30,35)	0.832	21	R(32,44)	0.646	45
R(28,31)	0.858	18	R(30,36)	0.849	19	R(32,45)	0.742	33
R(28,32)	0.846	20	R(30,37)	0.795	26	R(32,46)	0.638	46
R(28,33)	0.802	25	R(30,38)	0.662	43	R(32,47)	0.756	31
R(28,34)	0.605	52	R(30,39)	0.749	32	R(32,48)	0.615	49
R(28,35)	0.928	9	R(30,40)	0.825	22	R(32,49)	0.614	49
R(28,36)	0.882	15	R(30,41)	0.856	18	R(33,34)	0.747	33
R(28,37)	0.749	32	R(30,42)	0.826	22	R(33,35)	0.809	24
R(28,38)	0.601	51	R(30,43)	0.772	29	R(33,36)	0.857	18
R(28,39)	0.735	34	R(30,44)	0.786	27	R(33,37)	0.803	25
R(28,40)	0.826	22	R(30,45)	0.736	33	R(33,38)	0.717	36
R(28,41)	0.872	16	R(30,46)	0.764	30	R(33,39)	0.725	35
R(28,42)	0.859	18	R(30,47)	0.849	19	R(33,40)	0.707	37
R(28,43)	0.822	23	R(30,48)	0.694	39	R(33,41)	0.817	23
R(28,44)	0.786	27	R(30,49)	0.755	31	R(33,42)	0.818	23
R(28,45)	0.830	21	R(31,32)	0.890	14	R(33,43)	0.732	34
R(28,46)	0.687	40	R(31,33)	0.849	19	R(33,44)	0.667	42
R(28,47)	0.849	19	R(31,34)	0.661	44	R(33,45)	0.682	40
R(28,48)	0.649	45	R(31,35)	0.833	21	R(33,46)	0.788	27
R(28,49)	0.692	39	R(31,36)	0.912	11	R(33,47)	0.810	24
R(29,30)	0.856	18	R(31,37)	0.763	30	R(33,48)	0.733	34
R(29,31)	0.889	14	R(31,38)	0.615	49	R(33,49)	0.715	36
R(29,32)	0.877	16	R(31,39)	0.701	38	R(34,35)	0.608	51
R(29,33)	0.802	25	R(31,40)	0.762	30	R(34,36)	0.653	45
R(29,34)	0.571	56	R(31,41)	0.904	12	R(34,37)	0.769	30
R(29,35)	0.928	9	R(31,42)	0.857	18	R(34,38)	0.822	23
R(29,36)	0.913	11	R(31,43)	0.724	35	R(34,39)	0.736	34
R(29,37)	0.732	34	R(31,44)	0.707	37	R(34,40)	0.646	46
R(29,38)	0.584	53	R(31,45)	0.738	33	R(34,41)	0.631	48
R(29,39)	0.718	36	R(31,46)	0.685	40	R(34,42)	0.644	46
R(29,40)	0.793	26	R(31,47)	0.849	19	R(34,43)	0.698	39
R(29,41)	0.904	12	R(31,48)	0.662	43	R(34,44)	0.668	43
R(29,42)	0.842	20	R(31,49)	0.644	45	R(34,45)	0.469	69
R(29,43)	0.773	29	R(32,33)	0.803	25	R(34,46)	0.846	20
R(29,44)	0.722	35	R(32,34)	0.611	50	R(34,47)	0.607	51
R(29,45)	0.831	21	R(32,35)	0.836	21	R(34,48)	0.838	21

Продолжение таблицы 3

Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга	Пара образов	Значения парной корреляции	Значения расстояний Хэмминга
R(34,49)	0.856	19	R(37,44)	0.724	35	R(40,48)	0.725	35
R(35,36)	0.905	12	R(37,45)	0.613	49	R(40,49)	0.692	39
R(35,37)	0.756	31	R(37,46)	0.842	20	R(41,42)	0.857	18
R(35,38)	0.591	52	R(37,47)	0.771	29	R(41,43)	0.772	29
R(35,39)	0.741	33	R(37,48)	0.772	29	R(41,44)	0.706	37
R(35,40)	0.769	29	R(37,49)	0.818	23	R(41,45)	0.752	31
R(35,41)	0.896	13	R(38,39)	0.709	37	R(41,46)	0.717	36
R(35,42)	0.850	19	R(38,40)	0.662	43	R(41,47)	0.864	17
R(35,43)	0.812	24	R(38,41)	0.631	47	R(41,48)	0.647	45
R(35,44)	0.730	34	R(38,42)	0.646	45	R(41,49)	0.692	39
R(35,45)	0.824	22	R(38,43)	0.638	46	R(42,43)	0.787	27
R(35,46)	0.694	39	R(38,44)	0.638	46	R(42,44)	0.770	29
R(35,47)	0.825	22	R(38,45)	0.497	64	R(42,45)	0.803	25
R(35,48)	0.655	44	R(38,46)	0.819	23	R(42,46)	0.764	30
R(35,49)	0.699	38	R(38,47)	0.639	46	R(42,47)	0.897	13
R(36,37)	0.739	33	R(38,48)	0.796	26	R(42,48)	0.725	35
R(36,38)	0.607	50	R(38,49)	0.780	28	R(42,49)	0.676	41
R(36,39)	0.693	39	R(39,40)	0.843	20	R(43,44)	0.874	16
R(36,40)	0.738	33	R(39,41)	0.733	34	R(43,45)	0.734	34
R(36,41)	0.897	13	R(39,42)	0.795	26	R(43,46)	0.740	33
R(36,42)	0.818	23	R(39,43)	0.882	15	R(44,47)	0.762	30
R(36,43)	0.748	32	R(39,44)	0.851	19	R(44,48)	0.733	34
R(36,44)	0.683	40	R(39,45)	0.679	41	R(44,49)	0.715	36
R(36,45)	0.762	30	R(39,46)	0.795	26	R(45,46)	0.583	53
R(36,46)	0.693	39	R(39,47)	0.788	27	R(45,47)	0.793	26
R(36,47)	0.841	20	R(39,48)	0.803	25	R(45,48)	0.561	56
R(36,48)	0.670	42	R(39,49)	0.787	27	R(45,49)	0.557	56
R(36,49)	0.684	40	R(40,41)	0.777	28	R(46,47)	0.725	35
R(37,38)	0.819	23	R(40,42)	0.841	20	R(46,48)	0.835	21
R(37,39)	0.795	26	R(40,43)	0.819	23	R(46,49)	0.866	17
R(37,40)	0.763	30	R(40,44)	0.849	19	R(47,48)	0.686	40
R(37,41)	0.811	24	R(40,45)	0.769	29	R(47,49)	0.652	44
R(37,42)	0.795	26	R(40,46)	0.732	34	R(48,49)	0.843	20
R(37,43)	0.724	35	R(40,47)	0.833	21			

На основе полученных данных был сделан вывод что все образы являются зависимыми, так как отсутствуют значения коэффициентов корреляции равные нулю. Из расстояний Хэмминга можно сделать вывод о том, что первый образ имеет больше всего различающихся позиций.

18. После чего было вычислено математическое ожидание и стандартное отклонение для 1 и 12 образа. Результат вычисления были занесены в таблицу 4.

Таблица 4 – Математическое ожидание и стандартное отклонение

Образ	Математическое ожидание	Стандартное отклонение
1	-0,424938	0,083465
12	0,763576	0,201852

19. Далее интерпретируем полученные результаты в график. Результаты представлены на рисунках 49 – 50.

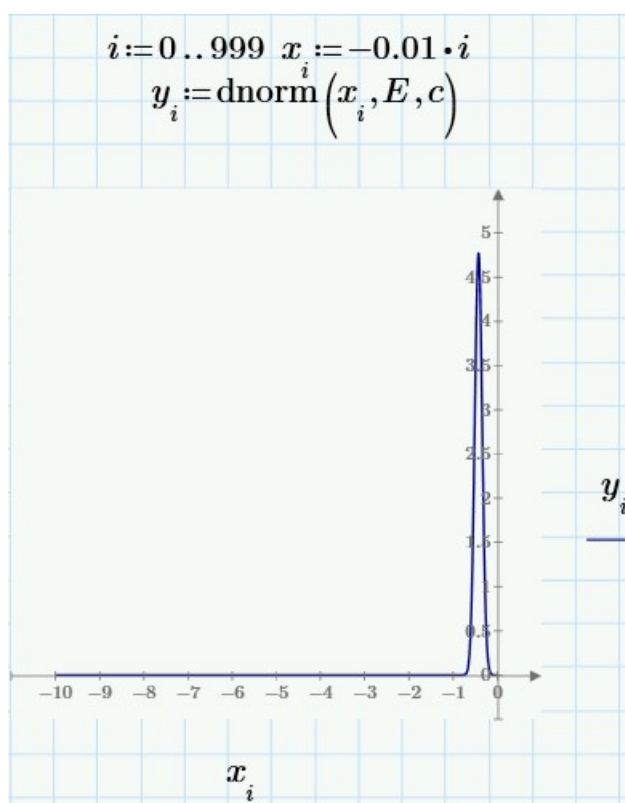


Рисунок 49 - График для 1 образа

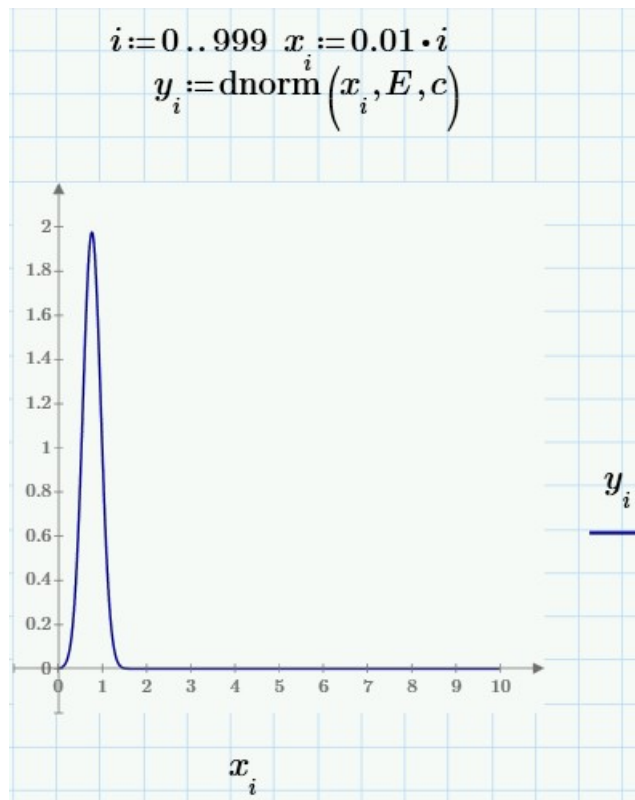


Рисунок 50 - График 12 образа

20. На основе полученных данных были произведены вычисления энтропии. Результаты вычисления представлены на рисунках 51 – 52.

$$\begin{aligned}
 c &:= .083465 \\
 E &:= -.424938 \\
 p &:= \frac{1}{c \cdot \sqrt{2 \cdot \pi}} \cdot \int_{-\infty}^1 \exp\left(\frac{-(x-E)^2}{2 \cdot c^2}\right) dx = 0.999 \\
 -\log(p, 2) &= -8.59 \cdot 10^{-10}
 \end{aligned}$$

Рисунок 51 - Энтропия для 1 образа

$$\begin{aligned}
 c &:= .201852 \\
 E &:= .763576 \\
 p &:= \frac{1}{c \cdot \sqrt{2 \cdot \pi}} \cdot \int_{-\infty}^1 \exp\left(\frac{-(x-E)^2}{2 \cdot c^2}\right) dx = 0.879 \\
 -\log(p, 2) &= 0.186
 \end{aligned}$$

Рисунок 52 - Энтропия для 12 образа

21. Сравнивая полученные результаты, мы видим, что 1 образ «Чужой» так и 12 образ «Чужой» не достиг образа «Свой».

6 Разработка индивидуальных вариантов выполнения практикума

Были разработаны индивидуальные варианты задания для выполнения практикума в количестве 55 штук, которые представлены в таблице 5.

Таблица 5 – Индивидуальные варианты задания

№ варианта	Символ для обучения системы	Символы для тестирования системы	
1	а	z	я
2	б	y	ю
3	в	x	э
4	г	w	ы
5	д	v	щ
6	е	u	ш
7	ж	t	ч
8	з	s	ц
9	и	r	х
10	к	q	ф
11	л	p	у
12	м	o	т
13	н	n	с
14	о	m	р
15	п	l	в
16	р	k	о
17	с	j	н
18	т	i	м
19	у	h	л
20	ф	g	к
21	х	f	и
22	ц	e	з
23	ч	d	ж
24	ш	c	е
25	щ	b	д
26	ы	a	г
27	э	v	б
28	ю	a	п

Продолжение таблицы 5

29	я	б	a
30	a	я	z
31	b	ю	y
32	c	э	x
33	d	ы	w
34	e	щ	v
35	f	ш	u
36	g	ч	t
37	h	ц	s
38	l	х	r
39	j	ф	q
40	k	у	p
41	l	т	o
42	m	с	n
43	n	р	m
44	o	п	l
45	p	о	k
46	q	н	j
47	r	м	i
48	s	л	h
49	t	к	g
50	u	и	f
51	v	з	e
52	w	ж	d
53	x	е	c
54	y	д	b
55	z	г	a

При выполнении практикума каждый студент получает свой индивидуальный вариант задания от 1 до 55.

7 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Согласно ГОСТ 12.0.003-2015 [9] опасные и вредные производственные факторы по характеру своего происхождения подразделяют:

- на факторы, порождаемые физическими свойствами и характеристиками состояния материальных объектов производственной среды;
- факторы, порождаемые химическими и физико-химическими свойствами используемых или находящихся в рабочей зоне веществ и материалов;
- факторы, порождаемые биологическими свойствами микроорганизмов, находящихся в биообъектах и (или) загрязняющих материальные объекты производственной среды;
- факторы, порождаемые поведенческими реакциями и защитными механизмами живых существ (укусы, ужаления, выброс ядовитых или иных защитных веществ и т.п.);
- факторы, порождаемые социально-экономическими и организационно-управленческими условиями осуществления трудовой деятельности (плохая организация работ, низкая культура безопасности и т.п.);
- факторы, порождаемые психическими и физиологическими свойствами и особенностями человеческого организма и личности работающего (плохое самочувствие работника, нахождение работника в состоянии алкогольного, наркотического или токсического опьянения или абстиненции, потеря концентрации внимания работниками и т.п.).

Вредные психофизические факторы подразделяют:

- на физические перегрузки, связанные с тяжестью трудового процесса;

- нервно-психические перегрузки, связанные с напряженностью трудового процесса.

Физические перегрузки подразделяют:

- на статические, связанные с рабочей позой;
- динамические нагрузки, связанные с массой поднимаемого и перемещаемого вручную груза;
- динамические нагрузки, связанные с повторением стереотипных рабочих движений. .

Специалист по защите информации каждый день на протяжении долгого времени находится в сидячем положении и зачастую выполняет монотонную работу. Долгое время препровождения в сидячем положении дает нагрузку на шейный и позвоночный отдел работника, негативно влияет на систему кровообращения организма. Большой поток информации снижает концентрацию и работоспособность специалиста по защите информации.

Для предотвращения развития болезней опорно-двигательного аппарата является повышение двигательной активности. Двигательная активность необходима человеку для правильного функционирования организма в целом и органов и тканей в частности. Снижение двигательной активности приводит к дегенеративным процессам в организме человека. Наиболее доступным средством увеличения двигательной активности являются занятия физической культурой, спортом. Следует уделять физическим упражнениям не меньше 150 минут в неделю. Это способствует укреплению костей и развитию мышц, что позволяет значительно снизить риск развития заболеваний опорно-двигательной системы и обеспечить достойную мышечную поддержку позвоночнику и костям.

Заключение

В ходе выполнения выпускной квалификационной работы был разработан практикум по оценке энтропии кодов откликов нейросети на примере рукописного образа «Чужой» в пространстве корреляционных связей между разрядами.

В процессе работы был произведен обзор средств тестирования биометрической аутентификации, разработан алгоритм для вычисления коэффициентов парной корреляции, а также программа, которая реализует данный алгоритм. Произведено тестирование разработанной программы, разработаны рекомендации для проведения практикума. Были составлены индивидуальные варианты задания на практику. В заключении были выделены вредные психофизические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации, и разработана методика, снижающая их воздействие.

Результатом выпускной квалификационной работы является практикум по оценке энтропии кодов откликов нейросети на примере рукописного образа «Чужой» в пространстве корреляционных связей между разрядами.

Таким образом, задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

1. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. – Москва, 2006.
2. ГОСТ Р 52633.5-2011 Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – Москва, 2011.
3. ГОСТ Р ИСО/МЭК 19795-1-2007 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура. – Москва, 2007.
4. ГОСТ Р 52633.3-2011 Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. – Москва, 2011.
5. Иванов А.И. Тестирование нейронных сетей, обученных алгоритмом ГОСТ Р 52633.5-2022, в среде моделирования «БиоНейроАвтограф»: учебно-методическое пособие / Издательство «Пензенского государственного университета», 2020, 36 с., доступно через библиотеку кафедры «Технические средства информационной безопасности» по ссылке <https://tsib.pnzgu.ru/page/39329>
6. Иванов А.И., Захаров О.С. Среда моделирования «БиоНейроАвтограф». Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ» <http://пниэи.пф/activity/science/noc/bioneuroautograph.zip> для свободного использования университетами России, Белоруссии, Казахстана.
7. Горбунов К.А., Никитин В.В. Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний хэмминга при их применении к ключам-откликам на примеры одного образа «Чужой» // Труды IV Всероссийской

конференции «Безопасность информационных технологий» Из-во Пензенского государственного университета 2021 г. Том. 1, с. 83 -86

8. Иванов А.И., Иванов А.П., Ратников К.А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга. Препринт. // Пенза – 2021 г. Издательство «ПГУ» – 56 с. Тираж 300 экз. ISBN -978-5-907364-94-3, DOI: 10.13140/RG.2.2.16514.35524.

9. ГОСТ 12.0.003–2015 Межгосударственный стандарт. Система стандартов по безопасности труда. Опасные и вредные производственные факторы. Классификация. – Стандартиформ, 2016.

Приложение А
(обязательное)
Алгоритм программы

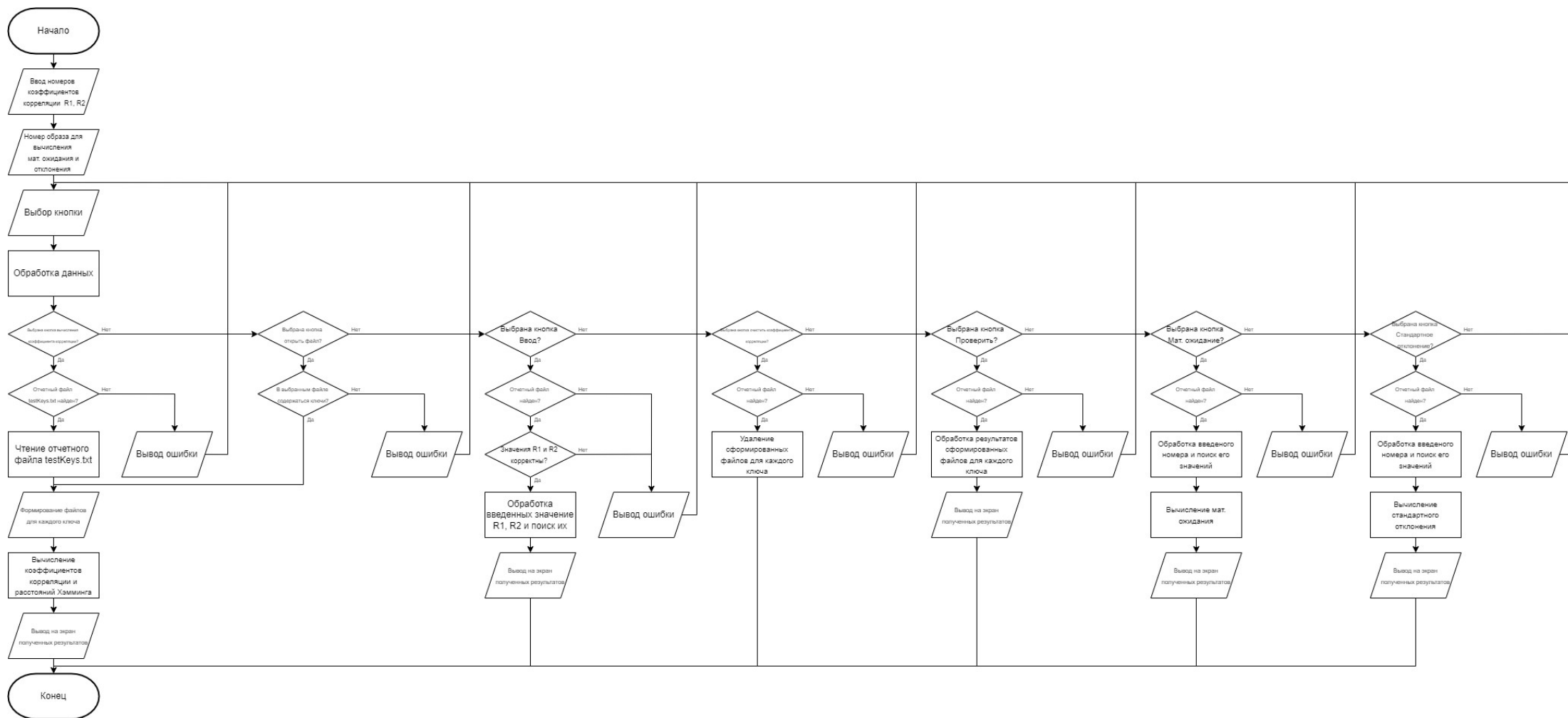


Рисунок А.1 – Алгоритм

В алгоритме имеется два блока ввода данных, которые получают номера образов для расчета коэффициентов корреляции и номер образа для расчета математического ожидания и стандартного отклонения. После получения номера пользователю предоставляется возможность выбора кнопки, для этого выделен еще один блок. Остальные 13 блоков служат для вывода полученных данных и сигналов об ошибках.

В алгоритме присутствует 15 логических блоков, 7 из которых отвечает за проверку выбранной кнопки, а остальные 8 за проверку полученных данных.

Блоки обработки информации в количестве 10 штук отвечают за вычисление коэффициентов парной корреляции, расстояний Хэмминга, математического ожидания, стандартного отклонения, а так же за обработку отчетных файлов среды моделирования «БиоНейроАвтограф».

Приложение Б

(справочное)

Статья, принятая к публикации в сборнике научных статей по материалам
Всероссийской научно-технической конференции «Безопасность
информационных технологий»

Статья для Тома 1 для V Всероссийской конференции БИТ 2022, Пенза, май
2022

КАЛЬКУЛЯТОР ОЦЕНКИ ЭНТРОПИИ КОДОВ ОТКЛИКОВ НЕЙРОСЕТИ НА ПРИМЕРЕ РУКОПИСНОГО ОБРАЗА «ЧУЖОЙ» В ПРОСТРАНСТВЕ КОРРЕЛЯЦИОННЫХ СВЯЗЕЙ МЕЖДУ ИХ РАЗРЯДАМИ

Владислав Алексеевич Сумин

Пензенский государственный университет, г. Пенза, Россия

suminvladislav777@gmail.com

Аннотация. Исследуются принципы работы биометрической нейросетевой аутентификации личности путем преобразования личных биометрических данных человека в его криптографический ключ. Параллельно с анализом кодов в пространстве расстояний Хэмминга исследуется возможность оценки энтропии в пространстве корреляционных связей разрядов, анализируемых кодов.

Ключевые слова. Биометрическая аутентификация, биометрический образ «Свой», биометрический образ «Чужой», коэффициенты корреляции между разрядами кода, расстояние Хемминга.

Большее половины мирового населения имеют аккаунты на одной или нескольких платформах. Как показывает практика, парольная защита доступа к личным интернет ресурсам имеет ряд уязвимостей. Пользователи обычно применяют короткие, легко подбираемые паролями. Для повышения

безопасности парольной защиты в настоящее время желательно использовать биометрическую аутентификацию.

Биометрическая аутентификация – процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа «Свой» и путём преобразования этого образа в соответствии с заранее определённым протоколом нейросетевой аутентификации по требованиям ГОСТ Р 52633.0-2006 [1].

Корректная работа биометрической аутентификации заключается в автоматическом обучении нейросетевого преобразователя по ГОСТ Р 52633.5-2011 [2]. Для обучения нейросетевого преобразователя биометрический код использует от 8 до 20 примеров образа «Свой» и не менее 256 примеров образа «Чужой».

Нейросетевой преобразователь – преобразователь, заранее обученный преобразовывать многомерные континуумы примеров биометрического образа «Свой» в почти однозначный выходной код криптографического ключа или длинного пароля доступа по ГОСТ Р 52633.0-2006. После каждого обучения нуждается в быстром автоматическом тестировании.

Биометрический образ «Свой» – биометрический образ человека, параметры которого порождают с высокой вероятностью от 0.92 до 0.95 на выходах обученной нейронной сети код его личного криптографического ключа.

Биометрический образ «Чужой» – случайный биометрический образ, параметры которого порождают на выходах обученной нейронной сети случайный выходной код.

Так как биометрические образы могут быть подвержены к атакам подбора, основным требованием является вычисление вероятности ошибок второго рода и выполнение процедур тестирования.

Ошибка второго рода – вероятность ложной идентификации пользователя, отсутствующего в базе данных. Такая ошибка должна

оцениваться либо по международным рекомендациям стандарта ГОСТ Р ИСО/МЭК 19795-1-2007, либо ГОСТ 3 52633.3-2011.

Если производить оценку по ГОСТ Р ИСО/МЭК 19795-1-2007, то придется использовать тестовые базы с объемом тестовых образов «Чужой» в 30 раз больше, чем обратная величина предполагаемой стойкости к атакам подбора. Так, если будет тестироваться защита образа с вероятностью ошибок в 0.0000001, размер тестовой базы должен составлять более 30 миллионов образов «Чужой». Это является значительным юридическим барьером для выполнения лабораторных работ по биометрии для университетов. Во всех странах сбор, хранение и использовать большие базы биометрических образов ЗАПРЕЩЕНО. Именно по этой причине мы постоянно даем «согласие» на обработку своих персональных данных.

Решить проблему возможно, если воспользоваться отечественным стандартом по быстрому тестированию на малых выборках. ГОСТ 3 52633.3-2011. Этот стандарт требует перехода от анализа обычных кодов к расстояниям Хэмминга между ними.

Метрика Хэмминга позволяет значительно сэкономить вычислительные ресурсы при реализации генетических алгоритмов направленного перебора. В рамках гипотезы нормального распределения расстояний Хэмминга позволяет вычислить математическое ожидание и стандартное отклонение [5]. По этим параметрам можно вычислить вероятность ошибок второго рода, что позволит определить процентное прохождение аутентификации биометрического образа «Чужой».

Немаловажно произвести логарифмические вычисления для поиска энтропии образа «Чужой». По результатам вычисления минимальная энтропия образа «Чужой» показывает насколько ближе к образу «Свой». Особенностью данных расчетов является оценка расстояний Хэмминга, которая в свою очередь требует данные в виде примеров образа «Свой» и данные о биокоде «Свой».

Корреляционная метрика среднего значения модулей коэффициентов парной корреляции способствует вычислению энтропии, минуя промежуточную оценку расстояний Хэмминга [6]. Каждый из образов будет иметь свое распределение корреляции, на основе которых будет сделан вывод о стойкость к атакам подбора.

В работе [7] путем проведения численного эксперимента было показано, что шкала расстояний Хэмминга, используемая ГОСТ Р 52633.3 [4] и шкала взаимных коэффициентов корреляции, исследуемых разрядов кодов обратны. К сожалению, численный эксперимент с был проведен на минимальной выборке в два образа «Чужой». Столь малая выборка была обусловлена необходимостью ручного редактирования отчетного файла среды моделирования «БиоНейроАвтограф» [6] testKeys.txt. Экранная форма стандартного редактора отчетного файла testKeys.txt, приведена на рисунке Б.1.

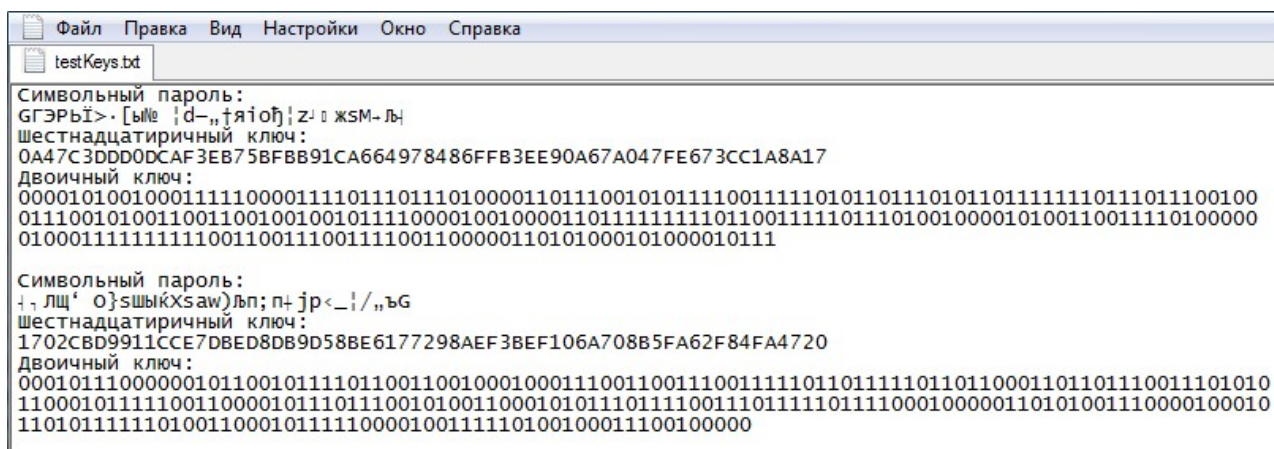


Рисунок Б.1 – Экранная форма стандартного редактора, которую приходилось при ручном редактировании, так как формат файла testKeys.txt специфичен и не читается обычными средствами автоматизации вычислений

Автоматизация чтения отчетного файла testKeys.txt среды моделирования «БиоНейроАвтограф» выполняется при запуске,

разработанного на С++ калькулятора коэффициентов корреляции. Экранная форма, разработанного калькулятора приведена на рисунке Б.2.

Корреляция R	Расстояние H
R(0,1) = 0.506	H(0,1) = 63
R(0,2) = 0.529	H(0,2) = 60
R(0,3) = 0.570	H(0,3) = 55
R(0,4) = 0.471	H(0,4) = 68
R(0,5) = 0.333	H(0,5) = 86
R(0,6) = 0.387	H(0,6) = 79
R(0,7) = 0.384	H(0,7) = 79
R(0,8) = 0.348	H(0,8) = 83
R(0,9) = 0.522	H(0,9) = 61
R(0,10) = 0.205	H(0,10) = 102
R(0,11) = 0.380	H(0,11) = 80
R(0,12) = 0.493	H(0,12) = 65
R(0,13) = 0.436	H(0,13) = 73
R(0,14) = 0.506	H(0,14) = 63
R(0,15) = 0.570	H(0,15) = 55
R(0,16) = 0.591	H(0,16) = 52
R(0,17) = 0.523	H(0,17) = 61
R(0,18) = 0.741	H(0,18) = 33
R(0,19) = 0.266	H(0,19) = 94

Рисунок Б.2 – Экранная форма, разработанного корреляционного калькулятора

Для того, что бы результаты вычислений «корреляционного калькулятора» были корректны перед его использованием необходимо удалять (стирать) уже существующий файл в среде моделирования DATA/testKeys.txt. Далее следует запустить среду моделирования в режиме тестирования для примеров одного биометрического образа «Чужой» [5]. При этом среда моделирования формирует новый файл отчетности DATA/testKeys.txt.

Программное обеспечение читает этот новый файл DATA/testKeys.txt, получая из него, например, 20 бинарных ключей длиной в 256 бит. Далее калькулятор вычисляет $(20 \times 20 - 20) / 2 = 190$ коэффициентов корреляции и расстояний Хэмминга. Очевидно, что 190 случайных коэффициентов корреляции и 190 расстояний Хэмминга должны давать более достоверные статистические оценки в сравнении с алгоритмом предсказания по ГОСТ Р 52633.3 [4], использующем только 20 расстояний Хэмминга [8].

В силу того, что корреляционный калькулятор должен давать доступ к большим массивам данных в его экранной форме предусмотрено два скроллинга для отображения массива коэффициентов корреляции и массива расстояний Хэмминга с отображением трех значащих десятичных цифр (рис.2). Для просмотра точного значения вычисляемых параметров (6 десятичных цифр) предусмотрен ручной набор номеров примеров образа «Чужой». Параллельно с выводом на экран корреляционный коррелятор записывает в данные постоянно обновляемые в отчетные файлы DATA/testKeys_R.txt и DATA/testKeys_H.txt.

Список литературы

1. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
2. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
3. ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура»
4. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
5. Иванов А.И. Тестирование нейронных сетей, обученных алгоритмом ГОСТ Р 52633.5-2022, в среде моделирования «БиоНейроАвтограф»: учебно-методическое пособие / Издательство «Пензенского государственного университета», 2020, 36 с., доступно через библиотеку кафедры «Технические средства информационной безопасности» по ссылке <https://tsib.pnzgu.ru/page/39329>

6. Иванов А.И., Захаров О.С. Среда моделирования «БиоНейроАвтограф». Программный продукт создан лабораторией биометрических и нейросетевых технологий, размещен с 2009 г. на сайте АО «ПНИЭИ» <http://пниэи.рф/activity/science/noc/bioneuroautograph.zip> для свободного использования университетами России, Белоруссии, Казахстана.

7. Горбунов К.А., Никитин В.В. Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний хэмминга при их применении к ключам-откликам на примеры одного образа «Чужой» // Труды IV Всероссийской конференции «Безопасность информационных технологий» Из-во Пензенского государственного университета 2021 г. Том. 1, с. 83 -86

8. Иванов А.И., Иванов А.П., Ратников К.А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга. Препринт. // Пенза – 2021 г. Издательство «ПГУ» – 56 с. Тираж 300 экз. ISBN -978-5-907364-94-3, DOI: 10.13140/RG.2.2.16514.35524.

Информация об авторах:

Сумин Владислав Алексеевич – студент каф ИБСТ, Пензенский государственный университет.