УДК 004.353.4

Подтверждение личности пользователя по его клавиатурному почерку

А.С. Калужин, Д.Д. Рудер

Алтайский государственный университет (Барнаул, Россия)

User Identity Confirmation with His Keystroke Pattern

A.S. Kaluzhin, D.D. Ruder

Altai State University (Barnaul, Russia)

Клавиатурный почерк относится к динамическим (поведенческим) биометрическим характеристикам, описывающим подсознательные действия, привычные для пользователя. Он характеризует динамику ввода парольной фразы с помощью клавиатуры. Опознавание клавиатурного почерка состоит в выборе соответствующего эталона из списка хранимых в памяти компьютера эталонов на основе оценки степени близости этому эталону параметров почерка одного из операторов, имеющих право на работу с данным компьютером. Решение задачи опознавания пользователя сводится к решению задачи распознавания образов. 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. Классический статистический подход к распознаванию пользователя по клавиатурному почерку (набор ключевых слов) выявил ряд интересных особенностей: зависимость почерка от буквенных сочетаний в слове, существование глубоких связей между набором отдельных символов, наличие «задержек» при вводе символов.

Ключевые слова: информационные технологии, информационная безопасность, защита информации, компьютерная система, биометрия, аутентификация, подтверждение личности.

A keystroke pattern belongs to dynamic (behavioral) biometric characteristics describing the subconscious actions familiar to a user. It characterizes the passphrase entering dynamics. The keystroke pattern recognition is based on a comparison of the pattern in question with a list of pattern templates stored in a memory of a computer. Thus, the problem of user identification reduces to a problem of pattern recognition. Keyboard usage analysis does not require special hardware and personnel for installation and further support. It allows the process of covert authentication and is transparent to end user, i.e. does not cause any inconvenience. Classic statistical approach to the keystroke pattern recognition (while typing several key words) reveals a number of interesting features: the dependence of character combinations in a typed word, a deep connection between a set of individual characters, a "delay" presence when typing characters.

Key words: information technology, information security, information security, computer system, biometrics, authentication, identity confirmation.

DOI 10.14258/izvasu(2015)1.1-28

Важнейшим аспектом информационной безопасности телекоммуникационных систем и сетей самого широкого назначения является разграничение доступа к управлению системой и ее ресурсам. Для достижения данной цели была написана программа, позволяющая проходить аутентификацию при помощи клавиатурного почерка.

Работа систем аутентификации пользователей состоит из ряда этапов [1, 2]:

1. Систему настраивают под определенных пользователей.

2. Пользователи многократно набирают заранее известные или случайные фразы, затем вычисляются заданные наборные характеристики пользователей.

3. Значения этих характеристик подвергаются статистической обработке: вычисляются математические ожидания и дисперсии и записываются в память, в дальнейшем эти значения являются эталонными.

4. После настройки система аутентифицирует пользователей и решает задачу выбора двух гипотез: гипотеза 1 означает, что пользователь, который набирает слова на клавиатуре, является одним из заре-

гистрированных; гипотеза 2, наоборот, означает, что пользователь не зарегистрирован.

Многие вопросы аутентификации пользователей на основе их клавиатурного почерка не изучены. Существующие программные реализации подобных систем характеризуются недостаточной достоверностью аутентификации. Актуальна разработка новых методов, алгоритмов и их программно-аппаратных реализаций, повышающих эффективность систем идентификации и аутентификации [3].

Целью работы является:

- написание приложения, которое позволило бы проходить аутентификацию с использованием клавиатурного почерка;
- тестирование написанного приложения.

Одной из систем аутентификации по клавиатурному почерку является программа BioKeyLogon [3].

Разработчики программы утверждают, что она позволит внести дополнительную безопасность в систему, так как использует биометрическую защиту. На самом деле программа работает некорректно, а точнее, она пускает в систему любого пользователя, который знает пароль, а также имеет ограниченную длину пароля — шесть символов.

В ходе работы было написано приложение, позволяющее проверить работоспособность аутентификации по клавиатурному почерку. Оно представляет собой программу, которая обрабатывает интервалы между нажатием на клавиши при вводе парольной фразы для каждого пользователя, считает математическое ожидание и дисперсию. Полученные данные считаются эталонными. После регистрации в системе данные передаются по защищенному каналу связи, где происходит запись их в базу данных. При входе в систему пользователю предлагается ввести логин и пароль, который он указал при регистрации. Если логина не существует в системе, то ввести пароль не получится, если логин существует, то пользователь вводит пароль, который сравнивается с тем, который хранится в базе данных, и с эталонными значениями. После чего происходит принятие решения: разрешить ли пользователю вход в систему или нет. Принцип работы изображен на рисунке 1.

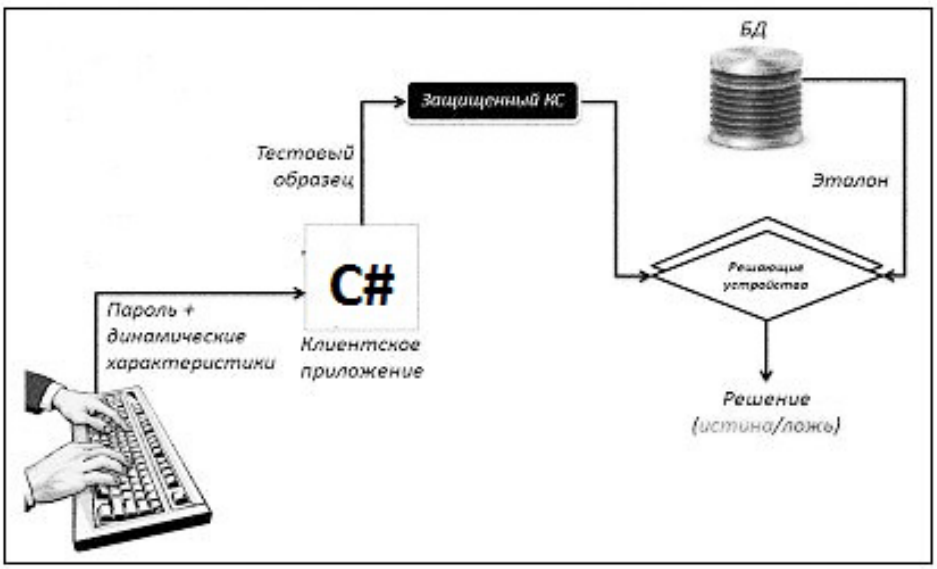

Рис. 1. Схема работы программы

Программа представляет собой оконное приложение (рис. 2), состоящее из трех окон. В первом окне происходит процесс авторизации пользователя.

Данное окно представляет собой две строки ввода:

- строка для ввода логина;
- строка для ввода пароля.

Пользователь может пройти авторизацию только в том случае, если его данные содержатся в базе данных. В случае если пользователь вводит неправильный пароль более шести раз, то программа блокирует возможность вводить пароль заново.

При вводе логина и пароля происходит поиск введенных значений в базе данных, если данные найдены, то программа выводит сообщение о том, что аутентификация прошла успешно. В случае если пользователя нет в базе данных, то программа предлагает зарегистрироваться и автоматически перенаправляет его в окно регистрации (рис. 3).

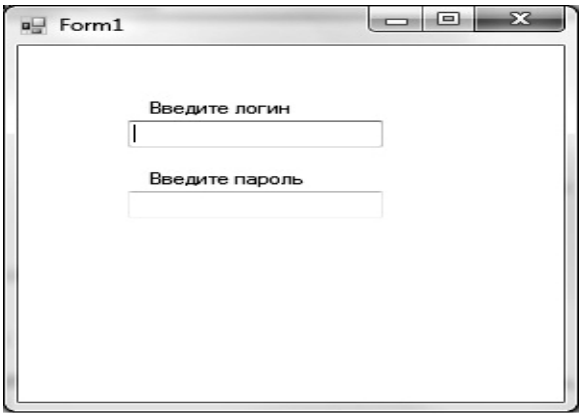

Рис. 2. Окно авторизации программы

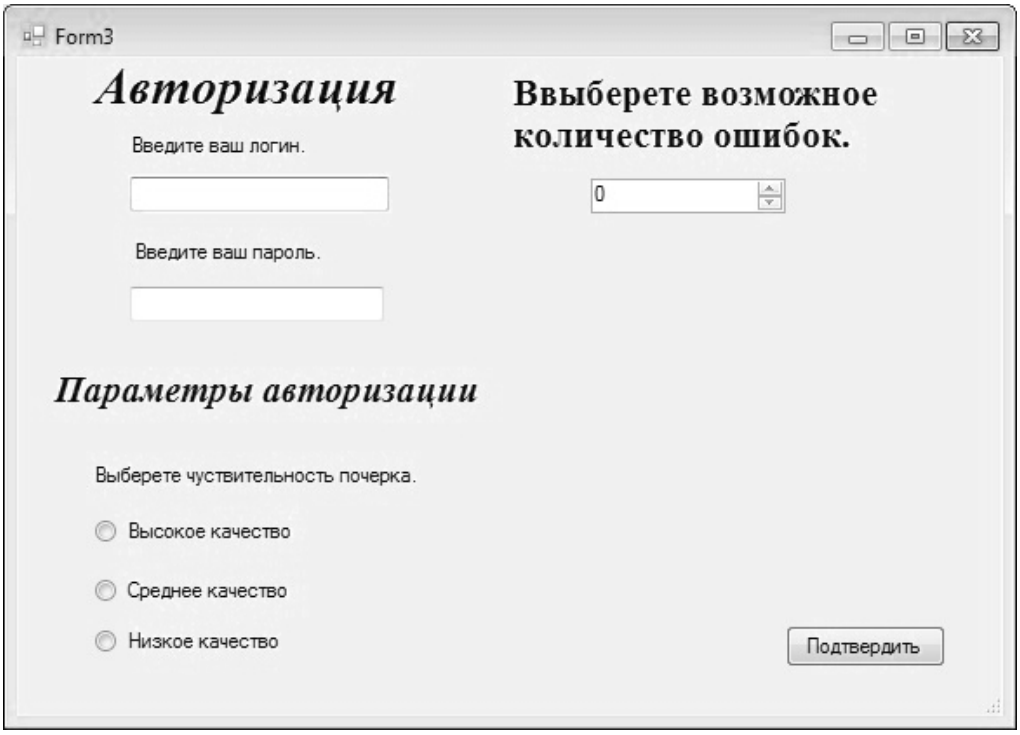

Рис. 3. Окно регистрации нового пользователя

В данном окне пользователь задает следующие параметры:

– в разделе «Авторизация» задается логин и пароль, который будет вводиться при последующем вводе;

– в разделе «Параметры авторизации» пользователь задает так называемую чувствительность почерка, этот параметр увеличивает допустимую погрешность при вводе пароля. Данные значения подобраны экспериментальным путем;

– в разделе «Выберите возможное количество ошибок» пользователь выбирает количество интервалов, в который можно не попасть при вводе парольной фразы. Например, если пароль будет «123456» и выбрано две ошибки, то пользователь может не попасть в два интервала времени, но все равно пройдет аутентификацию. Также если пользователь поставит число ошибок, равное количеству символов в парольной фразе, то динамическая характеристика (интервалы между нажатиями на клавиши) совсем не будут учитываться и пользователь пройдет аутентификацию только по правильности логина и пароля.

После нажатия на кнопку «Подтвердить» пользователя перенаправляют в третье окно, где происходит сам процесс ввода парольной фразы с учетом динамики ввода (рис. 4).

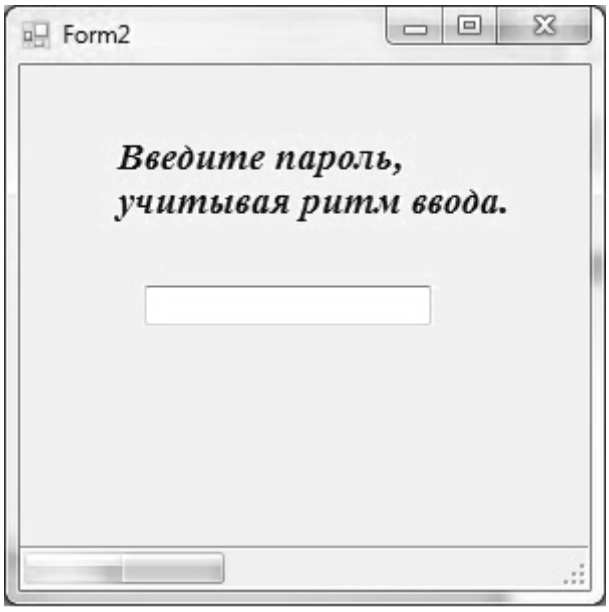

Рис. 4. Окно ввода пароля

Пользователь вводит пароль, который он задал в предыдущем окне, десять раз. После чего происходит вычисление математического ожидания и дисперсии. Далее рассчитанные значения заносятся в базу данных, и пользователь уже считается легитимным и может пройти процесс аутентификации.

Написанное приложение в отличие от выше упомянутого BioKeyLogon имеет неограниченную длину пароля, может настраиваться под любого пользователя. Если пользователь не захотел использовать динамику ввода для аутентификации, он может отключить эту функцию.

После написания программы по данным различных пользователей были построены графики (рис. 5, 6).

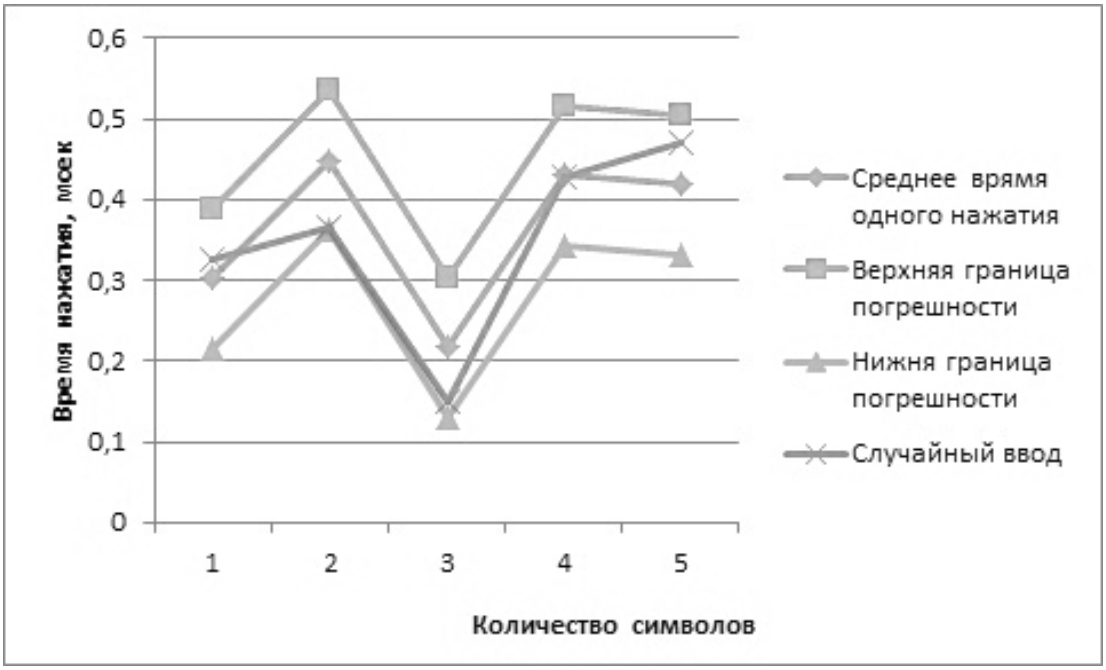

Рис. 5. График ввода парольной фразы первого пользователя

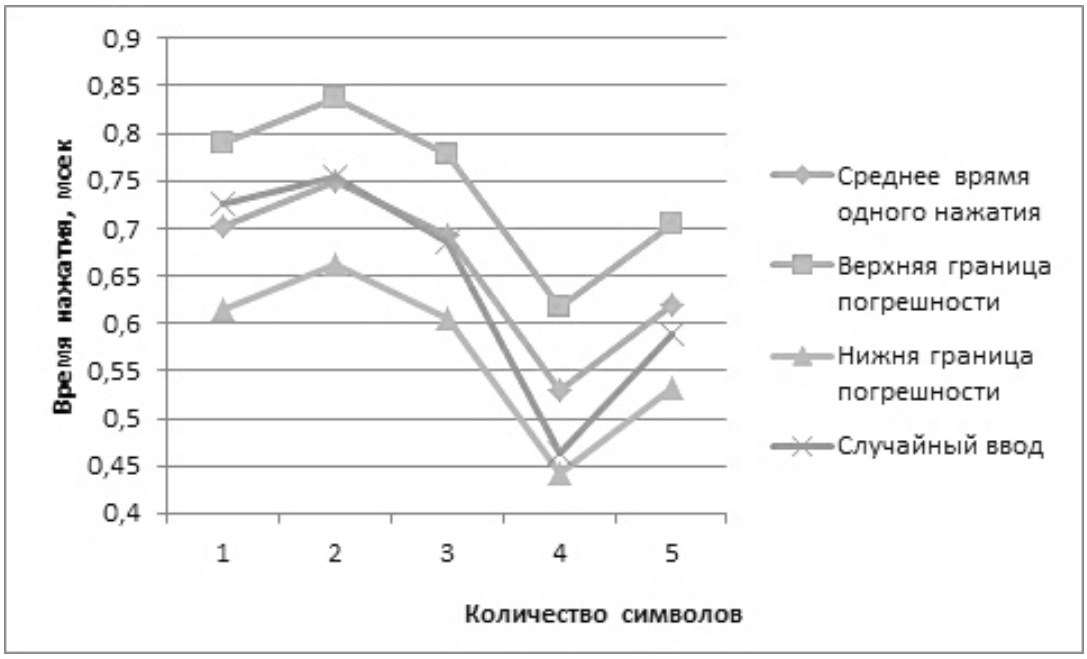

Рис. 6. График ввода парольной фразы второго пользователя

Из графиков следует, что пользователи вводят одно и то же слово по-разному, значит, при вводе парольной фразы посторонним пользователем система не позволит ему получить доступ к данным легитимного пользователя.

Таким образом, написанное приложение можно использовать для аутентификации, основанной на клавиатурном почерке, так и для аутентификации без учета динамической характеристики ввода парольной фразы.

Библиографический список

1. Фу К. Последовательные методы в распознавании образов и обучении машин : пер. с англ. / под ред. Л.А. Меровича. – М., 1971.

2. Фукунага К. Введение в статистическую теорию распознавания образов / пер. с англ. А.А. Дорофеюка. – М., 1979.

3. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. – М., 1993.