Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

Кафедра защиты информации

А. М. Прудник

АУТЕНТИФИКАЦИЯ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

методические указания к выполнению лабораторной работы по курсу
«Биометрические системы контроля доступа и
защиты информации в телекоммуникациях»
по специальностям 1–45 01 03 «Сети телекоммуникаций» и
1–45 01 05 «Системы распределения мультимедийной информации» и
«Биометрические системы контроля доступа в сетях телекоммуникаций»
по специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2015

Содержание

1. Цель работы

Изучить основные принципы аутентификации по клавиатурному почерку.

2. Теоретическая часть

Клавиатурный почерк относится к динамическим (поведенческим) биометрическим характеристикам, описывающим подсознательные действия, привычные для пользователя. Он характеризует динамику ввода парольной фразы с помощью клавиатуры. Стандартная клавиатура позволяет измерить следующие временные характеристики: время удержания клавиши нажатой и интервал времени между нажатиями клавиш.

Клавиатурный почерк могут характеризовать и другие параметры, описанные в работе [1]:

– общее время набора парольной фразы;

– частота возникновения ошибок при наборе;

– факт использования дополнительных клавиш (использование числовой клавиатуры);

– особенности ввода заглавных букв (использование клавиши Shift или Caps Lock) и т.д.

Использование клавиатурного почерка не требует установки специальных аппаратных средств и кадров для установки и поддержки, является прозрачным для конечного пользователя, т. е. не причиняет неудобств пользователю и позволяет проводить скрытую аутентификацию. Клавиатурный почерк также позволяет проводить реаутентификацию для подтверждения личности пользователя перед выполнением критичных операций. Кроме того, клавиатурный почерк обладает всеми преимуществами, присущими биометрическим методам аутентификации и описанными в работе [2].

Согласно работе [3], основные сложности в работе с клавиатурным почерком связаны с большим разнообразием навыков набора у пользователей и влиянием физиологических состояний человека на почерк: сонливости, тревоги, плохого самочувствия и т. п. На ритм ввода могут влиять и другие объективные причины: травма кисти или пальцев руки или устройство ввода нестандартного размера, обладающего другой эргономичностью. Все эти факторы должны быть учтены для обеспечения точной и эффективной работы системы аутентификации.

Системы идентификации по клавиатурному почерку основаны на вводе фиксированного слова, но предположительно они могут быть и независимыми от набираемого текста, как системы распознавания голоса.

Уже существуют и коммерческие продукты, основанные на подсчете времени набора текста.

В одной из исследовательских работ предлагается метод идентификации по клавиатурному почерку на основе сменных виртуальных клавиатур. Суть метода заключается в следующем.

При коллективной работе в автоматизированных информационно-управляющих системах каждому оператору предоставляется своя персональная виртуальная клавиатура, отображаемая на экране его компьютера. Вид и состав этой клавиатуры может быть произвольным, например таким же, как и стандартной, но расположение клавиш на клавиатуре отличается для каждого оператора. Вид клавиатуры генерируется системой либо из заранее подготовленного списка, либо на основе реализации некоторого алгоритма, либо случайно. Каждый оператор должен в течение достаточно длительного времени работать на «своей» виртуальной клавиатуре, предоставленной ему системой. Набор символов на виртуальной клавиатуре может выполняться путем перемещения курсора на экране одним из двух способов:

– мышью – нажатием соответствующих виртуальных клавиш кнопкой мыши;

– пятью клавишами на реальной клавиатуре компьютера (стрелки вверх, вниз, вправо, влево, ввод).

Оператор, достаточно длительное время работающий на «своей» виртуальной клавиатуре, приобретает индивидуальные навыки, которые выражаются в определенной картине скоростей ввода отдельных символов и текста в целом. В такой ситуации попытки подмены оператора хорошо идентифицируются системой анализа клавиатурного почерка.

С целью апробации предлагаемого метода была разработана программная тестовая модель системы клавиатурного мониторинга. Для ввода текста использовалась программно изменяемая

виртуальная клавиатура, содержащая все алфавитно-цифровые и основные функциональные клавиши, обычно используемые в стандартных клавиатурах.

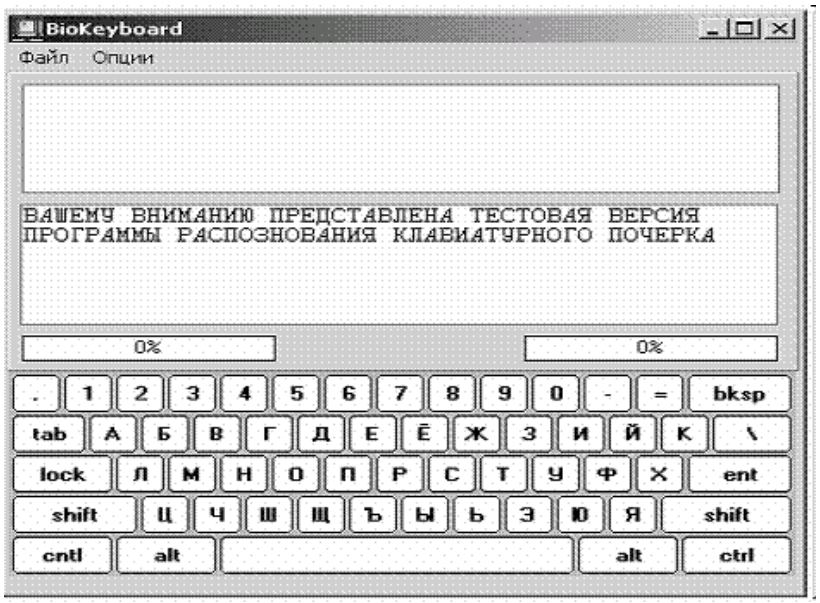

Рисунок 1. Интерфейс программной модели системы клавиатурного мониторинга

Работа с виртуальной клавиатурой осуществлялась с помощью компьютерной мыши. При постановке эксперимента в модели были использованы две виртуальные клавиатуры №1 и №2. Расположение клавиш клавиатуры №1 совпадает с расположением клавиш стандартной компьютерной клавиатуры. В клавиатуре №2 алфавитные клавиши расположены в порядке следования букв в алфавите.

В верхней части интерфейса (рис. 3.2) имеются два текстовых окна. В нижнем окне отображается текст, который необходимо ввести, а в верхнем – текст, который реально вводится.

Над цифровой частью виртуальной клавиатуры имеются два окна: левое показывает текущее число введенных символов текста (в процентах), правое – текущее число допущенных ошибок относительно эталона (в процентах).

Для тестирования системы была использована следующая методика:

– на первом этапе после некоторой тренировки на клавиатуре №2 пользователю «свой» предлагалось ввести на этой клавиатуре некоторый произвольный осмысленный текст, состоящий из 10–15 предложений. По результатам ввода формировался биометрический эталон пользователя «свой»;

– на втором этапе пользователь «свой» проверял работоспособность системы и при необходимости изменял точность аутентификации;

– на третьем этапе система тестировалась для пользователя «чужой». В качестве «чужого» использовался другой пользователь, имеющий хорошие навыки работы на стандартной клавиатуре. Этому пользователю предлагалось вводить тот же текст, используя клавиатуру пользователя «свой», т.е. клавиатуру №2. Предполагалось, что для «чужого» ввод с другой клавиатуры будет затруднен.

В результате тестирования система успешно разделяла пользователей «свой» и «чужой». Во время работы «своего» ошибка изменялась от 2 до 15 %. Для «чужого» интервал изменения ошибки аутентификации составил 70–100 %.

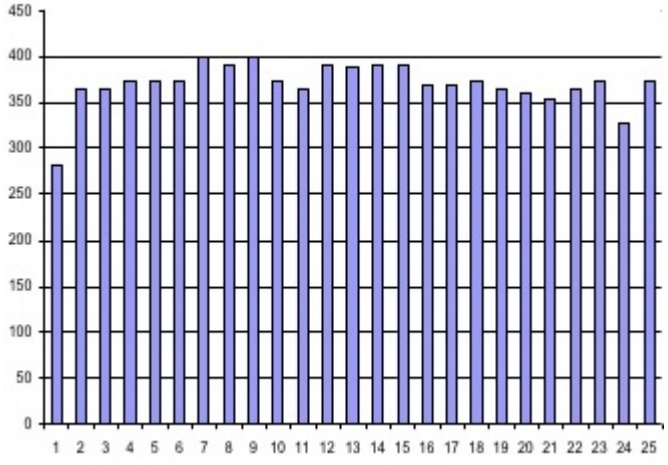

Рисунок 1. Двадцать пять испытаний скорости ввода парольной фразы

Для тестирования возможностей аутентификации посредством клавиатурного почерка воспользовались простой самописной программой. Придумаем некоторую парольную фразу, которую заставим многократно вводить испытуемых (в нашем случае, парольная фраза — «апельсинка»).

Скорость ввода в течении одного вечера будет варьироваться в некоторых приделах. Используя полученную статистику мы получим некоторое математическое ожидание, ожидание скорости и ее дисперсию.

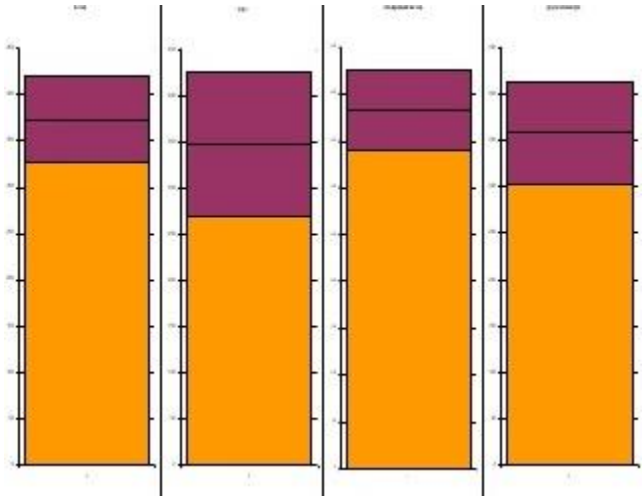

Рисунок 2. Математическое ожидание и дисперсия скорости в различное время суток

Проведя аналогичные испытания в других психофизических состояниях мы получим мат.ожидание и дисперсию и для них.

На рисунке слева показаны состояния:

– первый столбик — вечер (только написал программу);

– второй столбик — утро (только проснулся);

– третий столбик — другой вечер;

– четвертый столбик — другая клавиатура.

Теперь необходимо сравнить результаты тестов скорости с другими испытуемыми.

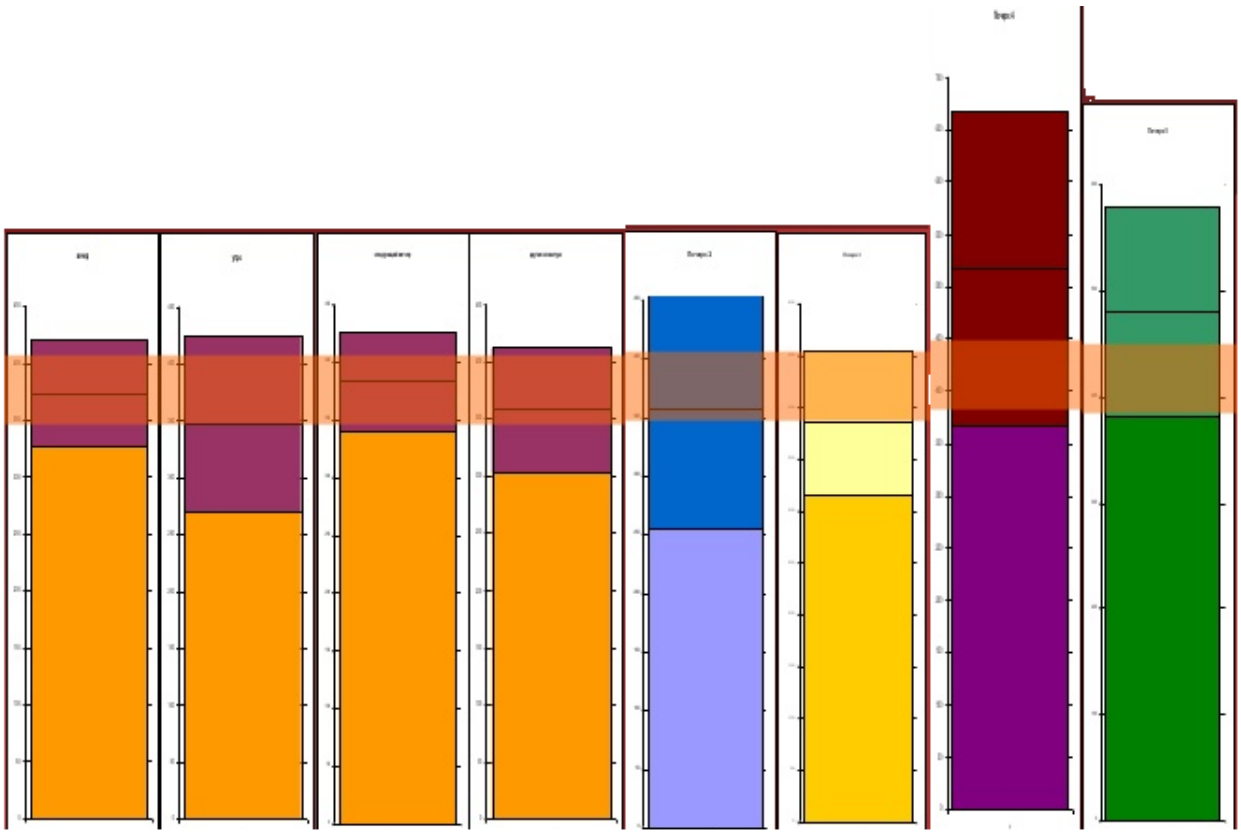

Рисунок 3. Результаты сравнения тестов скорости с другими испытуемыми

Несмотря на различия в скорости печатания всех испытуемых, существует диапазон скоростей в котором все они могли напечатать парольную фразу (рисунок справа). Поэтому, помимо скорости для уменьшения количества ложных срабатываний потребуется воспользоваться другими характеристиками клавиатурного почерка, а точнее динамикой ввода парольной фразы.

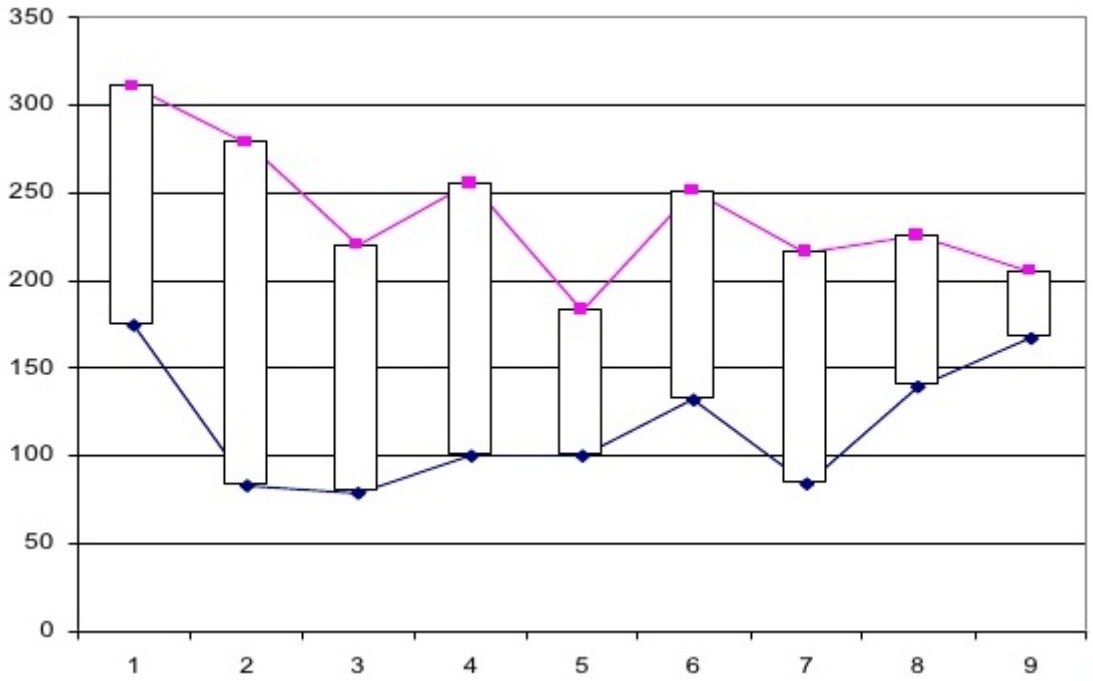

Рисунок 4. Результаты сравнения тестов скорости с другими испытуемыми

На рисунке 4 справа высота прямоугольников описывает интервалы времени между нажатиями соседних символов в парольной фразе «апельсинка».

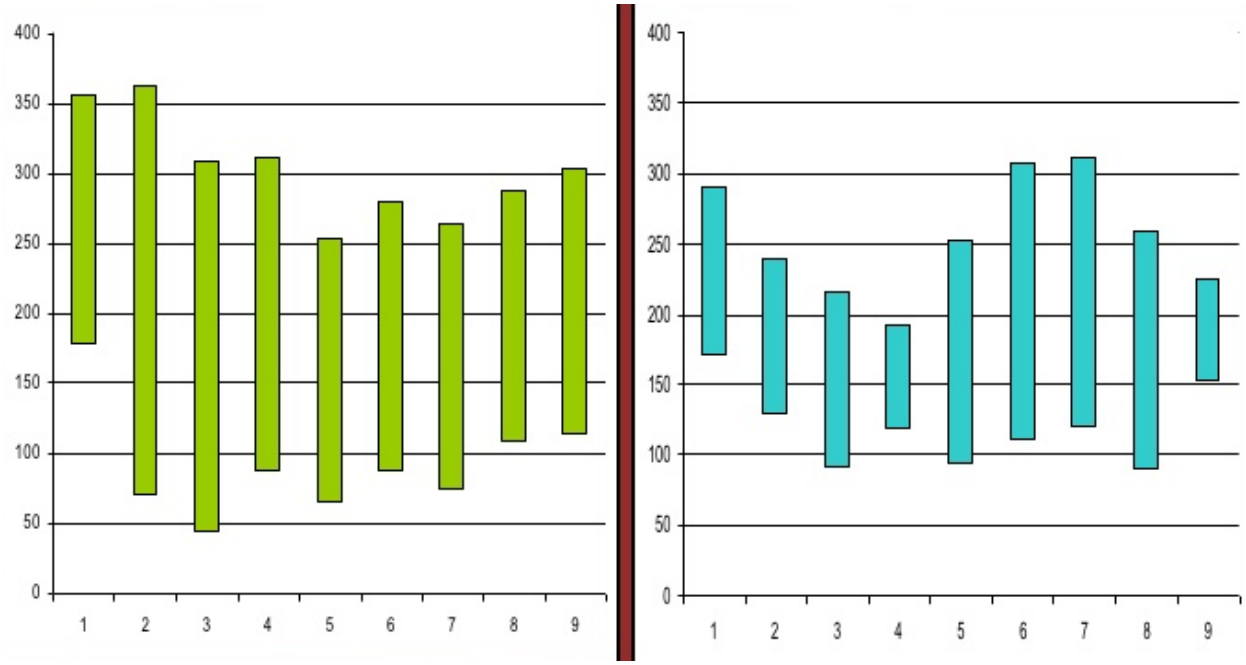

Рисунок 5. А —Другое состояние Hbceyjr Lheujt cjnjzybt

Сравним с другими состояниями:

Использование другой клавиатуры и ввод парольной фразы в состоянии «только что проснулся» приводят к значительным изменениям динамики ввода, поэтому для уменьшения ложных отказов в доступе требуется использование той же самой клавиатуры, а аутентификацию осуществлять с учетом времени суток, когда оная происходит.

Теперь сравним динамику ввода разных испытуемых:

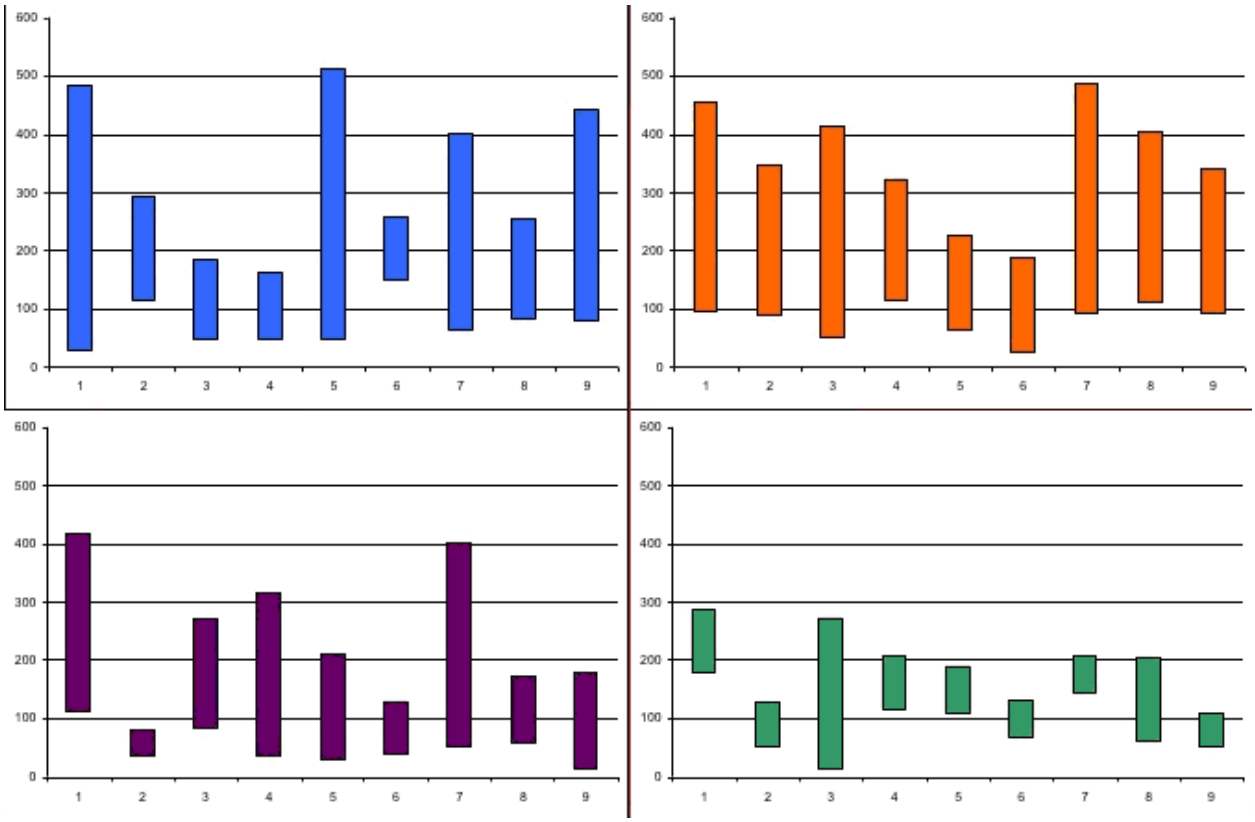

Рисунок 6. Динамика ввода испытуемых *t* (*N*, 31–*p*)

Наложением графиков динамики ввода друг на друга мы получим, опять же, что существует вероятность совпадения динамик различных испытуемых, но эта вероятность уже значительно ниже чем при учете только скорости ввода.

Преимущества клавиатурного почерка для аутентификации. Простота реализации и внедрения. Реализация исключительно программная, ввод осуществляется со стандартного устройства ввода (клавиатуры), а значит использование не требуется приобретение никакого дополнительного оборудования. Это самый дешевый способ аутентификации по биометрическим характеристикам субъекта доступа.

Не требует от пользователя никаких дополнительных действий, кроме привычных. Пользователь так или иначе, наверняка, использует пароль, который можно назначить парольной фразой, по которой будет проводиться аутентификация.

Возможность скрытой аутентификации — пользователь даже может быть не в курсе, что включена дополнительная проверка, а значит не сможет об этом сообщить злоумышленнику.

Недостатки клавиатурного почерка для аутентификации. Требуется обучение приложения.

Сильная зависимость от эргономичности клавиатуры (в случае смены, придется обучать программу заново).

Сильная зависимость от психофизического состояния оператора. Если человек заболел, то он вполне вероятно не сможет аутентифицироваться (с другой стороны может и не стоит этого делать в больном состоянии).

3. Ход работы

Работа выполняется совместно двумя студентами.

1. Запустить файл *index* в браузере Mozilla Firefox.

2. Аутентификация при постороннем наблюдении.

2.1. 1-й студент должен произвести регистрацию в системе посредством набора парольного слова из восьми букв. 2-й студент должен наблюдать за динамикой клавиатурного набора.

2.2. 2-й студент, который знает пароль и наблюдал за динамикой клавиатурного набора должен аутентифицироваться в системе (10 попыток).

2.3. По результатам аутентификации заполнить таблицы 1, 2. В таблицу 2 внести данные только по одной удачной и неудачной попытке. Таблицу 2 сделать для двух пользователей. Произвести расчет ошибок 1-го (коэффициент ложного доступа) и 2-го родов (коэффициент ложного отказа в доступе).

Таблица 1. Общая статистика аутентификации пользователей

Имя пользователя	Количество			Общее количество	Коэффициент ложного доступа	Коэффициент ложного отказа в доступе
	удачного ввода пароля	неверного ввода пароля	неверного клавиатурного подчерка			

Таблица 2. Общая статистика аутентификации пользователей

Номер попытки	Клавишный интервал	Эталон	Измеренный	Дельта, %

3. Аутентификация без постороннего наблюдения.

3.1. 1-й студент должен произвести регистрацию в системе посредством набора парольного слова из восьми букв. 2-й студент не должен наблюдать за динамикой клавиатурного набора.

3.2. 2-й студент, который знает пароль, но не наблюдал за динамикой клавиатурного набора должен аутентифицироваться в системе (10 попыток).

3.3. 1-й студент, который помнит свой пароль должен аутентифицироваться в системе (10 попыток).

3.4. По результатам аутентификации заполнить таблицы 1, 2. В таблицу 2 внести данные только по одной удачной и неудачной попытке. Таблицу 2 сделать для двух пользователей. Произвести расчет ошибок 1-го (коэффициент ложного доступа) и 2-го родов (коэффициент ложного отказа в доступе).

4. На основании рассчитанных значений ошибок 1-го и 2-го родов, а также на основании характеристик динамики клавиатурного набора, выданных системой (файлом *index*) сделать выводы.

4. Контрольные вопросы

1. К какому типу биометрических характеристик относится клавиатурный почерк?
2. На чем основывается аутентификация по клавиатурному почерку?
3. Каким путем можно осуществить защиту парольной фразы от перехвата?
4. В чем заключаются достоинства и недостатки метода идентификации по клавиатурному почерку?

Литература

1. *Ilonen J.* Keystroke Dynamics // Lappeenranta University of Technology. 2008.
2. *Checco J.C.* Keystroke Dynamics and Corporate Security // WSTA Ticker Magazine. 2003.
3. *El-Hadidi Kamal M.* Biometrics. What and How. 2007. http://www.net-security.org/dl/articles/Biometrics.pdf.