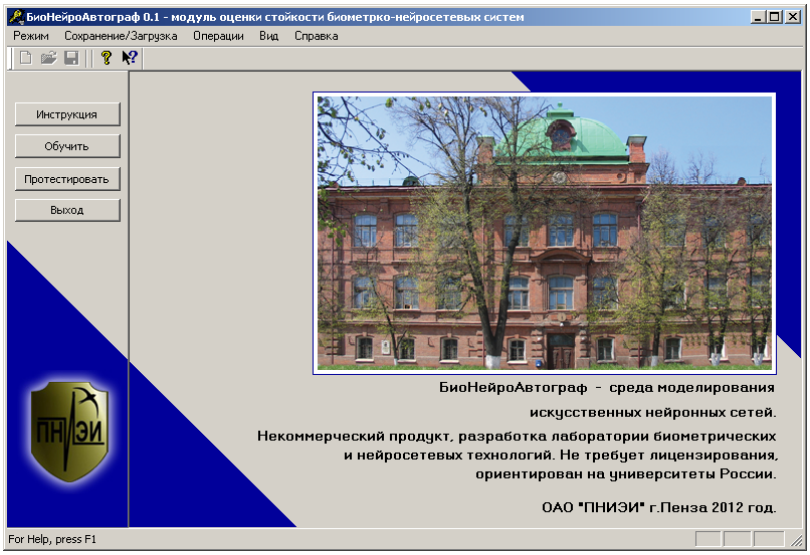
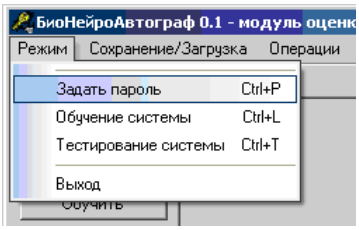
"Пензенский государственный университет"
Кафедра "Информационной безопасности систем и технологий"
Лабораторная работа №3 "Оценка вероятности ошибок первого рода (отказ в доступе "Своему"), использующая статистики расстояний Хэмминга"

1. Запустить среду моделирования БиоНейроАвтограф.exe при этом появится главное диалоговое окно программы.

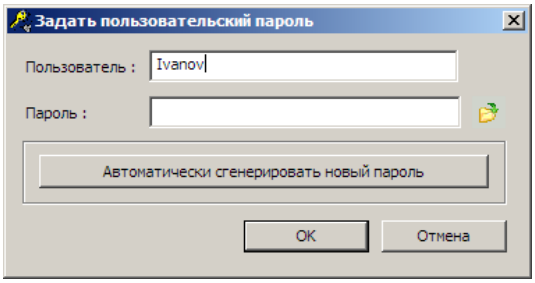


2. Выберете пункт меню "Режим".

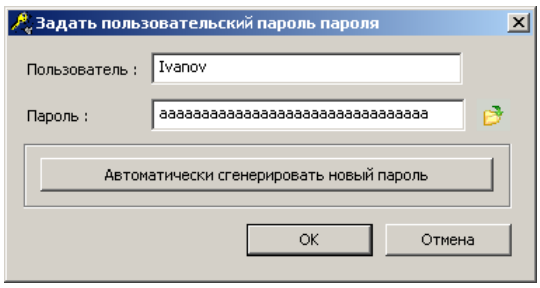


3. Выберите режим "Задать пароль".

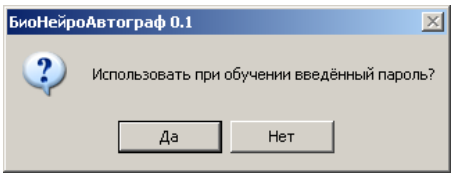
4. В появившейся форме создания пароля в поле "Пользователь" введите свою фамилию либо имя, под которым Вы будете работать в системе.



5. Далее в поле "Пароль" задайте пароль из 32 символов "*aaaaaa…aaaaaa*". Пароль вводится в латинской кодировке клавиатуры.

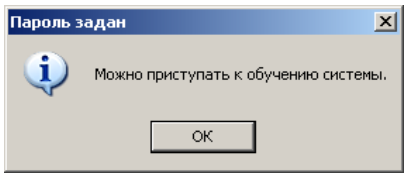


6. Далее нажмите "ОК".



7. В появившемся диалоговом окне нажмите "Да". После этого введённое имя пользователя и пароль будут использоваться при обучении и тестировании системы.

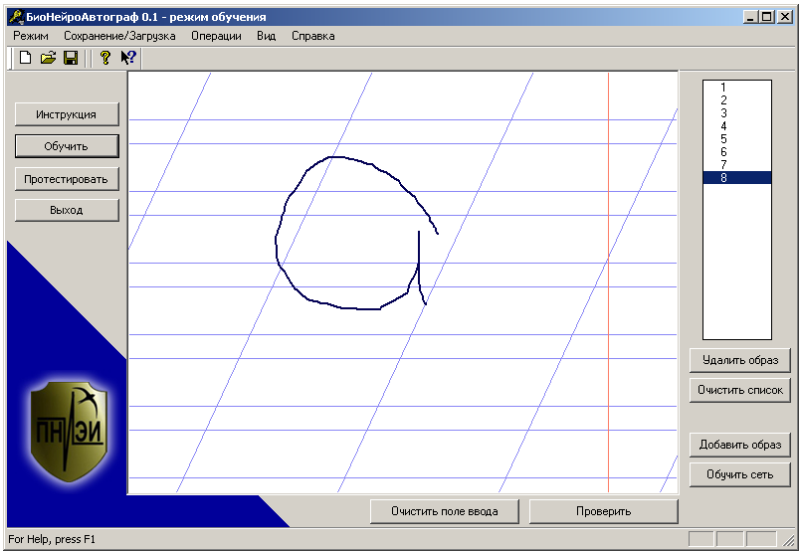
8. Если все пользовательские данные сохранены успешно, то появится сообщение об успешном создании пароля. Нажмите "ОК".



9. После создания пароля можно приступать к обучению системы. Для этого в главном диалоговом окне программы нажмите кнопку "Обучить".

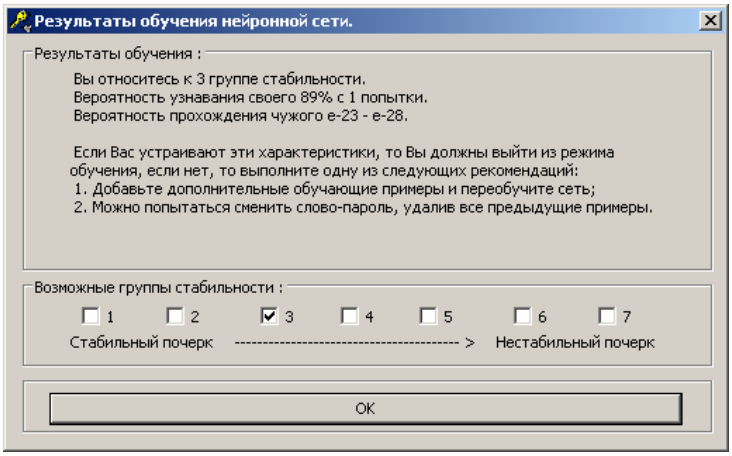
10. Появится диалоговое окно обучения с разлинованным полем ввода рукописных символов/слов. Рукописные слова/символы можно вводить как с помощью графического планшета, так и с помощью стандартной "мышки".

11. В поле ввода введите один рукописный символ "*а*", далее нажмите кнопку "Добавить образ".



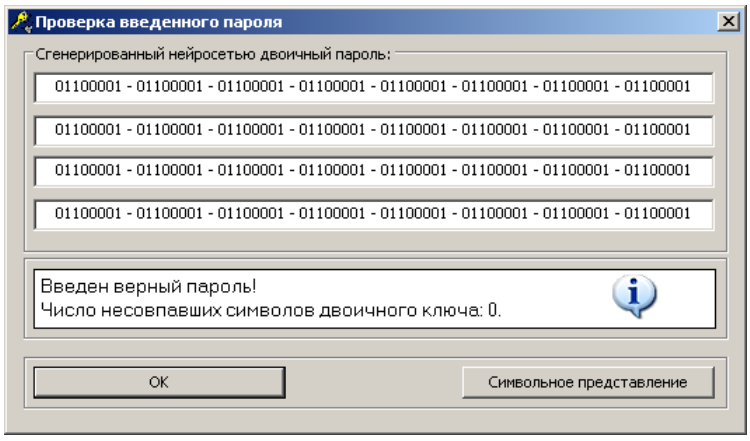
Повторите операцию ввода не менее 8 раз. Рукописные образы нужно писать быстро, опираясь на имеющиеся у вас подсознательные рефлексы, выработанные много лет назад на уроках чистописания.

12. После ввода достаточного количества примеров (8 – 12) нажмите кнопку "Обучить сеть", при этом начнётся процесс обучения и через несколько секунд появится окно с результатами обучения.

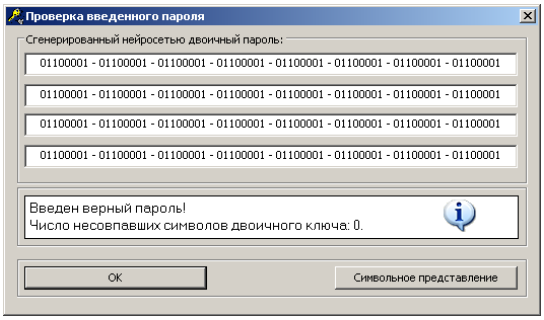


Для закрытия окна нажмите кнопку "ОК"

13. Для проверки качества обучения введите контрольный рукописный образ и нажмите кнопку "Проверить". Далее введите рукописный символ *"a"*. Если средство аутентификации Вас узнает, то появится сообщение "Введен верный пароль!".



14. Проведите тестирование способности узнавать "Своего", введя рукописный символ "а" 50 раз. При этом большинстве случаев должен получаться верный код, а в редких случаях получается неверный выходной код доступа.



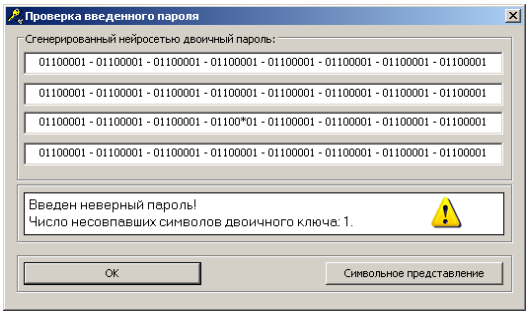


Таблица №1

Попытка / Образ	Расстояния Хэмминга до образа *"a"*									
	1	2	3	4	5	6	7	8	9	10
"a"	0	0	0	0	0	0	0	0	0	0
"a"	0	0	0	0	0	0	0	0	**1**	0
"a"	0	0	0	**3**	0	0	0	0	0	0
"a"	0	0	0	0	0	0	0	0	0	0
"a"	0	0	0	0	0	0	0	0	0	0

15. Вычислите вероятность ошибок первого рода по обычной формуле для 10, 20, 30, 40 и 50 опытов:

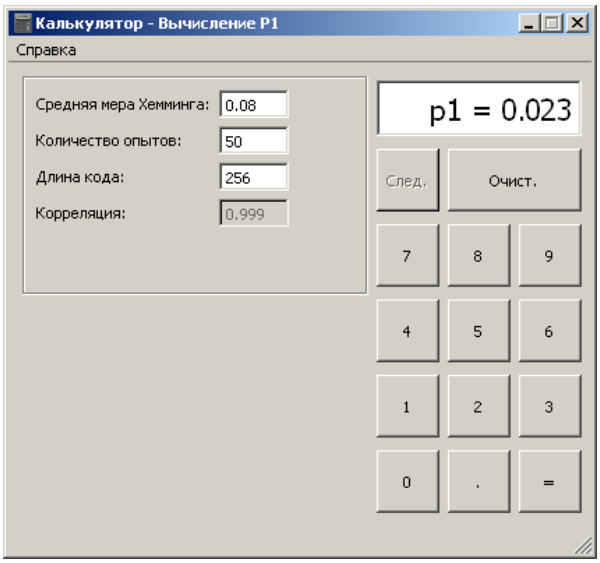
$$P1=\frac{0}{10}=0;\quad P1=\frac{1}{20}=0.05;\quad P1=\frac{2}{30}=0.066;\quad P1=\frac{2}{40}=0.05;\quad P1=\frac{2}{50}=0.04.$$

16. Вычислите математическое ожидание расстояний Хэмминга для 10, 20, 30, 40 и 50 опытов E(h)=0.0; E(h)=0.05; E(h)=0.134; E(h)=0.1; E(h)=0.08.

Далее вычислителе определенный интеграл распределения хи-квадрат расстояний Хэмминга с числом степеней свободы m= E(h)=0.0; 0.05; 0.134; 0.1; 0.08 в интервале от 1 до ∞:

$$P_1=\int_1^{\infty} p(\chi^2(h,m=0.08)\cdot dh=0.023$$

Для вычислений воспользуйтесь калькулятором вычисления вероятности P_1 (калькулятор CalculatorP1.exe находится в папке КАЛЬКУЛЯТОРЫ рядом с запускаемым файлом БиоНейроАвтограф.exe)



или любой из доступных Вам программ математического моделирования. При этом для данных, приведенных выше получим:

P1=0.026; P1=0.014; P1=0.038; P1=0.029; P1=0.023.

17. Убедитесь, что вычисления вероятности по обычной формуле (п.15) дает более нестабильные результаты (большой разброс результатов) в сравнении более стабильным результатом оценок ошибок первого рода с учётом выявленных значений расстояний Хэмминга (меньший разброс результатов).

18. Проверьте какая из оценок точнее. Для этой цели продолжите испытания, повторив еще 50 раз написание символа "*a*". Данные сведите в таблицу 2.

Таблица №1.

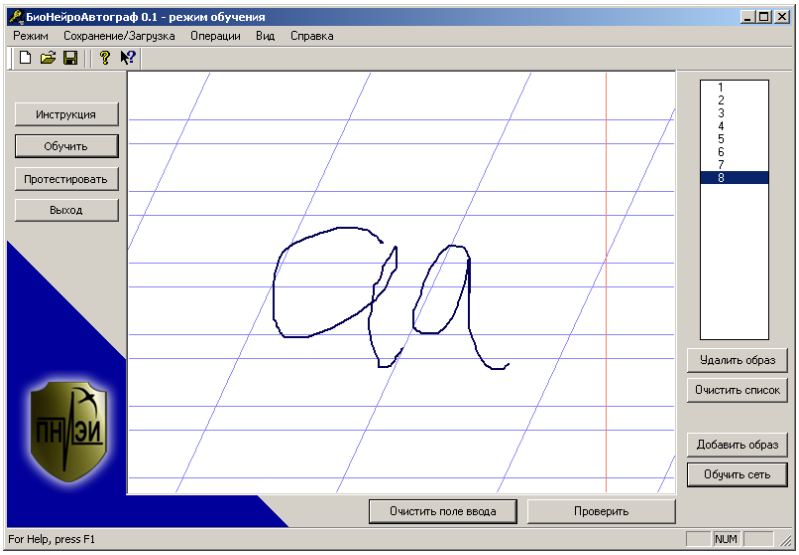
Попытка / Образ	Расстояния Хэмминга до образа "*a*"									
	1	2	3	4	5	6	7	8	9	10
"a"	0	0	0	0	0	0	0	0	0	0
"a"	0	0	0	0	0	0	0	0	0	0
"a"	0	0	0	0	0	0	0	0	0	0
"a"	0	0	0	0	0	0	0	0	0	0
"a"	**2**	0	0	0	0	0	0	0	0	0

19. Вычислите вероятность ошибок для всех 100 опытов (учитываются результаты таблицы 1 и таблицы 2):

$$P1 = \frac{3}{100} = 0.03$$

20. Сравните полученное значение вероятности ошибок первого рода с данными, вычисленными ранее на малом числе примеров. Примете решение, о том, какой метод вычисления ошибок вероятностей первого рода точнее на малых тестовых выборках.

21. Переобучите средство аутентификации на двух, вводимых подряд, рукописных символах "*аа*". Вводить данные следует не менее 8 раз.



22. Проверьте то, как Вас узнает средство аутентификации, введя 20 раз рукописный образ из двух символов. Данные введите в таблицу 3.

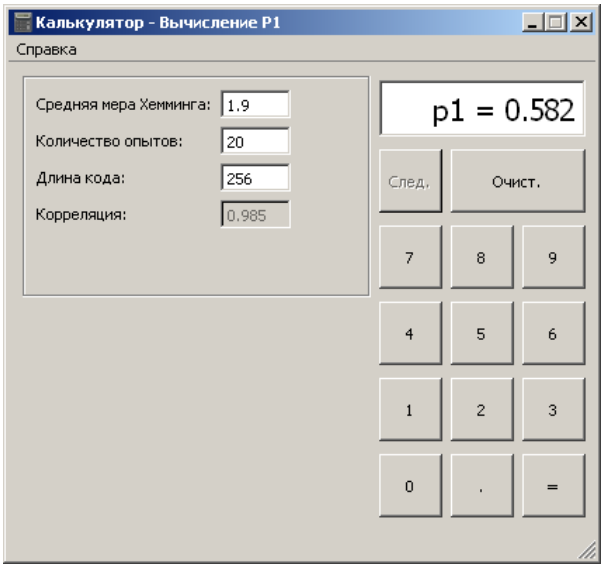
Таблица №3.

Попытка / Образ	Расстояния Хэмминга до образа "*аа*"									
	1	2	3	4	5	6	7	8	9	10
"*аа*"	1	7	0	0	3	0	0	2	0	10
"*аа*"	0	2	0	3	0	0	6	0	4	0

23. Вычислите вероятности ошибок первого рода по обычной формуле:

$$P1 = \frac{9}{20} = 0.45$$

24. Вычислите математическое ожидание расстояний Хэмминга E(h)=1.9 и по нему вычислите вероятность ошибок первого рода, пользуясь хи-квадрат распределением с 1.9 степенями свободы:



25. В связи с высоким уровнем вероятности ошибок первого рода средство аутентификации необходимо переобучить, дополнительно введя еще 4 образа "*аа*". (п. 12).

26. Повторите тестирование на 20 тестовых образах, данные сведите в таблицу 4.

Таблица №4.

Попытка / Образ	Расстояния Хэмминга до образа "*аа*"									
	1	2	3	4	5	6	7	8	9	10
"*аа*"	0	0	0	**1**	0	0	0	0	0	0
"*аа*"	0	0	0	0	0	**5**	0	0	0	0

27. Вычислите вероятность появления ошибки первого рода классическим методом:

$$P1 = \frac{2}{20} = 0.1.$$

28. Вычислите вероятность появления ошибок первого рода с учетом значений расстояний Хэмминга $E(h)=\frac{6}{20} = 0.3$ P1=0.09.

ВЫВОД:

1. Учёт дополнительной информации в виде математического ожидания расстояний Хэмминга при малом числе опытов позволяет получить более достоверные результаты при оценке вероятностей появления ошибок первого рода. Повышение достоверности оценки является следствием учета большего объёма исходной информации.

2. Сложные биометрические образы (состоящие из большего числа рукописных символов) обладают большей нестабильностью по сравнению с простыми биометрическими образами. Нестабильность биометрического образа может быть скомпенсирована за счёт увеличения тестовых примеров в обучающей выборке.