1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. —
4. Институт компьютерных наук и технологий
5. **Кафедра «Информационная безопасность компьютерных систем»**

**Расчетное задание №3**

1. по дисциплине
2. «Теория вероятностей и математическая статистика»

Выполнил

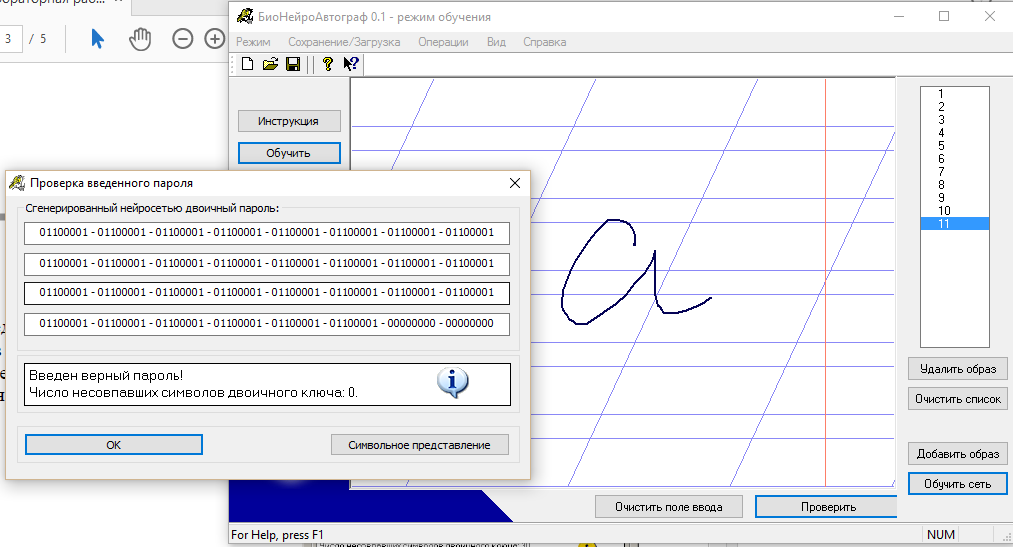
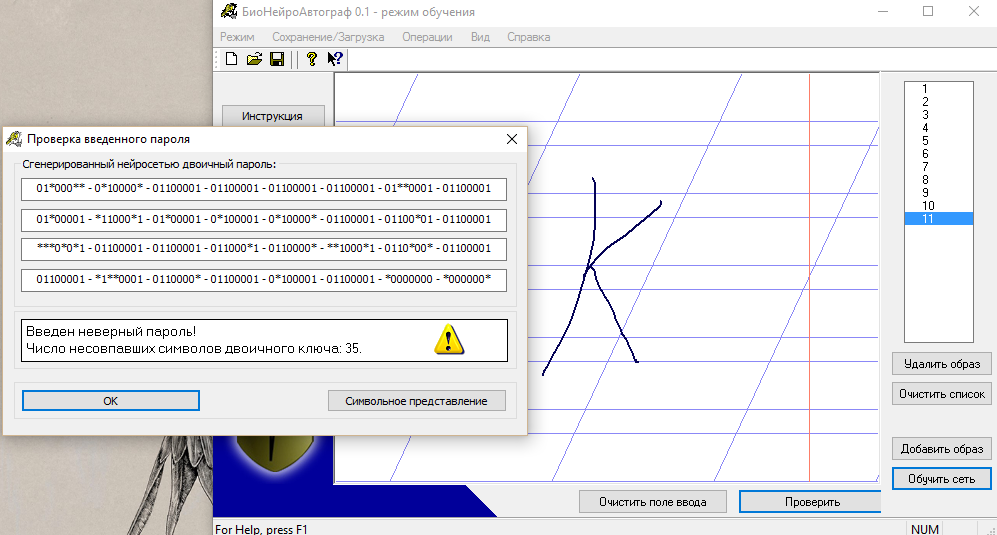
студент гр. 23508/4 Проценко Е.Г.

преподаватель Лаврова Д.С.

1. Санкт-Петербург
2. 2016

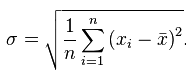
Результаты Работы

# Оценка вероятности ошибок второго рода

1. Сеть была обучена одиннадцатью образами и проверена  
   
2. Проверка другой рукописной буквы (например, ‘к’)  
   
3. Собираем статистику, вводя другие рукописные символы образов “Чужой”

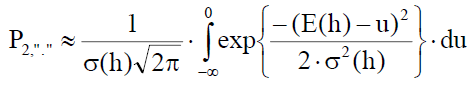
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Расстояния Хэмминга до образа «*а*» | | | | | | | | | | |
| Символ  число  ввода | Попыт-  ка -1 | Попыт-  ка -2 | Попыт-  ка -3 | Попыт-  ка -4 | Попыт-  ка -5 | Попыт-  ка -6 | Попыт-  ка -7 | Попыт-  ка -8 | Попыт-  ка -9 | Попыт-  ка -10 |
| “п” | 9 | 12 | 10 | 15 | 25 | 20 | 8 | 13 | 31 | 23 |
| “л” | 204 | 250 | 250 | 223 | 239 | 241 | 249 | 240 | 241 | 220 |
| “у” | 3 | 6 | 6 | 2 | 4 | 5 | 11 | 5 | 5 | 8 |
| “к” | 53 | 22 | 24 | 9 | 17 | 58 | 19 | 39 | 30 | 28 |
| “ж” | 145 | 96 | 205 | 147 | 104 | 112 | 147 | 187 | 78 | 154 |

1. Вычисление мат ожидания , среднеквадратического отклонения

Для символа “п” .  
Формула для среднеквадратического отклонения

|  |  |  |
| --- | --- | --- |
| Символ |  |  |
| “п” | 16,6 | 7,36 |
| “л” | 235,7 | 14,44 |
| “у” | 5,5 | 2,42 |
| “к” | 29,9 | 14,93 |
| “ж” | 137,5 | 38,15 |

1. Рассчитываем вероятности ошибок второго рода для каждого из использованных рукописных образов по формуле



|  |  |  |  |
| --- | --- | --- | --- |
| Символ |  |  |  |
| “п” | 16,6 | 7,36 | 0,0226267 |
| “л” | 235,7 | 14,44 | 3,18329 \* |
| “у” | 5,5 | 2,42 | 0,0114839 |
| “к” | 29,9 | 14,93 | 0,0226023 |
| “ж” | 137,5 | 38,15 | 0,000156284 |

1. Усредненная вероятность ошибки второго рода
2. Стойкость к атакам подбора

Вывод: для преодоления пароля такого пароля, если злоумышленник знает, что он состоит из одного символа, достаточно приблизительно 88 попыток.

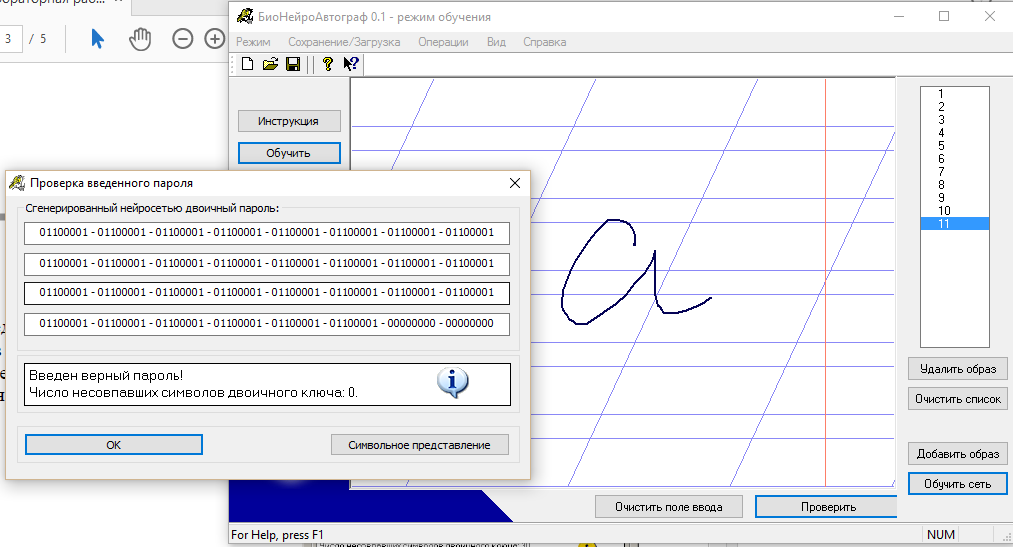
1. Эксперимент для ситуации, когда злоумышленник не знает длину рукописного пароля

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Расстояния Хэмминга до образа «*а*» | | | | | | | | | | |
| Символы | Попытка 1 | Попытка 2 | Попытка 3 | Попытка 4 | Попытка 5 | Попытка 6 | Попытка 7 | Попытка 8 | Попытка 9 | Попытка 10 |
| “г” | 5 | 45 | 14 | 18 | 43 | 98 | 32 | 150 | 37 | 39 |
| “гд” | 83 | 132 | 149 | 119 | 149 | 121 | 148 | 118 | 161 | 35 |
| “где” | 140 | 106 | 127 | 133 | 148 | 121 | 127 | 114 | 115 | 153 |

1. Вычисляем по таблице математическое ожидание и среднеквадратичное отклонение , вероятность появления нулевых расстояний Хэмминга.
2. Вычисляем стойкость к атакам подбора:

Вывод: Если злоумышленник не знает длину рукописного пароля, то для успешной атаки подбора простейшего рукописного пароля из одной буквы ему потребуется осуществить порядка 472 попыток. Время на одну попытку ввода рукописных биометрических данных составляет 10 секунд. Стойкость защиты составляет 4720 секунд или 79 минут.

# Оценка вероятности ошибок первого рода

1. Сеть была обучена одиннадцатью образами и проверена  
   
2. Ввод рукописного символа “а” 50 раз.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Расстояния Хэмминга до образа «*а*» | | | | | | | | | | |
| Символ | Попытка 1 | Попытка 2 | Попытка 3 | Попытка 4 | Попытка 5 | Попытка 6 | Попытка 7 | Попытка 8 | Попытка 9 | Попытка 10 |
| “a” | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| “a” | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| “a” | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 |
| “a” | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| “a” | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

1. Вероятность ошибок первого рода по обычной формуле для 10, 20, 30, 40 и 50 опытов

;

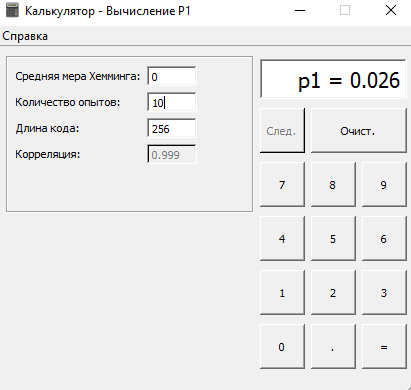
;

;

.1;

;

1. Вычисляем математическое ожидание расстояний Хэмминга для 10, 20, 30, 40 и 50 опытов
2. Вычисление определенного интеграла распределения хи-квадрат расстояний Хэмминга.



Вероятность по обычной формуле дает более нестабильные результаты (с большим разбросом)

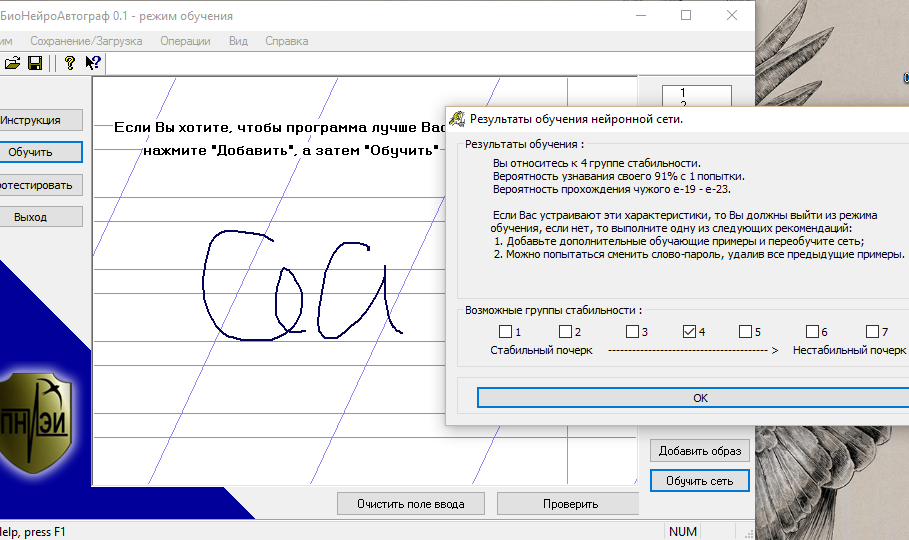
1. Проделываем еще 50 испытаний

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Расстояния Хэмминга до образа «*а*» | | | | | | | | | | |
| Символ | Попытка 1 | Попытка 2 | Попытка 3 | Попытка 4 | Попытка 5 | Попытка 6 | Попытка 7 | Попытка 8 | Попытка 9 | Попытка 10 |
| “a” | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 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 | 1 | 0 | 0 | 0 | 0 | 0 |
| “a” | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

1. Вероятность ошибок для всех 100 испытаний

Вывод: вероятность ошибок первого рода , полученная по калькулятору оказалась точнее.

1. Переучиваем средство аутентификации на два вводимых подряд рукописных символа “аа”

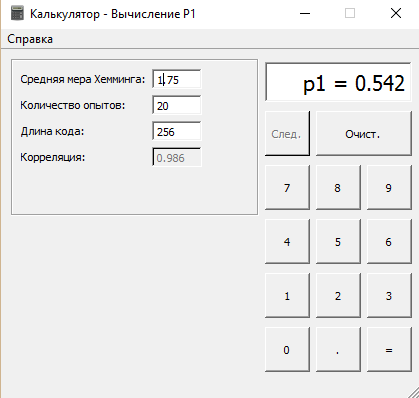


1. Вводим 20 раз рукописный образ из двух символов

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Расстояния Хэмминга до образа «*аа*» | | | | | | | | | | |
| Символ | Попытка 1 | Попытка 2 | Попытка 3 | Попытка 4 | Попытка 5 | Попытка 6 | Попытка 7 | Попытка 8 | Попытка 9 | Попытка 10 |
| “аа” | 2 | 1 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| “аа” | 0 | 6 | 0 | 1 | 5 | 0 | 4 | 0 | 6 | 0 |

1. Вероятность ошибки первого рода по обычной формуле
2. Вероятность ошибки первого рода, пользуясь хи-квадрат распределением.

Математическое ожидание



1. Усилим средство аутентификации дополнительно введя 4 образа “аа”. И повторим пункты 9)-12).

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Расстояния Хэмминга до образа «*аа*» | | | | | | | | | | |
| Символ | Попытка 1 | Попытка 2 | Попытка 3 | Попытка 4 | Попытка 5 | Попытка 6 | Попытка 7 | Попытка 8 | Попытка 9 | Попытка 10 |
| “аа” | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| “аа” | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

1. Вероятность ошибки первого рода по обычной формуле
2. С использование хи-квадрат распределения

