УДК 004.9.056 + 004.738.5

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА

Л.Н. Паламарчук, М.С. Никитин

В данной работе рассмотрены актуальность и возможные способы биометрической аутентификации. Подробно рассмотрена возможность аутентификации пользователя путем анализа его клавиатурного почерка.

Ключевые слова: биометрические характеристики, биометрическая аутентификация, клавиатурный почерк, пользователь.

В современных условиях глобальной сетевой инфраструктуры, когда повседневная жизнь каждого человека прочно пронизана цифровыми технологиями, реализованными в виде сайтов Государственных услуг, электронного правительства, электронного банкинга, «цифровой» медицины и так далее, особую важность приобретают вопросы защиты информации и персональных данных. Очевидно, что одна из основных задач обеспечения безопасности информационных компьютерных систем – это задача ограничения круга лиц, имеющих доступ к конкретной информации, и защиты ее от несанкционированного доступа.

Огромный объем данных, хранящихся на компьютерах пользователей по всему миру, может иметь разную степень значимости для конкретного человека: от фотографий из цифрового альбома до информации, представляющей существенную коммерческую значимость.

Одними из наиболее перспективных и активно развивающихся сейчас методов являются методы биометрической аутентификации.

Именно эти методы аутентификации и идентификации пользователя активно берут на вооружение кредитные организации. Так, в марте 2017 года на лекции в Московском физико-техническом институте (МФТИ) глава Сбербанка Герман Греф отметил: «Мы очень много инвестируем в создание идентификационных возможностей. Первая задача банка – идентификация клиента. У нас реализовано огромное количество проектов и стартапов на эту тему – распознавание сетчатки глаза, распознавание ладошки, отпечатков пальцев. … Распознаётся не только голос, кодовые слова, но и движения губ, которые произносят кодовые слова, это является уникальным и мышечную активность подделать невозможно» [4].

Защита информации в компьютерных системах и сетях – это комплексная задача, решение которой происходит с помощью внедрения различных

систем безопасности. Одну из главных ролей в решении данной задачи играет элемент, обеспечивающий контроль доступа к ресурсам компьютерной системы. Такой элемент выполняет свои функции при помощи процедур идентификации и аутентификации пользователей.

Аутентификация – процедура проверки подлинности субъекта доступа.

Аутентификатор – некоторый параметр, предоставляемый системе для проверки. Различают 3 типа аутентификаторов: уникальное знание (пароль, пин-код), уникальный предмет (ключ, смарт-карта, токен), уникальная характеристика самого субъекта – биометрический аутентификатор (статическая – отпечатки пальца, снимок сетчатки глаза, поведенческая – например, аутентификация по голосу) [3]. Таким образом, под биометрической аутентификацией будем понимать процедуру проверки подлинности субъекта доступа на основе его биометрической характеристики.

Методы аутентификации с помощью пароля или уникального предмета наиболее распространены ввиду простоты и относительной дешевизны, но при нарушении конфиденциальности, утере, краже пароля или ключа полностью нарушается защита информации владельца. Для устранения указанных недостатков при аутентификации можно использовать биометрические характеристики пользователя. Биометрия позволяет идентифицировать пользователей, опираясь на их поведенческие и физиологические характеристики. К физиологическим характеристикам можно отнести отпечатки пальцев, черты лица, геометрию ладоней, ушных раковин, сетчатка глаза и т.д. Поведенческие характеристики включают почерк человека, походку, тембр голоса, скорость набора текста на клавиатуре и т.п.

Если определение пользователя с помощью сканирования сетчатки глаза весьма дорогостоящий способ в связи со стоимостью оборудования, то идентификация пользователя по клавиатурному почерку – дешевый и достаточно простой для реализации вариант, так как для такой системы не нужно дополнительного оборудования. Требуется стандартный набор периферийных устройств, которые имеет в своем распоряжении любой персональный компьютер, – клавиатура и монитор. А в качестве системы безопасности будет выступать программный продукт, разработка которого и представляет основную сложность [1].

К биометрическим аутентификаторам относится и клавиатурный почерк. Рассматривают два способа аутентификации пользователя по клавиатурному почерку: по вводу известной фразы (пароля) и по вводу неизвестной фразы, генерируемой случайно. Оба способа включают два режима: обучения и аутентификации. В режиме обучения путем многократного повторения ввода рассчитываются эталонные характеристики набора текста. Как отмечают Г.А. Цанниева и Н.Р. Гасанова, для идентификации пользователя в большинстве случаев достаточно рассматривать временные интервалы между нажатием клавиш и временные интервалы удержания клавиш.

При аутентификации с помощью ввода известной и неизвестной фразы сравнивается разница между интервалами времени при вводе знакомой и незнакомой фразы. Это позволяет верно идентифицировать пользователя, несмотря на усталость или другие психофизические факторы. На основе клавиатурного почерка возможно проводить не только аутентификацию, но и скрытую идентификацию, анализ психофизического состояния [2].

Для аутентификации система должна хранить уникальные характеристики конкретного человека. Так что же такое клавиатурный почерк?

В процессе ввода с помощью клавиатуры пользователь вырабатывает уникальный личный стиль набора символов, который зависит от следующих параметров: количество пальцев, задействованных во время набора, длительность нажатия клавиш; время между нажатиями клавиш; использование основной или дополнительной части клавиатуры; характер сдвоенных или строенных нажатий; любимые сочетания «горячих клавиш» и др. Таким образом, клавиатурный почерк – это набор динамических характеристик работы на клавиатуре.

А.И. Аверин, Д.П. Сидоров отмечают, что важной особенностью задачи аутентификации пользователя по клавиатурному почерку является необходимость «обучения» программы, которая будет производить аутентификацию. Под обучением понимается накопление информации, характеризующей особенности работы каждого пользователя с клавиатурой. Далее эта информация подвергается обработке. Начальным этапом обработки данных является фильтрация. Входной поток данных преобразуется таким образом, чтобы он не содержал информацию о «служебных» клавишах – клавишах управления курсором, функциональных клавишах и т.п.

На следующем этапе выделяется информация, относящаяся к характеристикам пользователя: количество опечаток, время удержания клавиш, интервалы между нажатиями клавиш, число перекрытий между клавишами, скорость набора, степень аритмичности при наборе. После статистической обработки этих данных рассчитанные эталонные характеристики пользователя сохраняются в базе данных. При аутентификации опознавание пользователя состоит в сравнении биометрической информации, которая будет получена при вводе текста с соответствующей этому пользователю эталонной информацией, хранимой в памяти компьютера.

Однако нужно понимать, что системы биометрической аутентификации распознают пользователя с определенной вероятностью, так как биометрические характеристики прямо зависят от эмоционального состояния пользователя и условий, в которых он вводит кодовую фразу. Система может не распознать легального пользователя, даже предоставить доступ к информации человеку, которому она не предназначена. Поэтому в системах биометрической аутентификации присутствуют две оценочные характеристики: отказ в доступе (*false rejection rate*, FRR – ошибка первого рода) –

это вероятность, с которой система не узнает зарегистрированного пользователя, и ложный доступ (*false access rate*, FAR – ошибка второго рода) – вероятность ошибочного допуска нелегального пользователя [1].

И. Агурьянов приводит оценки клавиатурного почерка по следующим параметрам: скорость ввода – количество введенных символов, разделенное на время печатания, динамика ввода – характеризуется временем между нажатиями клавиш и временем их удержания, частота возникновения ошибок при вводе, использование клавиш (рис. 1).

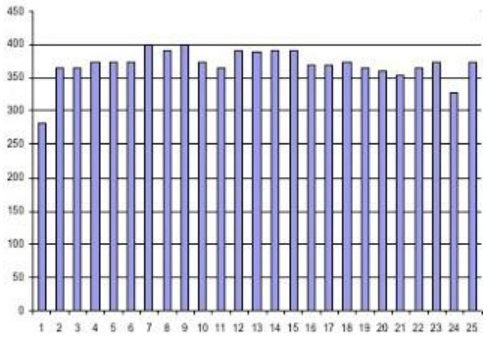

Рис. 1. 25 испытаний скорости ввода парольной фразы

Для тестирования возможностей аутентификации посредством клавиатурного почерка он воспользовался парольной фразой – «апельсинка», которую многократно вводили испытуемые, и программой. Проводились испытания скорости ввода в разное время суток и в разных психофизических состояниях у нескольких испытуемых (рис. 2).

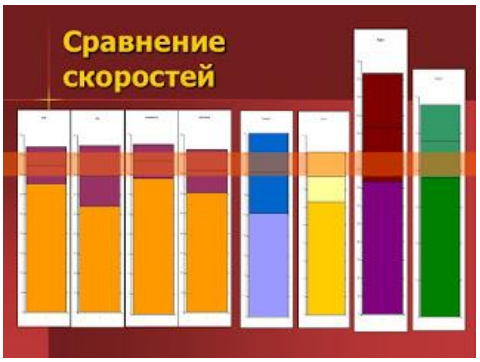

Рис. 2. Сравнение скоростей

Несмотря на различия в скорости печатания всех испытуемых, существует диапазон скоростей, в котором все они могли напечатать парольную фразу. Поэтому помимо скорости для уменьшения количества ложных срабатываний была использована ещё одна характеристика – динамика ввода парольной фразы. Сравнивая с другими состояниями, И. Агурьянов

отмечает, что 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 (рис. 3):

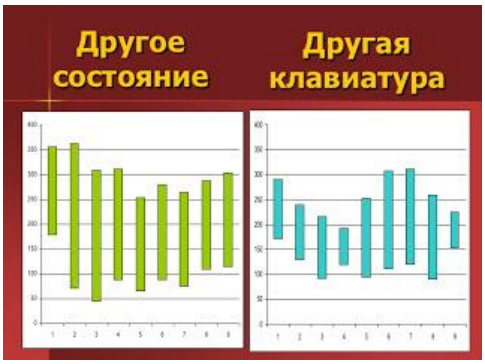

Рис. 3. Сравнение с другими состояниями

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. Сравнивая динамику ввода разных испытуемых (рис. 4), приходим к выводу, что существует вероятность совпадения динамик различных испытуемых, но эта вероятность уже значительно ниже, чем при учете только скорости ввода [3].

Рис. 4. Динамика ввода

Отметим также ряд некоторых интересных особенностей, выявленных на основе статистических данных и приведенных А.И Авериным и Д.П. Сидоровым: вероятность аутентификации пользователя по времени удержания клавиш в зависимости от длины ключевой фразы является бо-

лее стабильной характеристикой клавиатурного почерка пользователя, чем время между нажатиями клавиш (пауз), которое и растет с ростом длины ключевой фразы. Это объясняется тем, что процесс нажатия клавиши на клавиатуре является истинно подсознательным процессом мышления. Время между нажатиями клавиш является менее стабильной характеристикой клавиатурного почерка пользователя, чем время удержания клавиш. Функция вероятности идентификации от пауз между нажатиями клавиш имеет максимум своего значения при длине ключевой фразы порядка 810 символов. Это объясняется тем, что ключевые фразы небольшой длины, состоящие из одного, максимум двух слов, пользователь набирает подсознательно. Подсознательные движения стабильны до тех пор, пока в них не вмешивается более высокий сознательный уровень мышления, что приводит к появлению эффекта «сороконожки», сбивающейся при попытке понять, как же она ходит.

Проявление данного эффекта объясняет уменьшение вероятности аутентификации пользователя при превышении длины ключевой фразы некоторого критического уровня. Следует отметить, что значение данного порога достаточно сильно варьируется для пользователей с различным опытом работы с клавиатурой и может колебаться от 6 до 30 символов. После этого предела даже у квалифицированных машинисток наблюдается эффект включения сознательного мышления и остановок в наборе текста для принятия решения. В соответствии с изложенными выводами можно говорить о том, что в системах аутентификации пользователя по особенностям клавиатурного почерка не рекомендуется использовать слишком длинные выражения в качестве ключевой фразы, так как это приводит к тому, что пользователь начинает «осмысленно» выполнять набор [1].

Г.А. Цанниева и Н.Р. Гасанова предлагают следующий алгоритм. Система аутентификации пользователя по клавиатурному почерку должна работать в трёх режимах:

– режим обучения (в нем определяются и сохраняются эталонные характеристики клавиатурного почерка пользователя);

– режим анализа (в нем система сравнивает эталонные характеристики с вновь введёнными, после чего может оставаться в режиме анализа или перейти в режим блокировки);

– режим блокировки (в этом режиме система просит ввести пароль, который будет проверен на подлинность и вновь пройдет анализ клавиатурного почерка; если все пройдет успешно, то программа перейдет в режим анализа).

Сбор биометрической информации о работе пользователя происходит при помощи замеров времен удержаний клавиш и интервалов между нажатиями клавиш, после этого полученные результаты формируются в матрицу межсимвольных интервалов и вектор времен удержаний клавиш. После

того как сбор биометрической информации будет выполнен, полученные данные сравниваются с эталонными значениями, а затем происходит процесс фильтрации полученных результатов. Затем принимается решение, пройдена аутентификация или нет. Принятие решения заключается в том, что аутентификация считается положительной, если процентное содержание результатов соотношений характеристик меньше определенного порога. Если процентное содержание пиков превышает предельно допустимое значение, то результат аутентификации считается отрицательным. Если аутентификация была отрицательной, то выдается сообщение, которое предлагает подтвердить подлинность пользователя. При положительном результате аутентификации пользователь продолжает работу над прикладной задачей, и процесс аутентификации остается незаметным [2].

Таким образом, систематизируя выше сказанное, можно констатировать актуальность проблемы разработки методов биометрической аутентификации вообще и по клавиатурному почерку в частности, а также преимущества и недостатки аутентификации по клавиатурному почерку.

Преимущества:

1. Простота реализации и внедрения. Реализация исключительно программная, ввод осуществляется со стандартного устройства ввода (клавиатуры), а значит – использование не требует приобретения никакого дополнительного оборудования. Это самый дешевый способ аутентификации по биометрическим характеристикам субъекта доступа.

2. Не требует от пользователя никаких дополнительных действий и навыков. Пользователь, так или иначе, наверняка использует пароль, который можно назначить парольной фразой, по которой будет проводиться аутентификация. Возможно, мошеннику удастся получить логин и пароль для входа в систему, но вот скопировать клавиатурный почерк не представляется возможным.

3. Возможность скрытой аутентификации – пользователь может не знать, что включена дополнительная проверка, а значит, не сможет сообщить об этом злоумышленнику.

Недостатки:

1. Требуется обучение приложению.

2. Сильная зависимость от эргономичности клавиатуры (в случае замены клавиатуры придется обучать программу заново).

3. Сильная зависимость от психофизического состояния оператора [3].

Рассмотренные методы могут применяться в комплексе с другими механизмами для решения задач аутентификации. Во-первых, это может быть повышение защищенности информационных ресурсов в организациях с высокими требованиями к защите информации. Во-вторых, благодаря анализу психофизического состояния данные методы могут применяться в организациях, в которых необходимо обеспечить высокий уровень концен-

трации внимания сотрудников во время работы. Основным достоинством методов является отсутствие необходимости использования дополнительного оборудования, что позволяет создавать гибкие настраиваемые подсистемы аутентификации и мониторинга действий оператора информационной системы. Однако, несмотря на свои достоинства, это направление мало изучено и весьма перспективно. Аутентификация лишь с использованием анализа клавиатурного почерка неприемлема в системах, требующих высокого уровня защиты, но в сочетании с другими системами аутентификации может оказаться весьма эффективной. Существующие программные реализации систем аутентификации на основе клавиатурного почерка пока не обладают достаточной достоверностью [1], поэтому актуальна разработка новых методов, алгоритмов, программно-аппаратных реализаций, повышающих эффективность систем идентификации и аутентификации.

Библиографический список

1. Аверин, А.И. Аутентификация пользователей по клавиатурному почерку / А.И. Аверин, Д.П. Сидоров. – URL: http://journal.mrsu.ru/wp-content/uploads/2015/10/averin-sidorov.pdf.

2. Цанниева, Г.А. Клавиатурный почерк как способ аутентификации и идентификации пользователя / Г.А. Цанниева, Н.Р. Гасанова. – URL: https://www.scienceforum.ru/2016/1802/26053.

3. Агурьянов, И. Клавиатурный почерк как средство аутентификации / И. Агурьянов. – URL: http://www.securitylab.ru/blog/personal/aguryanov/29985.php.

4. Сбербанк планирует опознавать клиентов по движению губ: РИА Новости. – Выступление Г. Грефа на лекции в МФТИ. – URL: https://ria.ru/economy/20170316/1490208132.html.

К содержанию