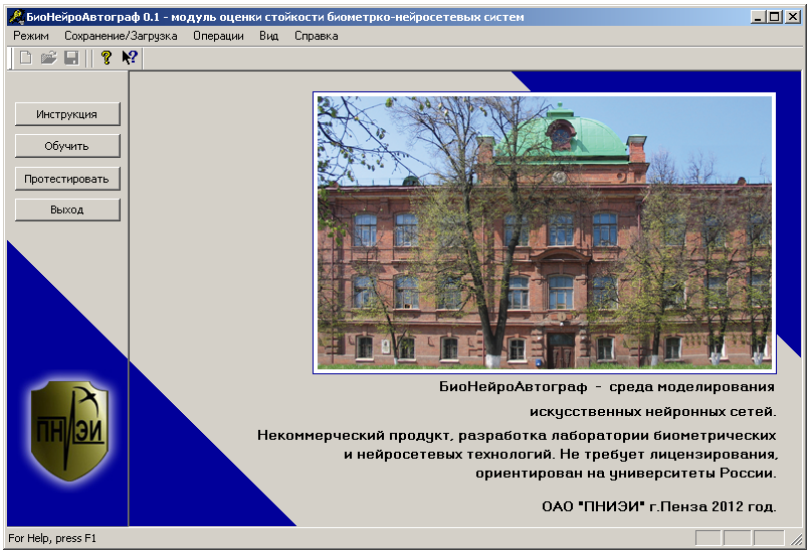
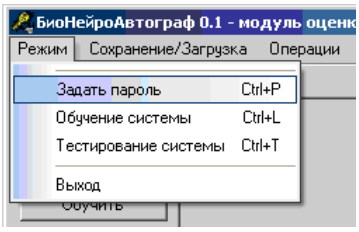
Научно-образовательный центр "Информационная безопасность систем и технологий" ОАО "ПНИЭИ" и ФБГОУ ВПО "Пензенского государственного университета"

Лабораторная работа №5 "Оценка стойкости к атакам подбора частично и полностью скомпрометированного рукописного пароля"

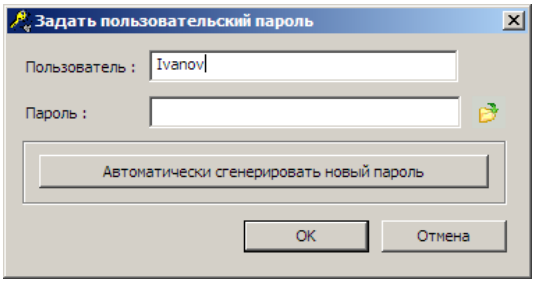
1. Подключите к ПЭВМ графический планшет любой фирмы, установите драйвера графического планшета. Запустите среду моделирования "БиоНейроАвтограф" (файл БиоНейроАвтограф.exe), при этом появится главное диалоговое окно программы.



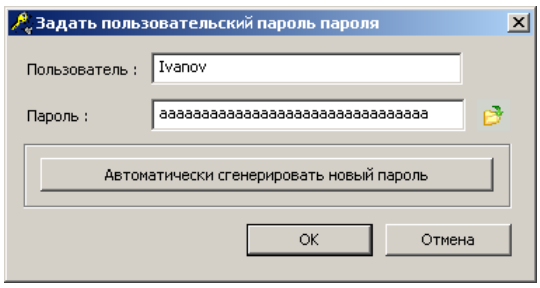
2. Выберите пункт меню "Режим".
3. Выберите режим "Задать пароль".



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

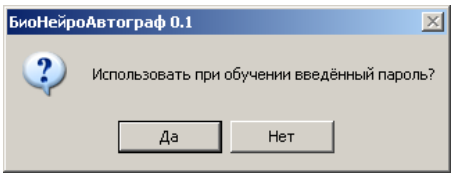


5. Далее в поле "Пароль" задайте пароль из 32-х символов "*aaaaaa…aaaaaa*". Пароль вводится в латинской кодировке клавиатуры.

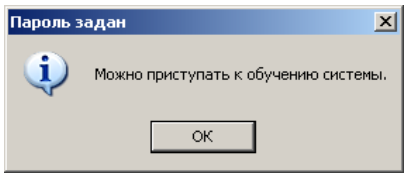


6. Далее нажмите "ОК".

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



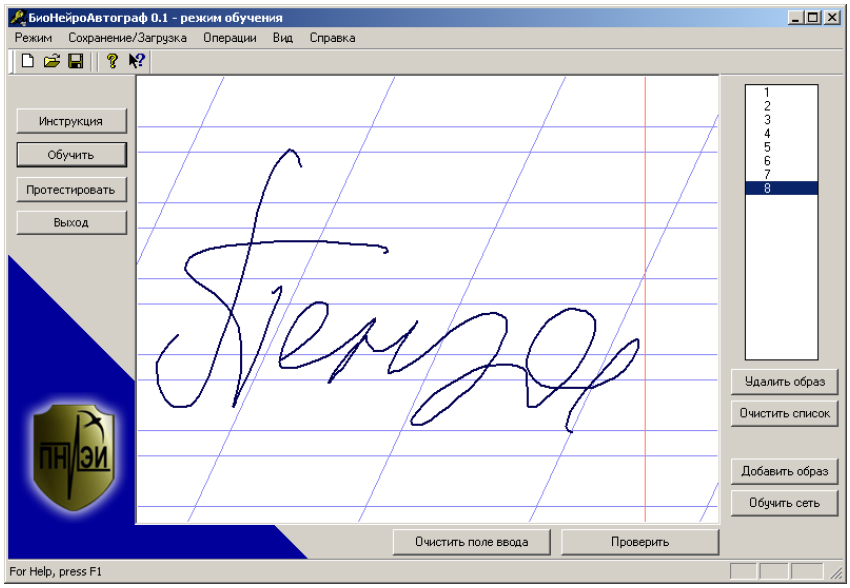
8. Если все пользовательские данные сохранены успешно, то появится сообщение об успешном создании пароля. Нажмите "ОК".



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

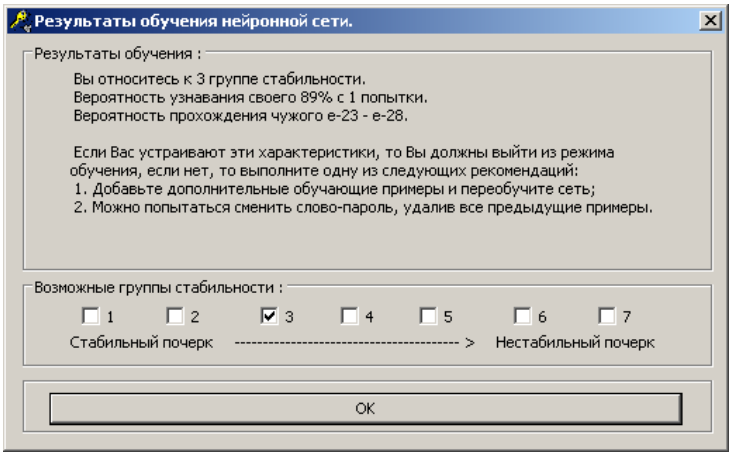
10. Появится диалоговое окно обучения с разлинованным полем ввода рукописных символов/слов. Рукописное слово-пароль вводить с помощью графического планшета.

11. В поле ввода введите один пример рукописного слова-пароля "*Пенза*" своим почерком (ввод слова печатными буквами не допускается), далее нажмите кнопку "Добавить образ".



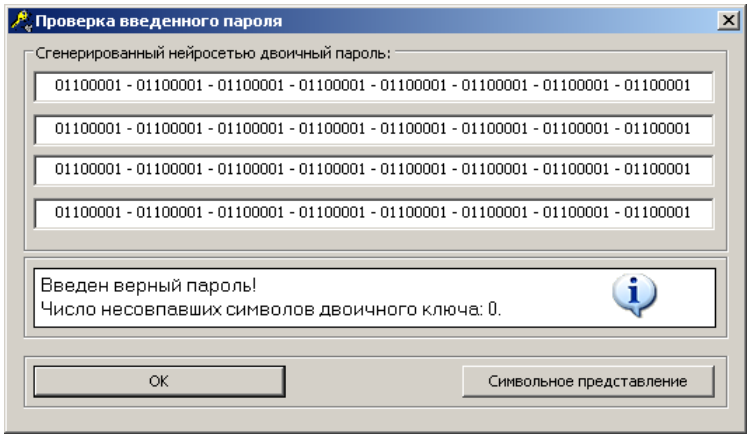
Повторите операцию ввода не менее 8 раз. Рукописные образы нужно писать быстро, опираясь на имеющиеся у вас подсознательные рефлексы, выработанные много лет назад на уроках чистописания.

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

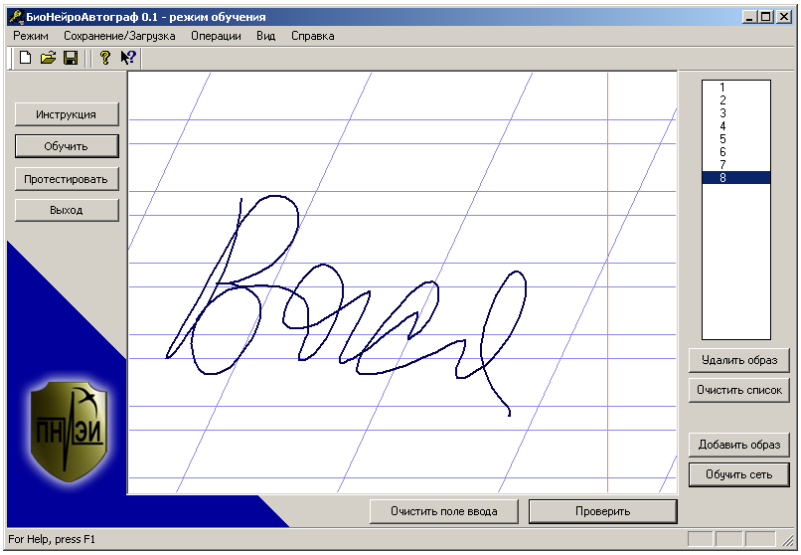


Для закрытия окна нажмите кнопку "ОК"

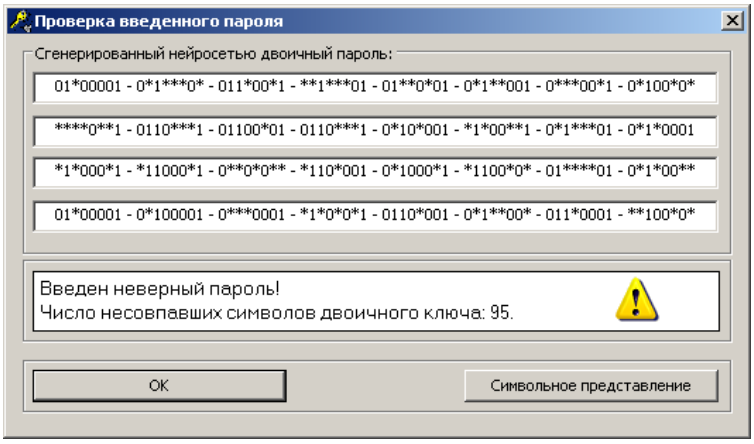
13. Для проверки качества обучения введите контрольный рукописный образ *"Пенза"* и нажмите кнопку "Проверить". Если средство аутентификации Вас узнает, то появится сообщение "Введен верный пароль!".



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



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

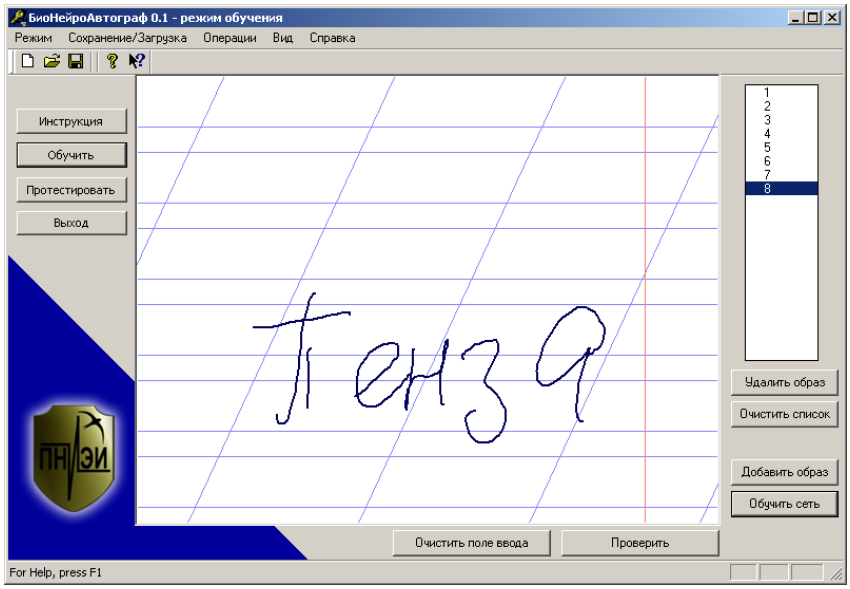


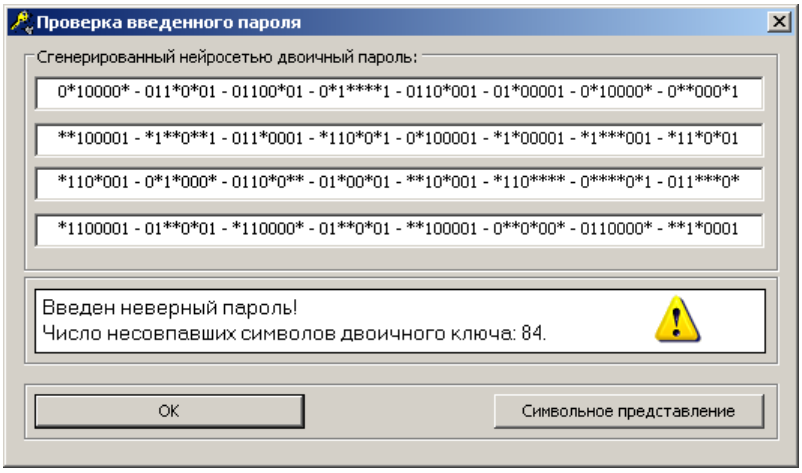
15. Введите слова: "*Серёга*", "*Ольга*", "*Толя*", "*Надя*", "*Яна*", "*Лука*", "*Саша*", "*Даша*", "*Маша*", "*Каша*". Данные о расстоянии Хэмминга внесите в таблицу 1.

Таблица 1.

Мера Хемминга h	95	141	107	132	98	125
	124	152	129	151	111	122
Математическое ожидание E(h)	123,9					
Стандартное отклонение б(h)	18					
Качество q = E(h) / б(h)	123,9 / 18=6,88					
Интеграл Лапласа $\Phi_0(q)$	$\frac{1}{1\cdot\sqrt{2\pi}}\cdot\int_0^{6,88} e^{\frac{-x^2}{2}}\,dx = 0,499999999997008$					
Вероятность ошибки второго рода $P2=0,5-\Phi_0(q)$	0,5 – 0,499999999997008=0,000000000003					

16. Повторите испытание, исходя из того, что злоумышленник знает парольное слово, но не знает почерк донора биометрии "Свой". Для этого пригласите другого студента и попросите его написать слово "*Пенза*" 12 раз его почерком:





Сведите полученные данные в таблицу 2.

Таблица 2.

Мера Хемминга h	84	67	100	52	34	67
	109	61	98	31	69	42
Математическое ожидание E(h)	67,9					
Стандартное отклонение б(h)	24,7					
Качество q = E(h) / б(h)	67,9 / 24,7=2,749					
Интеграл Лапласа $\Phi_0(q)$	0,497011130688845					
Вероятность ошибки второго рода P2=0,5 – $\Phi_0(q)$	0,0029888693112 ≈ 0,003					

17. Сравните данные таблицы 1 и таблицы 2.

ВЫВОД: даже частичная компрометация рук
описного пароля катастрофически снижает его стойкость к атакам подбора. Стойкость к атакам подбора уменьшается в 10 000 000 раз (в десять миллионов раз).

18. Воспроизведите ситуацию полной компрометации рукописного пароля. Для этой цели попросите донора биометрии написать на бумаге рукописное слово, которое использовалось при обучении. Далее наложите бумагу на графический планшет и осуществите быстрый обвод рукописного образа и нажмите "Проверить". Повторите данные манипуляции по обводу нарисованного слова 12 раз и запишите полученные меры Хемминга в таблицу 3. Необходимо отметить, что обводить обучающий образ должен не донор биометрии, а другой человек.

Таблица 3.

Мера Хемминга h	27	14	39	11	5	34
	21	74	18	53	8	31
Математическое ожидание E(h)	27,9					
Стандартное отклонение б(h)	19,3					
Качество q = E(h) / б(h)	27,9 / 19,3=1,4					
Интеграл Лапласа $\Phi_0(q)$	0,419243340766229					
Вероятность ошибки второго рода P2=0,5 – $\Phi_0(q)$	0,5 – 0,419 = 0,081					

ВЫВОД: Полная компрометация рукописного пароля приводит к практически полной утрате его стойкости к атакам подбора. Стойкость снижается до 10 – 20 попыткам атаки подбора.