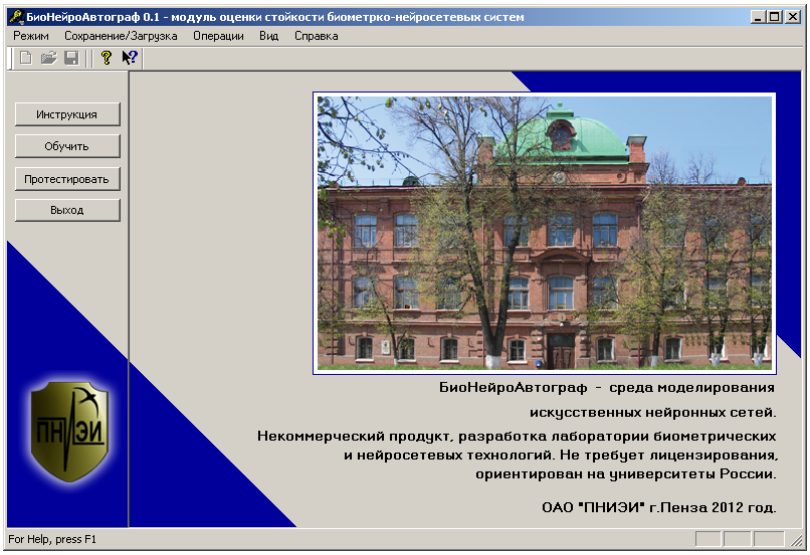
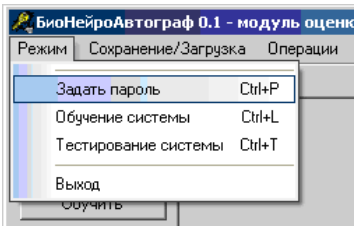
"Пензенский государственный университет"
Кафедра "Информационная безопасность систем и технологий"
Лабораторная работа №2 "Оценка вероятности ошибок второго рода (пропуск "Чужого") по ГОСТ Р 52633.3-2011, использующая статистики расстояний Хэмминга"

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

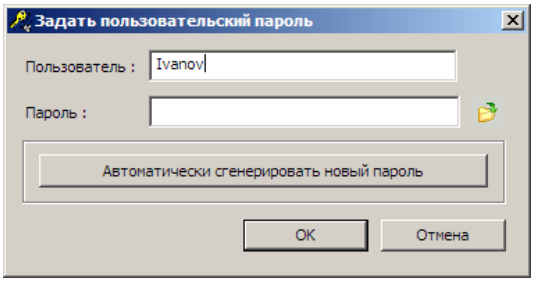


2. Выберете пункт меню "Режим".

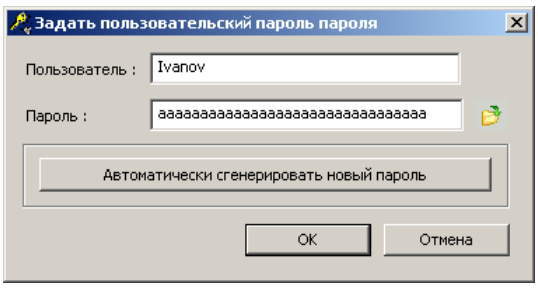


3. Выберите режим "Задать пароль".

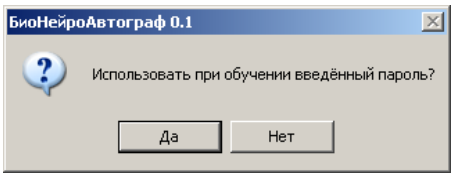
4. В появившейся форме создания пароля в поле "Пользователь" введите свою фамилию либо имя, под которым Вы будете работать в системе.



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

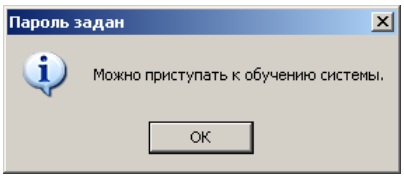


6. Далее нажмите "ОК".



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

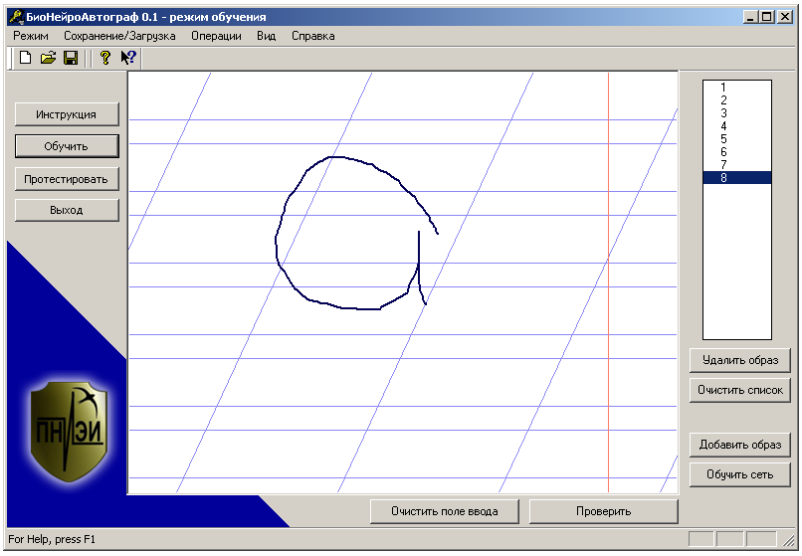
8. Если все пользовательские данные сохранены успешно, то появится сообщение об успешном создании пароля. Нажмите "ОК".



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

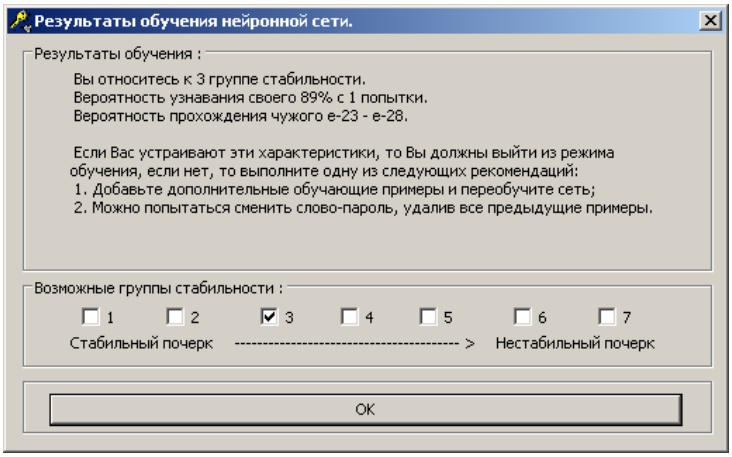
10. Появится диалоговое окно обучения с разлинованным полем ввода рукописных символов/слов. Рукописные слова/символы можно вводить как с помощью графического планшета, так и с помощью стандартной "мышки".

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



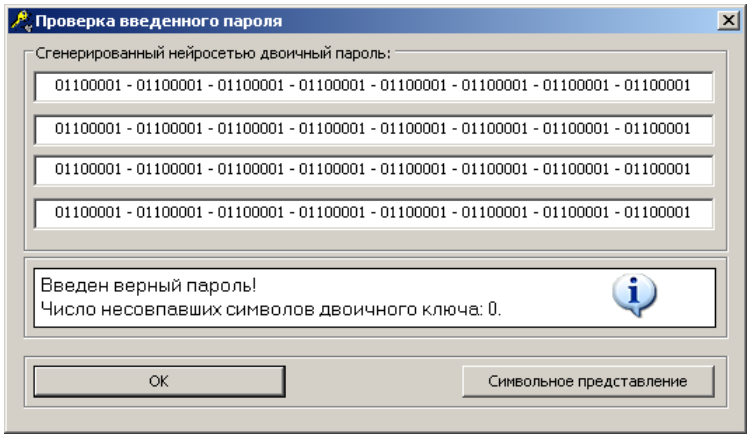
Повторите операцию ввода не менее 8 раз. Рукописные образы нужно писать быстро, опираясь на имеющиеся у вас подсознательные рефлексы, выработанные много лет назад на уроках чистописания.

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.



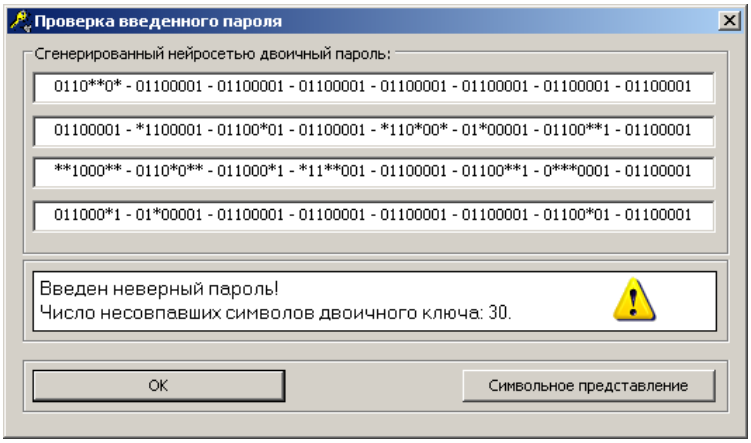
Для закрытия окна нажмите кнопку "ОК"

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



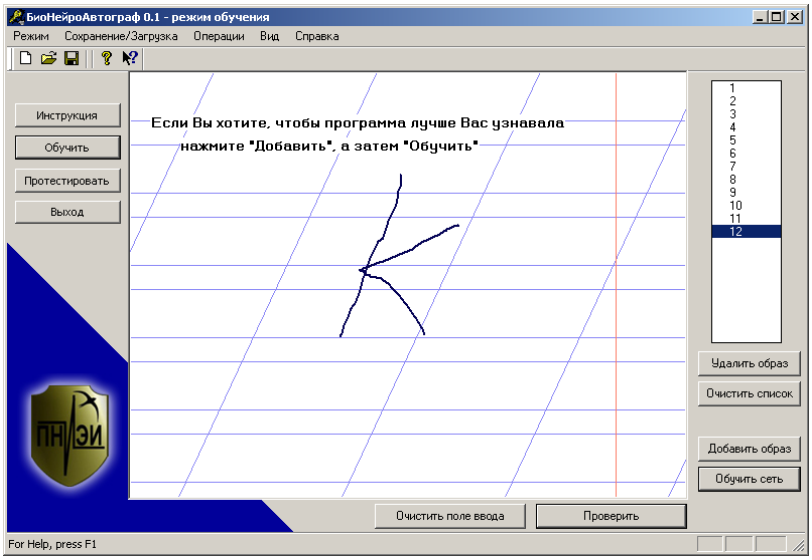
Если средство не узнает своего хозяина, то необходимо его дообучить, увеличив число примеров обучения по п. 11.

14. Проведите тестирование, введя другой рукописный символ, например, символ "*к"*. При этом получается неверный выходной код доступа.



Отображенное на экранной форме число несовпавших символов двоичного ключа (30) является расстоянием Хэмминга между кодом "Свой" рукописного образа *"а"* и кодом "Чужой" рукописного образа *"к"*. Несовпавшие биты отображаются на экранной форме символом "*".

После нажатия кнопки "ОК" появляется сообщение:



Переобучать средство не следует, так как образ "*к*" относится к классу "Чужой".

Для продолжения работы нажмите кнопку "Очистить поле ввода".

15. Соберите статистику, введя другие рукописные символы образов "Чужой" и заполните таблицу 1.

Таблица №1.

Попытка / Образ	Расстояния Хэмминга до образа "*а*"									
	1	2	3	4	5	6	7	8	9	10
"*к*"	30	21	16	52	33	8	41	19	24	64
"*н*"	7	27	6	16	4	5	8	20	11	31
"*у*"	27	82	44	49	21	51	101	111	67	77
"*о*"	21	30	34	26	20	96	19	51	8	10
"*е*"	64	44	56	94	78	101	90	107	103	99

16. По каждой строке таблицы №1 вычислите математическое ожидание E(h) и стандартное отклонение σ(h) расстояний Хэмминга, данные сведите в таблицу 2.

Таблица № 2

Символ	E(h)	σ(h)	$P_{2,"."}$
"*к*"	30.8	16.37	0.037
"*н*"	13.5	9.13	0.085
"*у*"	63.1	28.4	0.054
"*о*"	31.5	24.48	0.106
"*е*"	85.6	23.78	0.0037

17. Располагая данными о математическом ожидании и стандартном отколонении рассчитайте вероятности ошибок второго рода для каждого из использованных рукописных образов " . ", пользуясь гипотезой нормального закона распределения расстояний Хэмминга:

$$P_{2,"."} \approx \frac{1}{\sigma(h)\sqrt{2\pi}} \cdot \int_{-\infty}^{0} \exp\left\{\frac{-(E(h)-u)^2}{2\cdot\sigma^2(h)}\right\} \cdot du \qquad (1).$$

Полученные данные подставьте в четвертый столбец таблицы 2.

18. Вычислите для всех введенных биометрических образов усредненную вероятность ошибки второго рода:

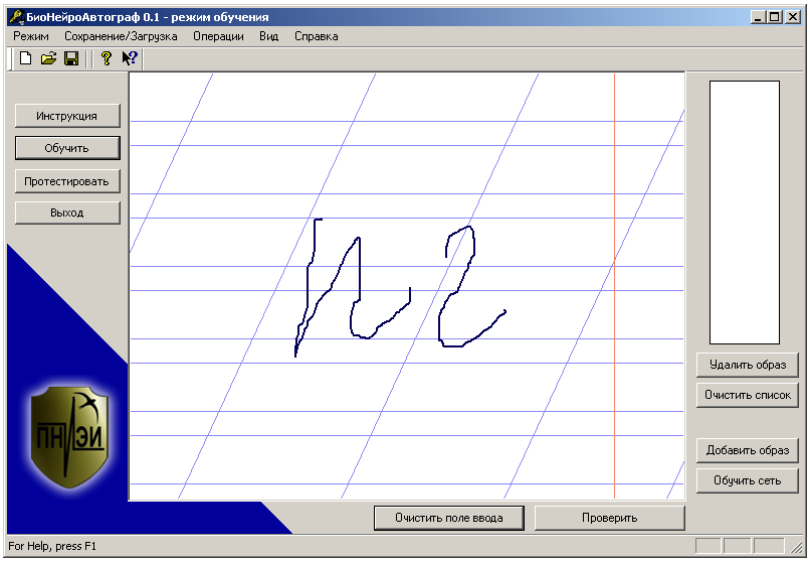
$$P_2 \approx \frac{0.035+0.85+0.054+0.106+0.0037}{5} = 0.057$$

19. Оцените стойкость к атакам подбора как обратную величину усредненной вероятности ошибки второго рода:

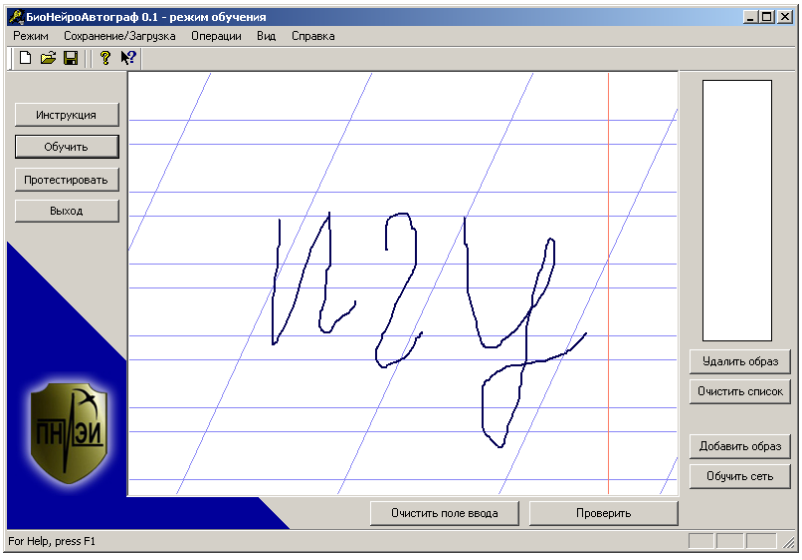
$$(P_2)^{-1} \approx \frac{1}{0.057} = 17.5$$

ВЫВОД: Рукописный биометрический образ "*а*", состоящий из одного символа, воспроизведенный манипулятором "мышь", является очень слабой защитой. Для её преодоления достаточно примерно 17 попыток атаки воспроизведения пароля, если злоумышленник знает, что пароль состоит из одного рукописного символа.

20. Повторите численный эксперимент для ситуации, когда злоумышленник не знает длину рукописного пароля. Для этой цели введите пароль из одной рукописной буквы "*п*", затем пароль из двух рукописных букв "*пг*".



Затем введите пароль из трех рукописных букв "*пгу*".



Полученные данные сведите в таблицу 3.

Таблица 3.

Попытка / Образ	Расстояния Хэмминга до образа "*а*"									
	1	2	3	4	5	6	7	8	9	10
"*п*"	103	31	33	65	133	148	47	111	53	114
"*пг*"	163	135	163	167	141	148	162	152	149	123
"*пгу*"	156	82	71	109	93	91	106	101	108	98

21 Вычислите для данных таблицы 3 математическое ожидание E(h)=112 и стандартное отклонение б(h)=39.4.

22. Вычислите вероятность появления нулевых расстояний Хэмминга по формуле (1):

$$P_2 \approx \frac{1}{39.4\sqrt{2\pi}} \cdot \int_{-\infty}^{0} \exp\left\{\frac{-(112-u)^2}{2\cdot(39.4)^2}\right\} \cdot du = 0.0023$$

2. Вычислите стойкость к атакам подбора:

$$(P_2)^{-1} \approx \frac{1}{0.0023} = 435 \text{ попыток.}$$

ВЫВОД: Если злоумышленник не знает длину рукописного пароля, то для успешной атаки подбора простейшего рукописного пароля из одной буквы ему потребуется осуществить порядка 435 попыток. Время на одну попытку ввода рукописных биометрических данных составляет примерно 10 секунд. Стойкость защиты составляет 4350 секунд или 72 минуты.