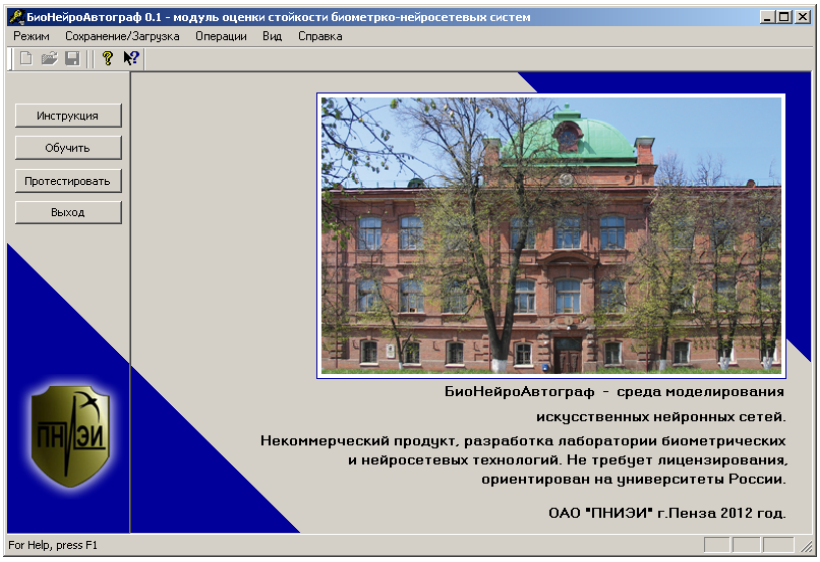
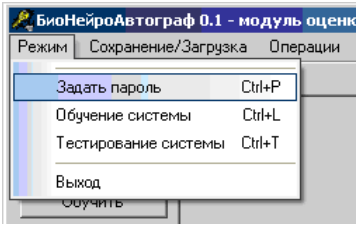
Научно-образовательный центр "Информационная безопасность систем и технологий" ОАО "ПНИЭИ" и ФБГОУ ВПО "Пензенского государственного университета"

Лабораторная работа №7 "Тестирование стойкости к атакам подбора преобразователя биометрия-код на случайных и зависимых данных"

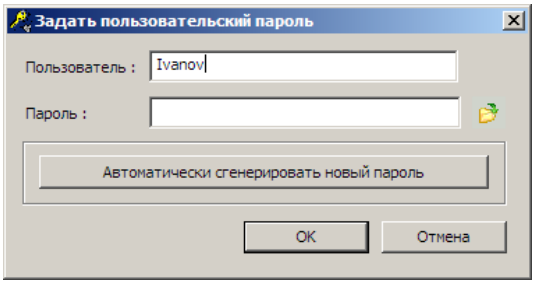
1. Подключите к ПЭВМ графический планшет любой фирмы, установите драйвер графического планшета. Запустите среду моделирования "БиоНейроАвтограф" (файл БиоНейроАвтограф.exe), при этом появится главное диалоговое окно программы.



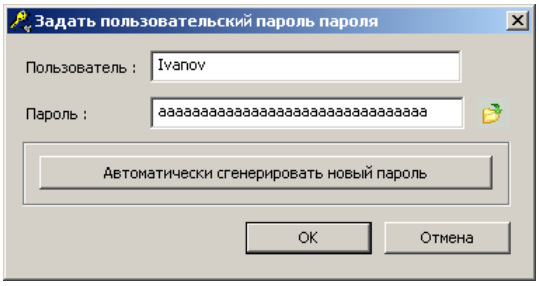
2. Выберите пункт меню "Режим".
3. Выберите режим "Задать пароль".



4. В появившемся диалоговом окне создания пароля в поле "Пользователь" введите свою фамилию либо имя, под которым вы будете работать в системе.

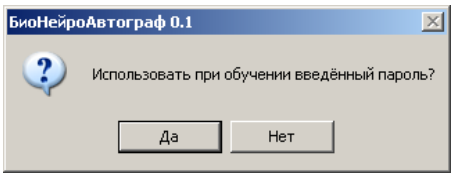


5. Далее в поле "Пароль" задайте пароль из 32-х символов "*аааааа…аааааа*". Пароль вводится в латинской кодировке клавиатуры.

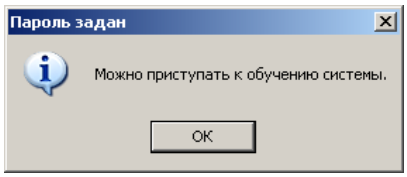


6. Далее нажмите "ОК".

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



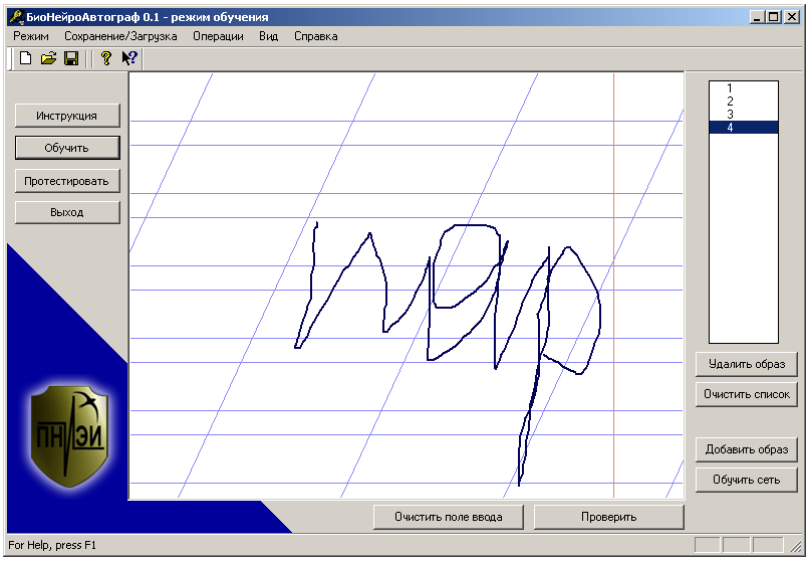
8. Если все пользовательские данные успешно сохранены, то появится сообщение об успешном создании пароля. Нажмите "ОК".



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

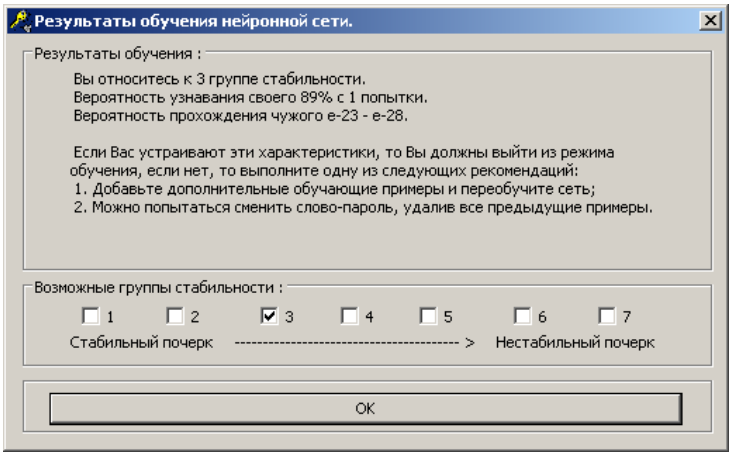
10. Появится диалоговое окно обучения с разлинованным полем ввода рукописных символов/слов. Рукописные слова-пароли вводятся с помощью графического планшета.

11. В поле ввода введите один пример рукописного слова-пароля "*пар*" своим почерком, пользуясь манипулятором "мышь" или графическим планшетом (ввод слова печатными буквами не допускается), далее нажмите кнопку "Добавить образ".



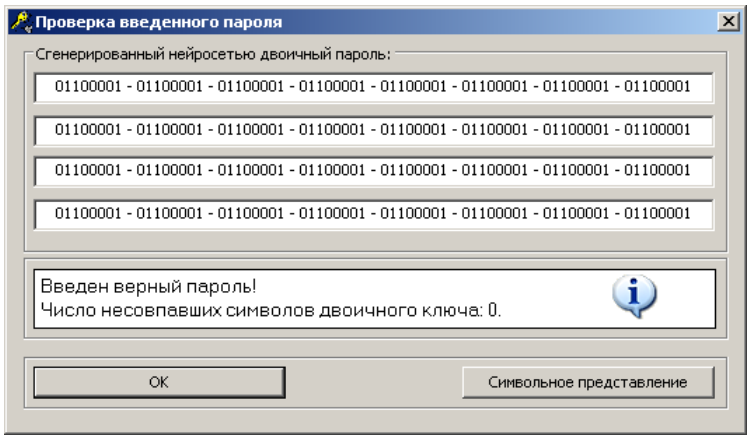
Повторите операцию ввода не менее 8 раз. Рукописные образы нужно писать быстро, опираясь на имеющиеся у вас подсознательные рефлексы, выработанные много лет назад на уроках чистописания.

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

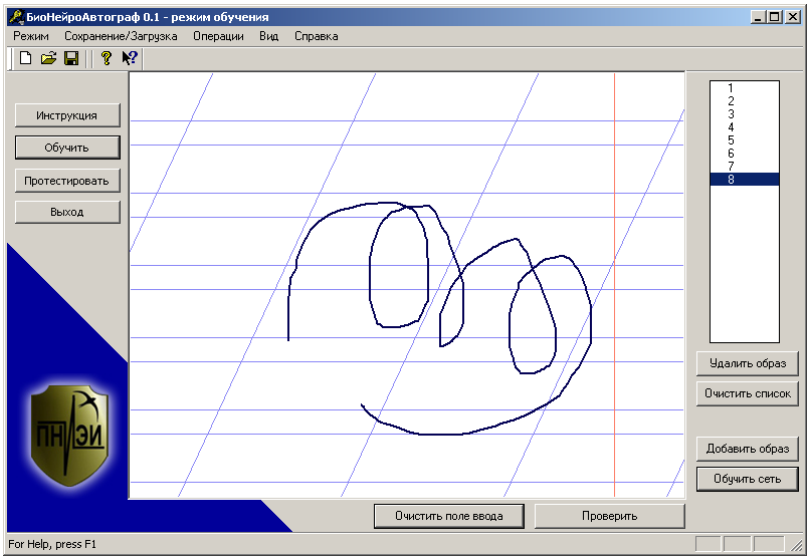


Для закрытия окна нажмите кнопку "ОК".

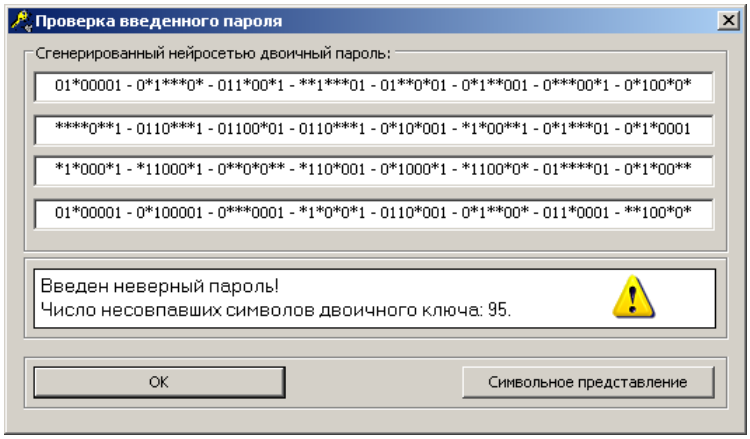
13. Для проверки качества обучения введите контрольный рукописный образ *"пар"* и нажмите кнопку "Проверить". Если средство аутентификации Вас узнает, то появится сообщение "Введен верный пароль!".



14. Воспроизведите попытки атаки, когда "Чужой" не знает правильный пароль. Для этой цели напишите произвольное слово и нажмите "Проверить".



При этом нейронная сеть перестаёт узнавать образ. Убедитесь в этом, рассматривая полученный ключ в двоичной и символьной кодировках.

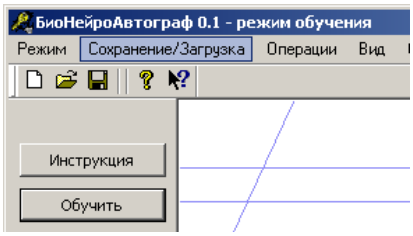


15. Сохраните все обучающие примеры в отдельный файл, выбрав пункт меню "Сохранение/Загрузка" подпункт "Сохранить образы на диск" или нажатием на кнопку с пиктограммой дискеты.

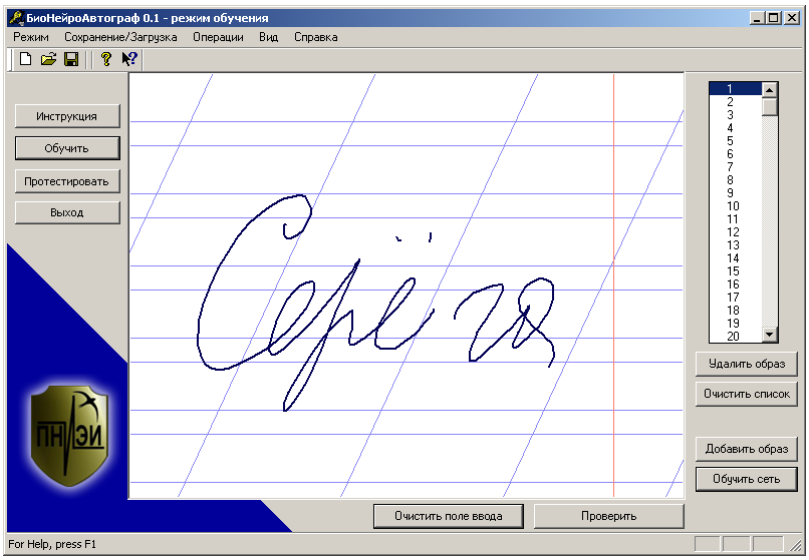
16. Удалите все обучающие примеры из списка, нажав кнопку "Очистить список".

17. Создайте тестовую базу образов "Чужие". Тестовая база должна содержать от 128 до 256 различных рукописных слов. Ввод и добавление тестовых образов в список осуществляется аналогично вводу обучающих образов.

18. Сохраните сформированную тестовую базу (пункт меню "Сохранение/Загрузка" подпункт "Сохранить образы на диск").



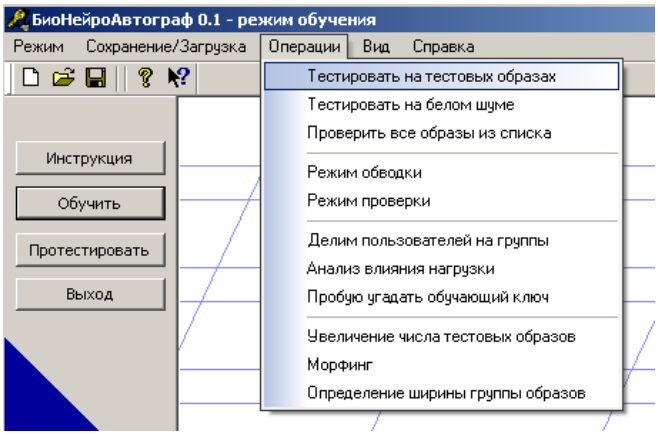
Допускается использование готовой базы образов "все Чужие", созданной совместными усилиями нескольких человек. Загрузка сформированной ранее базы образов осуществляется с помощью подпункта "Загрузить образы с диска" меню "Сохранение/Загрузка". В появившемся диалоговом окне необходимо выбрать файл с образами, например, "256_ВСЕ_ЧУЖИЕ.dat". Загруженные примеры рукописных слов отображаются в списке.



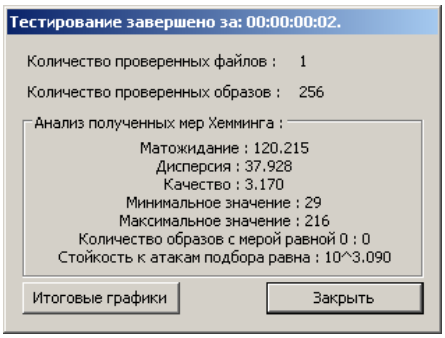
19. Выберите один из загруженных примеров, щёлкнув по его номеру "мышкой" в списке образов. Проверьте насколько выбранный образ отличается от обучающих, нажав на кнопку "Проверить".

20. Для ускоренного тестирования обученной нейронной сети на загруженных образах выберите режим проверки, установив галочку возле подпункта "Режим проверки" пункта меню "Операции".

21. Оцените стойкость к атакам подбора биометрическими образами, имеющими коррелированные данные (все реальные биометрические образы имеют сильно коррелированные данные). Для этого необходимо запустить тестирование на тестовых образах (пункт меню "Операции" подпункт "Тестировать на тестовых образах") и в появившемся окне указать путь к файлу с тестовыми образами.

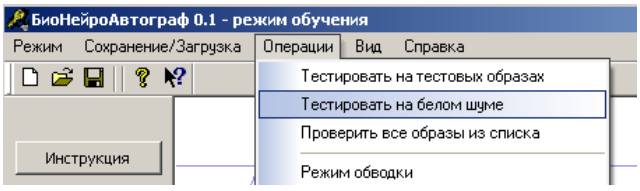


После завершения тестирования выводится диалоговое окно с результатами.

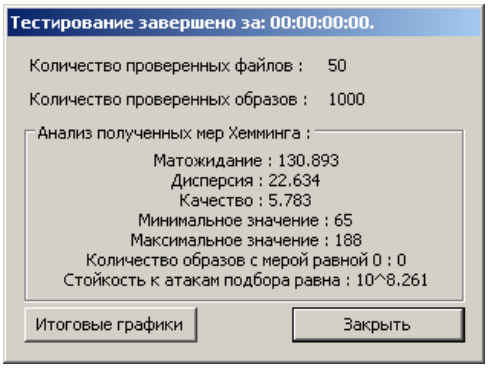


Из экранной формы видно, что на случайных образах с зависимыми биометрическими данными значение стойкости преобразователя биометрия-код к атакам подбора равно $10^{3.09}$.

22. Оцените стойкость к атакам подбора биометрическими образами, имеющими некоррелированные данные (на "белом шуме"), полученными от встроенного программного генератора случайных чисел. Для этого необходимо запустить тестирование на белом шуме (пункт меню "Операции" подпункт "Тестировать на белом шуме").



После завершения тестирования выводится диалоговое окно с результатами.



Из экранной формы видно, что на случайных образах с независимыми биометрическими данными значение стойкости преобразователя биометрия-код к атакам подбора равно $10^{8.261}$.

23. Повторите тестирование преобразователя биометрия-код на зависимых и независимых биометрических данных, обученного на других биометрических образах, например, "*вар*", "*дар*", "*шар*", "*рар*". Полученные данные запишите в таблицу 1.

Таблица №1.

N	Биометрический образ	Стойкость к атакам подбора на белом шуме	Стойкость к атакам подбора на реальных биометрических образах с сильно зависимыми или сильно коррелированными данными
1	*"пар"*	$10^{8.261}$	$10^{3.090}$
2	*"вар"*	$10^{6.452}$	$10^{2.611}$
3	*"дар"*	$10^{9.443}$	$10^{3.721}$
4	*"шар"*	$10^{10.443}$	$10^{4.135}$
5	*"рар"*	$10^{7.236}$	$10^{2.892}$

ВЫВОД: Тестирование на совершенно случайных данных, полученных от программного генератора случайных чисел, даёт значительную методическую погрешность, завышающую стойкость к атакам подбора. Следовательно, тестирование стойкости преобразователя биометрия-код необходимо проводить на реальных биометрических образах, имеющих значительно коррелированные данные.