УДК 004.715

Стрельцов О. В.,
канд. техн. наук,
доцент кафедри комп'ютерних систем,
ovstreltsov@gmail.com
Войтов В. М.,
бакалавр кафедри комп'ютерних систем,
Одеський національний
політехнічний університет,
м. Одеса, Україна,
baksy93@gmail.com

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Розробки в області біометричної автентифікації за клавіатурним почерком мають ряд переваг і недоліків, для скасування яких був запропонований метод автентифікації з використанням властивостей комп'ютерної логіки, спрямованої на усунення математичної обробки даних у системах парольної автентифікації. За рахунок створеного алгоритму можлива авторизація користувачів з невираженим клавіатурним почерком і низьким навиком володіння клавіатурою. Використання даного методу в пристроях з різними способами введення даних дозволяє мінімізувати ймовірність виникнення помилок як першого, так і другого роду.

Ключові слова*: клавіатурний почерк; біометрична автентифікація; приховані системи моніторингу клавіатурного почерку; аналіз алгоритмів біометричної автентифікації; аналіз методів біометричної автентифікації; біометричні системи контролю доступу.*

За последние четверть века благодаря развитию науки и технологий большинство людей обзавелись умными электронными устройствами и пользуются ими ежедневно для общения, поиска информации, торговли, банковских и прочих операций. Каждый из пользователей подобных устройств несколько раз в день сталкивается с процедурой идентификации, которая является обязательным первичным этапом получения доступа к какой-либо современной компьютерной системе, после неё осуществляется аутентификация и авторизация. Одним из элементов подобных систем является подсистема управления доступом к информационным ресурсам, которая дает возможность разграничить доступ круга пользователей, имеющих доступ к информации и предотвратить сбои в работе информационной системы в целом.

Существует множество методов идентификации и аутентификации, которые отличаются своей сложностью, надежностью, стоимостью и другими показателями. Традиционные методы основываются на использовании электронных ключей, карт, паролей и кодов доступа. После получения данных от пользователя они сравниваются с данными, которые находятся в специальной защищенной базе данных и, в случае успешной аутентификации, проводят авторизацию с последующим допуском пользователя к работе в системе. Основной недостаток таких методов идентификации и аутентификации обусловлен неоднозначностью идентифицируемой личности. Прежде всего, это связано с тем, что для установления аутентичности личности используют атрибутивные и основанные на знаниях распознавательные характеристики. Другим важным недостатком традиционных методов идентификации и аутентификации является отсутствие возможности обнаружения подмены идентифицированного пользователя, что дает возможность злоумышленнику получить доступ к ресурсам системы, который ограничен лишь правами идентифицированного пользователя [1]. Вышеперечисленные недочеты можно исправить, дополнив систему защиты методами биометрической аутентификации, которая заключается в распознавании человека по его уникальным физиологическим или поведенческим характеристикам. Все методы биометрической идентификации и аутентификации разделяются на статические и динамические. Статические методы основываются на физиологической характеристике человека, т.е. уникальной особенности, врожденной и неотъёмной (рисунок сетчатки и радужной оболочки глаза, отпечатки пальцев, геометрия руки). Динамические методы основываются на поведенческой (динамической) характеристике человека, т.е. учитывают особенности, характерные для подсознательных движений в процессе какого-либо действия. Среди этих методов биометрической аутентификации значительный интерес вызывают методы аутентификации по динамическому почерку человека и клавиатурному (компьютерному) почерку в связи с их доступностью и отсутствии

необходимости приобретения дополнительных устройств ввода.

Клавиатурный почерк – это совокупность индивидуальных характеристик, определяющих особенность работы пользователя в режиме ввода текста с клавиатуры. Надёжность такой системы напрямую зависит от того, сколько пальцев использует пользователь при наборе текста, его скорость набора, использование дополнительных клавиш и т.п.

Несмотря на значительный интерес к системам биометрической аутентификации по клавиатурному почерку, эти системы характеризуются низкой точностью аутентификации личности. С целью определения причин, которые влияют на низкую точность, на рис.1 приведены основные этапы разработки и создания систем биометрической аутентификации по клавиатурному почерку [5].

Рис. 1. Этапы разработки и создания системы биометрической аутентификации по клавиатурному почерку

Первым этапом проектирования систем биометрической аутентификации по клавиатурному почерку является создание математических моделей, которые бы адекватно отображали важные показания, стороны временной структуры данных, которые приходят от клавиатуры. Математическая модель задаёт потенциал и, по большей части, эффективность созданных информационных технологий, обуславливает структуру программной и аппаратной составляющих проектирующейся информационной системы. От качества математической модели данных существенно зависит точность и достоверность методов их обработки системой биометрической аутентификации, уровень информативности аутентификационных и идентификационных свойств, достоверность принятия решений [2].

Из приведённого анализа, основной причиной низкой точности систем биометрической аутентификации по клавиатурному почерку является недостаточная эффективность соответствующего математического обеспечения. Учитывая вышеупомянутый вывод, проведем сравнительный анализ существующих математических моделей, методов и систем аутентификации по клавиатурному почерку с целью обнаружения основных недостатков.

Прежде всего, стоит сказать, что разные математические модели методы и системы биометрической аутентификации по клавиатурному почерку отличаются использованием и назначением. Во-первых, клавиатурный почерк может рассматривается как средство мониторинга психофизического состояния оператора ЭВМ. В этом случае предложен подход по построению подсистемы, основанный на математической модели биометрической обработки клавиатурного почерка, на математической модели определения психофизического состояния и алгоритме принятия решения по оповещению оператора, принимающего решение [2]. Для решения этой задачи выбирается математический аппарат обработки биометрических данных нейронными сетями.

Разработан и реализован полигауссовский алгоритм аутентификации пользователей по клавиатурному почерку с целью повышения достоверности аутентификации, который тоже дает возможность отследить психофизическое состояние человека [3]. При использовании данного алгоритма параметры клавиатурного почерка систематизируются и для повышения достоверности аутентификации пользователей вводится новый параметр – скорость нажатия клавиш. Так же разработан способ вычисления скорости движения клавиш во время набора пользователем символов на клавиатуре, где скорость движения клавиш представляется как процесс изменения ёмкости контактной пары клавиш во времени. Проведено исследование стандартных плёночных клавиатур и получено значение ёмкостей контактных пар клавиш, а также решена проблема паразитных составляющих за счет интегрированного способа измерения ёмкости. Данный методы и полигауссовский алгоритм позволяют повысить коэффициент достоверности аутентификации до уровня 95 %. Преимуществом такого направления аутентификации по клавиатурному почерку является возможность определения адекватного психофизиологического состояния человека. Однако, высокая точность аутентификации в данном методе не достигнута т.к. используется только отклонение от нормального значения временных характеристик клавиатурного почерка. Кроме того, принято во внимание, что с разработкой новых материалов, которые будут использоваться для изготовления компьютерных клавиатур, временные характеристики компьютерного почерка будут изменяться, и, в следствии, будут изменяться временные характеристики компьютерного почерка, что приведет к изменению класса точности системы биометрической аутентификации в целом т.к. скорость нажатия клавиш не будет постоянной.

Предложен метод формирования и коррекции баз биометрических эталонов пользователей разделённых информационных систем по поведенческим характе-

ристикам, что дает возможность упростить реализацию процедур анализа биометрических профилей и учесть возможность изменения поведенческих характеристик пользователей [4]. Данные методы идентификации пользователей по клавиатурному почерку по стилю работы с использованием теории нечётких множеств позволяют учесть неопределенности, характерные для этапа формирования поточных биометрических профилей пользователей.

В ряде случаев используется парольный метод аутентификации с использованием усиленного метода биометрической аутентификации на основе параметрического обучения классификатора [5]. Вектор биометрических характеристик определяется при помощи обработки полученных от пользователя данных с использованием вычисления математических ожиданий параметров полученных векторов и последующего вычисления элементов ковариационной матрицы. После чего определяется дискриминантная функция и оптимальный коэффициент Стьюдента, определяющий величину допуска, полученного экспериментальным методом для N пользователей, проводящих тестирование метода.

Используется также метод биометрической аутентификации пользователя по клавиатурному почерку на основе разложении Хаара и меры близости Хэмминга [6]. Количество членов разложения ряда Фурье определяет погрешность данного метода, исходя из чего, предлагается подбирать максимальную длину пароля на этапе экспериментального исследования. Результат разложения вектора в ряд Фурье является недостаточно оптимальным по ряду причин, поэтому предлагается использовать функции Хаара, которые образуют ортонормированную, периодическую, полную систему непарных функций, обладающих свойством и локальной и глобальной чувствительности. После дискретизации по времени полученной от пользователя функции и ее преобразования на основе разложения Хаара определяется искомый вектор биометрических параметров. Предложенный метод рассчитан на максимальную длину парольной фразы для уменьшения погрешности при вводе, является гибким и точность данного метода определяется числом коэффициентов разложения, зависящих от длины парольной фразы.

Существует метод гистограммного распознавания клавиатурного почерка [7]. Предложено формировать вектор биометрических характеристик на основании длительности событий удержаний и пауз путём преобразования их в r-мерный вектор биометрических параметров. Для обучающей выборки определяется диапазон изменения каждого из компонентов и приводится к началу координат. Они, в свою очередь, определяют координаты приведенной r-мерной области распределения векторов. После разбиения области на подобласти строится оценка плотности векторов и проводится сравнение с плотностью распределения векторов обучающей выборки по закону, основанному на формировании отношения правдоподобия. К преимуществам данного метода можно отнести его простоту и ясный физический смысл, к недостаткам – отсутствие оптимального способа разбиения области на подобласти, невозможность достижения сходимости при увеличении объема обучающей выборки, необходимость неоднократного ввода парольной фразы для создания необходимого количества векторов биометрических данных для проведения аутентификации.

Наибольший интерес представляют методы и математические модели скрытого клавиатурного мониторинга с длительным использованием клавиатуры. Одной из последних разработок биометрической аутентификации по клавиатурному почерку является метод основанный на использовании аппарата теории вероятностей и математической статистики для оценивания математического ожидания и времени удержания клавиш как характеристики клавиатурного почерка оператора [8]. Предложен метод распознавания клавиатурного почерка по вводу свободного текста в основании механизма анализа клавиатурного ввода данных. Данный метод реализован в алгоритме распознавания клавиатурного почерка по времени удержания клавиш и времени введения часто употребляемых в письме последовательностей букв (N-грамм). Разработанная система аутентификации оператора системы информационной инфраструктуры имеет точность 98 %, если количество операторов, зарегистрированных в системе, равняется 100. Также доказано, что в связи с использованием метода определения клавиатурного почерка в основе учёта времени удержания клавиш, становится возможным определение клавиатурного почерка по свободному тексту. Метод не учитывает промежуток времени между нажиманием клавиш, который иногда увеличивает точность определения, в связи с перекрытием соседних клавиш.

Предлагаемый метод основан на элементах клавиатурного почерка, однако вместо математического аппарата использована компьютерная логика, что позволяет избавиться от ряда недостатков, которые присутствуют в предыдущих методах, позволяя увеличить эффективность системы аутентификации как среди уверенных пользователей клавиатуры, так и среди новичков.

При регистрации пользователя сопровождает аудио/световой сигнал с t_k=250мс-1000мс (определяется программой), позволяющий корректировать время нажатия клавиш. Каждые 250мс-1000мс программа регистрирует данные о нажатии/отпускании клавиш и на их основе создается вектор параметров. Максимальное количество одновременно нажатых клавиш, количество изменений статуса нажатых клавиш, используемые клавиши для каждого пользователя являются их личными биометрическими характеристиками. В зависимости от предельных показателей вышеупомянутых характеристик определяется время t_k, задающее временной промежуток для пользователя в зависимости от его навыков работы на клавиатуре. Вводится парольная фраза/комбинация клавиш, известная пользователю. Каждый промежуток времени t_k регистрируется информация о нажатых и отпущенных клавишах в виде массива массивов. Учитывается порядок нажатия и отпускания клавиш, а также промежутки, в которых они были нажаты.

Если пользователь не смог N раз повторить фразу при регистрации, ему предлагается её упростить, если максимальное значение t_k достигнуто. После успешного прохождения регистрации программа предлагает пользователю авторизироваться и продолжить работу.

Пример: простая парольная фраза «QWERTY» и несколько вариаций её ввода в течении 8с пользователями с разным уровнем работы на клавиатуре изображены на рис. 2, 3, 4.

Рис. 2. Ввод парольной фразы QWERTY пользователем 1

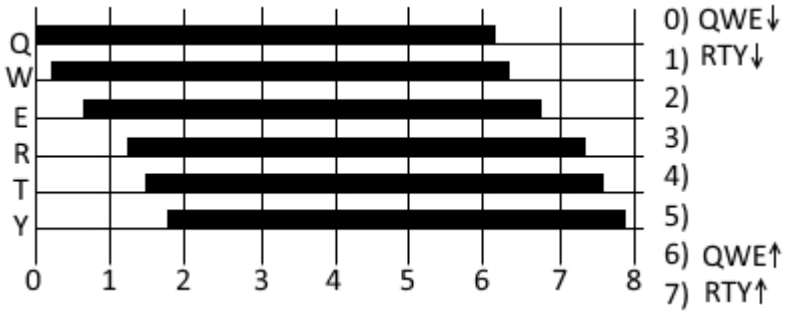

Рис. 3. Ввод парольной фразы QWERTY пользователем 2

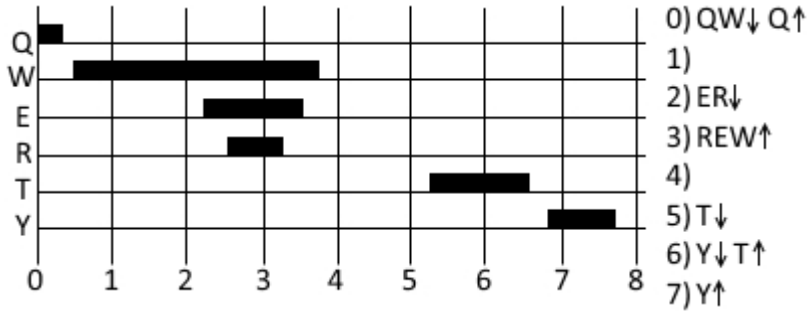

Рис. 4. Ввод парольной фразы QWERTY пользователем 3

В связи с точным определением пользователем времени нажатия и отпускания клавиш, точность определения этого метода может достигать 100 %, а вероятность возникновения ошибки второго рода стремится к нулю при увеличении сложности парольной фразы.

Общая статистика по проведенным анализам предыдущих разработок систем клавиатурной аутентификации отображена в следующих таблицах 1, 2.

Таблица 1

Анализ алгоритмов аутентификации по клавиатурному почерку

Автор; Название	В. Г. Абашин; Автоматизация процесса определения психофизиологического состояния оператора автоматизированного рабочего места в АСУТП	Р. Р. Шарипов; Разработка полигауссового алгоритма аутентификации пользователей в телекоммуникационных системах и сетях по клавиатурному почерку	Л. Э. Чалая; Сравнительный метод аутентификации пользователей компьютерных систем по клавиатурному почерку	И. А. Ходашинский, М. В. Савчук, И. В. Горбунов, Р. В. Мещеряков; технология усиленной аутентификации пользователей информационных процессов
Время удержания клавиш	–	+	+	+
Скорость нажатия клавиш	–	+	–	–
Скорость набора текста/фразы	+	+	+	+
Интервалы между нажатиями	–	+	+	+
Перекрытия	–	–	+	+
Возможность ошибки	+	+	+	+
Динамика (стабильность) ввода	–	–	+	+
Аритмичность ввода	–	–	+	+
Психофизическое состояние	+	–	+	–
Коды клавиш клавиатуры	–	–	–	+
Использование шаблонов групп клавиш	–	–	–	–
Особенности				
Коэффициент сложности для пользователя	–	–	+	–
Смена клавиатуры не влияет на показания	+	–	–	+
Однократный ввод контрольной фразы	–	+	+	+
Авторизация по неизвестной парольной фразе	–	–	+	+
Использование управляющего воздействия (аудио/цвет)	+	–	–	–
Не используется дополнительное оборудование	+	–	+	+
Сравнение полученных данных с 1 пользователем из базы данных	–	–	+	+

Табл. 1. Продолжение

Автор; Название	В. Г. Абашин; Автоматизация процесса определения психофизиологического состояния оператора автоматизированного рабочего места в АСУТП	Р. Р. Шарипов; Разработка полигауссового алгоритма аутентификации пользователей в телекоммуникационных системах и сетях по клавиатурному почерку	Л. Э. Чалая; Сравнительный метод аутентификации пользователей компьютерных систем по клавиатурному почерку	И. А. Ходашинский, М. В. Савчук, И. В. Горбунов, Р. В. Мещеряков; технология усиленной аутентификации пользователей информационных процессов
Определение подмены пользователя во время работы	+	–	–	–
Формирование эталона КП	Длительное обучение	30 дней	Длительное обучение	3–5 минут
Статистика				
Вероятность ошибки I рода (профи) %	не приведено	не приведено	1,81	8,6
Вероятность ошибки II рода (профи) %	не приведено	не приведено	1,75	7
Вероятность ошибки I рода (новичок) %	не приведено	не приведено	не приведено	не приведено
Вероятность ошибки II рода (новичок) %	не приведено	не приведено	не приведено	не приведено
Эффективность метода для проф %	не приведено	95 %	98,20 %	91,70 %
Эффективность метода для новичков %	не приведено	не приведено	не приведено	не приведено

Таблица 2

Анализ алгоритмов аутентификации по клавиатурному почерку

Автор; Название	Ю. А. Брюхомицкий, М. Н. Казарирн; метод биометрической идентификации пользователя по клавиатурному почерку на основе разложении Хаара и меры близости Хэмминга	Ю. А. Брюхомицкий; гистограммный метод распознавания клавиатурного почерка	А. Н. Савинов; методы модели и алгоритмы распознавания клавиатурного почерка в ключевых системах	Войтов В. М.; Исследование алгоритмов аутентификации пользователя по клавиатурному почерку
Время удержания клавиш	+	+	+	+
Скорость нажатия клавиш	–	–	–	–
Скорость набора текста/фразы	–	–	+	–
Интервалы между нажатиями	+	+	+	+
Перекрытия	+	+	+	+

Табл. 2. Продолжение

Автор; Название	Ю. А. Брюхомицкий, М. Н. Казарирн; метод биометрической идентификации пользователя по клавиатурному почерку на основе разложении Хаара и меры близости Хэмминга	Ю. А. Брюхомицкий; гистограммный метод распознавания клавиатурного почерка	А. Н. Савинов; методы модели и алгоритмы распознавания клавиатурного почерка в ключевых системах	Войтов В. М.; Исследование алгоритмов аутентификации пользователя по клавиатурному почерку
Возможность ошибки	–	–	+	–
Динамика (стабильность) ввода	–	–	+	–
Аритмичность ввода	–	–	+	–
Психофизическое состояние	–	–	+	+
Коды клавиш клавиатуры	–	–	–	+
Использование шаблонов групп клавиш	–	–	+	+
Особенности				
Коэффициент сложности для пользователя	–	–	–	+
Смена клавиатуры не влияет на показания	–	–	–	+
Однократный ввод контрольной фразы	+	–	–	+
Авторизация по неизвестной парольной фразе	+	–	–	+
Использование управляющего воздействия (аудио/цвет)	–	–	–	+
Не используется дополнительное оборудование	+	–	+	+
Сравнение полученных данных с 1 пользователем из базы данных	+	–	–	+
Определение подмены пользователя во время работы	–	–	+	–
Формирование эталона КП	5–10 минут	3–5 минут	Длительное обучение	3 минуты
Статистика				
Вероятность ошибки I рода (профи) %	3	не приведено	не приведено	2
вероятность ошибки II рода (профи) %	не приведено	не приведено	не приведено	0
Вероятность ошибки I рода (новичок) %	не приведено	не приведено	не приведено	18
Вероятность ошибки II рода (новичок) %	не приведено	не приведено	не приведено	0

Табл. 2. Продолжение

Автор; Название	Ю. А. Брюхомицкий, М. Н. Казарирн; метод биометрической идентификации пользователя по клавиатурному почерку на основе разложении Хаара и меры близости Хэмминга	Ю. А. Брюхомицкий; гистограммный метод распознавания клавиатурного почерка	А. Н. Савинов; методы модели и алгоритмы распознавания клавиатурного почерка в ключевых системах	Войтов В. М.; Исследование алгоритмов аутентификации пользователя по клавиатурному почерку
Эффективность метода для проф %	91,50 %	не приведено	98 %	99 %
Эффективность метода для новичков %	не приведено	не приведено	не приведено	90 %

Проведенный анализ алгоритмов и методов аутентификации пользователей по клавиатурному почерку позволяет сделать следующие выводы:

1. Системы скрытого мониторинга позволяют достичь более высокой точности, нежели методы аутентификации по парольной фразе, однако требуют длительного времени для обучения.

2. Системы парольной аутентификации делятся на ввод фразы с экрана компьютера и ввод известной лишь оператору парольной фразы. При вводе фразы с экрана компьютера без длительного обучения программы наиболее вероятно возникновение ошибки второго рода.

3. При смене клавиатуры или изменении психофизического состояния пользователя повы-шается вероятность возникновения ошибки первого рода, а в скрытых системах мониторинга позволяет следить за состоянием пользователя.

4. При повышении коэффициента достоверности аутентификации, у пользователей с низким навыком владения устройством ввода критично увеличивается вероятность возникновения ошибки первого рода, а при его уменьшении возрастает вероятность ошибки второго рода, что уменьшает эффективность всей системы в целом.

5. Количество используемых параметров, которые учитываются при создании математической модели, позволяют уменьшить вероятность возникновения ошибки второго рода, однако повышают вероятность возникновения ошибки первого. Для нахождения «золотой середины» используются коэффициенты достоверности, которые разграничивает области «свой» и «чужой».

Сравнение результатов тестирования разработанного метода с анализированными позволяет сделать следующие выводы:

1. Разработанный метод позволяет исключить вероятность возникновения ошибки второго рода, если пользователь не знает точную последовательность и время нажатия/отпускания клавиш.

2. Метод не использует математический аппарат, не требует использования коэффициента достоверности, который разграничивает области «свой» и «чужой», поэтому в отличии от других методов его эффективность может достигать 100 % (в отличии от 99.9 %, используемых в системах скрытого мониторинга с длительным обучением).

3. Имеет высокую точность и занимает от 3 до 20 минут на регистрацию пользователя в зависимости от навыков владения клавиатурой.

4. Возможность привязки к одной учетной записи разных паролей в зависимости от используемого устройства для авторизации в системе/базе данных и т. д.

5. При замене клавиатуры на другой тип повышает вероятность возникновения ошибки первого рода у пользователей с низким навыком владения клавиатурой и пользователей с высокой сложностью ввода парольной фразы. При использовании на разных платформах предлагается использовать разные пароли для удобства.

6. Может быть реализован как на ПК с клавиатурой, так и на компьютерах с тачскрином, мобильных устройствах, планшетах (удобство зависит от площади области ввода).

7. Эффективна при авторизации пользователей с низким уровнем владения устройства ввода.

ЛИТЕРАТУРА

1. Казарин М. Н. Разработка и исследование методов скрытного клавиатурного мониторинга [Электронный ресурс] / Казарин М. Н. – Таганрог, 2006. – Режим доступа : http://www.dissercat.com/content/razrabotka-i-issledovanie-metodov-skrytnogo-klaviaturnogo-monitoringa. – Загл. с экрана.
2. Абашин В. Г. Автоматизация процесса определения психофизиологического состояния оператора автоматизированного рабочего места в АСУТП [Электронный ресурс] / В. Г. Абашин. – Орел, 2007. – Режим доступа : http://www.dissercat.com/content/avtomatizatsiya-protsessa-opredeleniya-psikhofiziologicheskogo-sostoyaniya-operatora-avtomat. – Загл. с экрана.
3. Шарипов Р. Р Разработка полигауссового алгоритма аутентификации пользователей в телекоммуникационных системах и сетях по клавиатурному почерку [Электронный ресурс] / Р. Р. Шарипов. – Казань, 2006. – Режим доступа :

http://tekhnosfera.com/razrabotka-poligaussovogo-algoritma-autentifikatsii-polzovateley-v-telekommunikatsionnyh-sistemah-i-setyah-po-klaviaturno. – Загл. с экрана.
4. Чалая Л. Э. Сравнительный метод аутентификации пользователей компьютерных систем по клавиатурному почерку [Электронный ресурс] / Л. Э. Чалая. – Харьков, 2008. – Режим доступа : https://goo.gl/9JuhYu. – Загл. с экрана.
5. Технология усиленной аутентификации пользователей информационных процессов [Электронный ресурс] / Ходашинский И. А., Савчук М. В., Горбунов И. В., Мещеряков Р. В. – Томск, 2011. – Режим доступа : http://cyberleninka.ru/article/n/tehnologiya-usilennoy-autentifikatsii-polzovateley-informatsionnyh-protsessov. – Загл. с экрана.
6. Метод биометрической идентификации пользователя по клавиатурному почерку на основе разложении Хаара и меры близости Хэмминга [Электронный ресурс] / Брюхомицкий Ю. А., Казарин М. Н. – Таганрог, 2003. – Режим доступа : http://cyberleninka.ru/article/n/metod-biometricheskoy-identifikatsii-polzovatelya-po-klaviaturnomu-pocherku-na-osnove-razlozheniya-haara-i-mery-blizosti-hemminga. – Загл. с экрана.
7. Брюхомицкий Ю. А Гистограммный метод распознавания клавиатурного почерка [Электронный ресурс] / Ю. А. Брюхомицкий, Таганрог, 2010. – Режим доступа : http://cyberleninka.ru/article/n/gistogrammnyy-metod-raspoznavaniya-klaviaturnogo-pocherka. – Загл. с экрана.
8. Савинов А. Н. Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах [Электронный ресурс] / Савинов А. Н. – Йошкар-Ола. – Режим доступа : http://tekhnosfera.com/metody-modeli-i-algoritmy-raspoznavaniya-klaviaturnogo-pocherka-v-klyuchevyh-sistemah. – Загл. с экрана.

О. В.Стрельцов,
В. М. Войтов,
Одесский национальный политехнический университет, г. Одесса, Украина

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Разработки в области биометрической аутентификации по клавиатурному почерку имеют ряд преимуществ и недостатков, для упразднения которых был предложен метод аутентификации по клавиатурному почерку в виде системы с использованием свойств компьютерной логики, направленной на устранение коэффициента эффективности в системах парольной аутентификации. Таким образом, за счет созданного алгоритма, появилась возможность как авторизации пользователей с не выраженным клавиатурным почерком и низким навыком владения, так и использования данного метода в устройствах с разными способами ввода данных, минимизировав вероятность возникновения ошибок как первого так и второго рода.

Ключевые слова: *клавиатурный почерк; биометрическая аутентификация; скрытые системы мониторинга клавиатурного почерка; анализ алгоритмов биометрической аутентификации; анализ методов биометрической аутентификации; биометрические системы контроля доступа; метод биометрической аутентификации на основе компьютерной логики.*

O. V. Streltsov,
V. M. Voytov,
Odesa National Polytechnic University, Odesa, Ukraine

RESEARCH OF KEYBOARD HANDWRITING AUTHENTICATION ALGORITHMS

Developments in the field of keyboard handwriting biometric authentication have a number of advantages and disadvantages for which the abolition of the authentication method was proposed based on the keyboard in the form of handwriting system using the properties of computer logic, aimed at addressing the efficiency ratio in the password authentication systems. Thus, by an algorithm, it is possible as the user authentication with no pronounced keyboard handwriting and low skill ownership and use of this method in devices with different methods of data entry, minimizing the likelihood of errors of both the first and second kind.

Key words: *handwriting keyboard; biometric authentication; hidden keyboard monitoring system of handwriting analysis algorithms for biometric authentication; biometric authentication methods of analysis; biometric access control systems; biometric authentication method based on computer logic.*

Рецензенти: д. т. н., проф. ***М. П. Мусієнко;***
к. т. н., доц. ***І. М. Журавська.***

Дата надходження статті до редколегії 10.10.16