DOI 10.36622/VSTU.2023.26.2.011
УДК 004.056

БИОМЕТРИЯ ПАРОЛЬНОГО ВВОДА: НОВАЯ МОДЕЛЬ АУТЕНТИФИКАЦИИ

В.А. Минаев, И.С. Стручков

В статье рассматривается возможность усиления метода аутентификации сочетанием пароля и клавиатурного почерка пользователя на входе в компьютерную систему. Для обоснования новой биометрической модели аутентификации рассматриваются результаты экспериментов по замерам забывания информации, полученные в XIX веке немецким психологом Г. Эббингаузом. Выдвигается и проверяется гипотеза, что процесс ввода пользователем пароля с клавиатуры характеризуется кривой экспоненциального типа, когда вначале скорость ввода минимальна, соответственно, время ввода – максимально, а затем по мере новых повторений скорость ввода увеличивается, а время ввода уменьшается, стремясь к некоторому пределу. При этом для каждого пользователя наблюдаются характерные только ему параметры экспоненциальной кривой. Для построения модели клавиатурного почерка с 30 участниками проведены эксперименты по изучению его динамических параметров. Мерой соответствия между теоретической и экспериментальной кривой, а также критерием аутентификации пользователя служит значение коэффициента детерминации R^2. Анализ результатов моделирования показал, что участники эксперимента делятся на три типологические группы в пространстве параметров клавиатурного почерка. Группы значимо различаются гендерными и психологическими признаками, отражающими типохарактер пользователя.

Ключевые слова: биометрический метод, аутентификация, клавиатурный почерк, кривая забывания, математическая модель, типология.

Введение

В условиях стремительного роста значимости информации все более серьезными становятся угрозы информационной безопасности [1]. Усиливаются и системы защиты информации, включая методы аутентификации, основанные на биометрических характеристиках пользователей [2-4].

Сегодня у современных пользователей существуют десятки способов оставить свой след при входе в информационные системы и сети, иные места контролируемого доступа [5-8]. Биометрические технологии позволяют идентифицировать пользователя по его уникальным биологическим характеристикам – отпечаткам пальцев, свойствам радужной оболочки глаза, параметрам голоса, и многому другому.

Первые примеры биометрической защиты появились несколько столетий назад, но с развитием информационных технологий системы биометрическая аутентификации стали активно набирать обороты. И уже в нынешнем веке трудно встретить мобильный телефон, в котором не применяется разблокировка по отпечатку пальца или распознаванию лица собственника.

Сейчас биометрические системы используют уже несколько факторов аутентификации, за счет чего технологии распознавания все более приближаются к 100% гарантии. Такими факторами могут быть характеристики человека, параметры аппаратных устройств или нечто нематериальное, например, парольная аутентификация.

Аутентификация по сути – это мера безопасности, применяемая для защиты данных путем дополнительного ввода информации, гарантирующей подлинность пользователя.

Обычно выделяют два подхода к аутентификации – однофакторную и многофакторную. К первому относится процесс проверки индивида, например, парольного ввода. Второй подход реализует метод проверки, требуя от индивида предоставления большего объема идентифицирующей информации.

Очевидно, что для доступа к системе наиболее приемлема многофакторная аутентификация, когда уязвимость

защищаемой системы существенно снижается. Такая аутентификация подходят для предприятий и организаций, работающих с конфиденциальными данными.

Биометрическая аутентификация весьма необходима в сфере использования персональных данных для установления подлинности индивида. В этой связи в Федеральном законе № 152 «О персональных данных» от 27 июля 2006 года сформулирована статья 11 «Биометрические персональные данные», в которой четко указано, что подлинность человека можно установить на основании его уникальных биометрических характеристик. А в статье 19 «Меры по обеспечению безопасности персональных данных при их обработке» указано, что эти данные должны защищаться от неправомерного и случайного доступа.

Нужно также отметить, что в национальных стандартах по биометрии одним из основных стал ГОСТ Р ИСО\МЭК 19794 2013 года [2], в котором указаны требования к биометрическим параметрам человека и их измерению. В стандарте разъясняется порядок применения биометрических признаков и указаны виды аутентификации - простая, усиленная или строгая.

Существуют основные показатели безопасности биометрической аутентификации – вероятности ошибок первого (запрещаем доступ легальному пользователю) и второго рода (разрешается доступ злоумышленнику), характеризующие любую биометрическую систему. Эти две вероятности взаимосвязаны настолько, что, например, делая информационную систему более защищенной от злоумышленника, проектант в то же время увеличивает вероятность отказа легальному пользователю.

Из сказанного следует вывод, что биометрическая аутентификация представляет собой эффективный метод проверки подлинности личности пользователя. Каждый из методов имеет свои преимущества и недостатки, завися от конкретного контекста применения. Второй вывод связан с тем, что регулирование биометрической аутентификации осуществляется с учетом нормативно-правовых документов, обеспечивающих защиту персональных данных, приватности и прав пользователя. Наконец, третий вывод отражает констатацию того, что применение аутентификации по биометрическим характеристикам эффективно при необходимости повышении уровня информационной защиты.

Биометрический метод аутентификации удобен по сравнению с парольным вводом с его сложным сочетанием цифр и букв, подчас осуществляемым в разных регистрах и алфавитах. Да еще и украсть могут пароль или подсмотреть.

А почему бы, исходя из этих опасений, не использовать для проверки сочетание пароля и клавиатурного почерка на входе? Клавиатурного почерка пользователя, который нельзя потерять или забыть?

Да, потерять-то невозможно, ну, только, если вместе с головой! А вот забыть…?

О кривой забывания информации

Кривая забывания информации является ключевым понятием в области психологии памяти [1], описывая этот процесс во времени. Причем запомненные факты или материалы вначале утрачиваются быстро, а затем темп забывания замедляется. Как показали эксперименты Г. Эббингауза еще в XIX веке, кривая забывания похожа на экспоненциальную [9], как на рис. 1.

Рис. 1. Кривая забывания по Эббингаузу [9]

Основываясь на своих наблюдениях, Эббингауз выявил, что наиболее резкое забывание происходит в течение первых двадцати минут и является значительным в

течение первого часа. Общий важный вывод, сделанный выдающимся психологом, заключается в том, что после каждого последовательного замера в памяти сохраняется все меньше информации. Он также заметил, что люди склонны к лучшему запоминанию, если распределить повторения по времени. “Интервальное повторение” сегодня является ключевым принципом при реализации образовательного процесса.

Подобное поведение кривой забывания привело авторов настоящей статьи к идее выдвижения гипотезы, что процесс ввода пользователем пароля с клавиатуры характеризуется кривой экспоненциального типа, когда вначале время скорость ввода минимальна, соответственно, время ввода – максимально, а затем по мере новых повторений скорость ввода увеличивается, а время ввода уменьшается, стремясь к некоторому пределу. При этом для каждого пользователя наблюдаются характерные только ему параметры экспоненциальной кривой.

Заметим, что для более точной аутентификации важно учитывать следующие факторы:

- к забыванию и вводу неверного пароля может привести стресс;
- на способность концентрироваться и запоминать влияет усталость;
- причиной ошибок может стать отвлечение пользователя при вводе пароля.

Модель клавиатурного почерка

Для моделирования клавиатурного почерка проведены эксперименты по изучению изменения скорости ввода пароля в зависимости от времени, прошедшего с их начала. При этом исследовались режимы ввода 8-ми символьного пароля, состоящего из цифр и букв. Время ввода τ оценивалось до десятой доли секунды с помощью специально разработанной программы.

Анализ периода ввода одного и того же пароля τ, выраженного в секундах, показал, что он снижается в зависимости от времени t, прошедшего с начала экспериментов, по экспоненте вида:

$$\tau = \alpha \cdot \exp(-\beta \cdot t) + \gamma, \qquad (1)$$

где α, β – коэффициенты, определяемые экспериментально применительно к каждому пользователю, длине и составу пароля,

γ – минимальное время ввода пароля при многократном повторении последнего. Очевидно, последний из указанных параметров зависит как условий эксперимента

В том случае, когда происходит подмена пользователя или изменение условий ввода (принуждение пользователя, изменение его психического состояния, изменение пароля и т. п.) в динамике экспериментальной кривой происходят существенные вариации.

Мерой соответствия между теоретической (1) и экспериментальной кривой может служить значение коэффициента детерминации R^2 [2]. Исходя из того, что коэффициенты α и β устойчивы применительно к одному и тому же пользователю, R^2 может использоваться для его аутентификации при вводе пароля. При его значениях, ниже определенного критерия, происходит отказ в доступе к компьютерной системе.

Проведенные эксперименты [10] позволили сделать вывод, что, если значение коэффициента R^2 больше или равно 95 %, то аутентификация пройдена успешно, и пользователь может приступить к работе на компьютере.

Если значение коэффициента R^2 больше 80 %, но меньше 95 %, то администратору информационной системы необходимо обратить на это внимание и разобраться в причинах, почему пользователь не показывает устоявшиеся характеристики аутентификации при тех же условиях ввода пароля, которые были ранее.

Когда значение коэффициента R^2 меньше 80 %, и система аутентификации не пропускает пользователя, то необходимо тщательно разобраться: нет ли подмены пользователя, не передан ли пароль постороннему лицу, соответствует ли психофизиологическое состояние пользователя нормальному для него.

Экспериментальная часть

Для построения модели клавиатурного почерка с 30 участниками проведены

эксперименты по изучению его динамических параметров. Каждый участник вводил заранее определенные логин и пароль в специальную программу, которая подсчитывала время ввода пароля на каждом шаге эксперимента. Исследование осуществлялось для каждого испытуемого в течение 10 часов с дискретом в один час. В рамках проведения эксперимента все участники вводили с клавиатуры пароль одинаковой длины, содержащий как цифры, так и буквы.

Далее строилась зависимость времени ввода пароля от текущего времени проведения эксперимента. Результаты эксперимента визуализировались в виде построения экспериментальной и теоретической кривых экспоненты.

На рис. 2 показан пример сравнения экспериментальной и теоретической кривой. Очевидно их хорошее согласование, R^2 = 97%. Это означает, что данная кривая объясняет 97% вариации экспериментальной кривой.

Такие сравнения проведены для всех 30 участников эксперимента. Сравнения показали, что коэффициент R^2 варьировался в диапазоне 80-99%, что свидетельствует об очень хорошем Чтобы снизить влияние посторонних факторов на результаты (громкий отвлекающий шум, телефонные разговоры, резкие движение вокруг, домашние животные, отвлекающие сообщения и т.д.), всем участникам экспериментов были обеспечены одинаковые условия.

Таким образом, подтверждена гипотеза о том, что экспоненциальная модель хорошо описывает эмпирические данные о зависимости времени ввода пароля от текущего времени эксперимента. Эта модель, описывающая клавиатурный почерк пользователя, достаточно устойчива и может применяться при аутентификации пользователей компьютерных систем и сетей. В табл. 1 представлены данные по всем 30 участникам экспериментов, где представлены параметры клавиатурного почерка при вводе пароля и коэффициент детерминации.

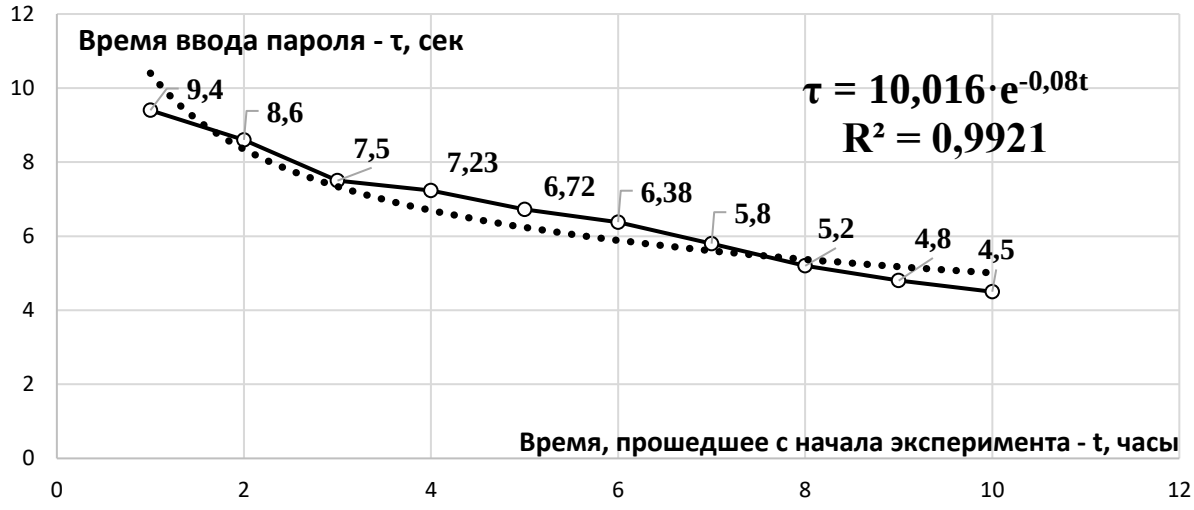

Рис. 2. Зависимость времени ввода пароля от текущего времени эксперимента (сплошная – эксперимент, пунктирная – теория)

Углубленный анализ данных табл. 1 привел к формированию еще одной гипотезы, а именно о делении участников, вводивших пароль, на достаточно однородные типологические группы по параметрам клавиатурного почерка α и β. Рассмотрим результаты типологизации.

Типологизация пользователей по клавиатурному почерку

Общий подход к построению типологической модели таков – пользователи различаются параметрами клавиатурного почерка, и сам парольный ввод у них разный.

Таблица 1

Параметры моделей пользователей, вводящих алфавитно-цифровые пароли

Номер участника	α	β	R^2
1	14,232	0,097	87%
2	14,917	0,091	96%
3	13,925	0,098	87%
4	13,829	0,08	95%
5	11,338	0,046	94%
6	10,351	0,075	92%
7	7,4878	0,048	86%
8	10,016	0,08	99%
9	8,7234	0,039	88%
10	11,343	0,078	97%
11	12,628	0,094	93%
12	12,785	0,077	98%
13	13,145	0,114	94%
14	14,218	0,087	98%
15	10,171	0,072	95%
16	11,859	0,071	93%
17	11,672	0,111	98%
18	10,491	0,074	98%
19	11,049	0,107	93%
20	11,892	0,105	93%
21	9,7902	0,087	97%
22	9,3708	0,069	92%
23	6,5965	0,039	80%
24	7,5566	0,056	91%
25	6,4027	0,036	84%
26	8,0435	0,046	81%
27	8,8228	0,075	95%
28	5,8255	0,049	93%
29	6,3755	0,047	82%
30	6,7915	0,048	86%

Типологизация участников экспериментов осуществлена в пространстве параметров парольного ввода α и β – рис. 3.

Результаты показали, что все участники делятся на три группы:

– с относительно низкими параметрами α и β,

– со средними параметрами α и β,

– с относительно высокими параметрами α и β.

Так, в первой группе участник в среднем характеризовался следующими показателями: α = 7,4441; β = 0,0453.

Во второй группе участник в среднем характеризовался следующими показателями: α = 11,52158; β = 0,0756.

И, наконец, в третьей группе участник характеризовался следующими усредненными показателями: α = 11,9366; β = 0,1092.

То есть, выделенные группы наибольшим образом различались параметром β. Так, вторая группа отличается от первой по нему в 1,7 раза; третья группа от второй по нему же – в 1,4 раза, в то же время третья группа от первой – в 2,4 раза.

Это свидетельствует о том, что параметр, характеризующий скорость увеличения ввода пароля со временем, является доминирующим.

Отметим, что различие по параметру α между второй и первой группой составляет 1,55 раза, в то же время между третьей и второй группой различия практически нет, а между третьей и первой группами – в 1,6 раза.

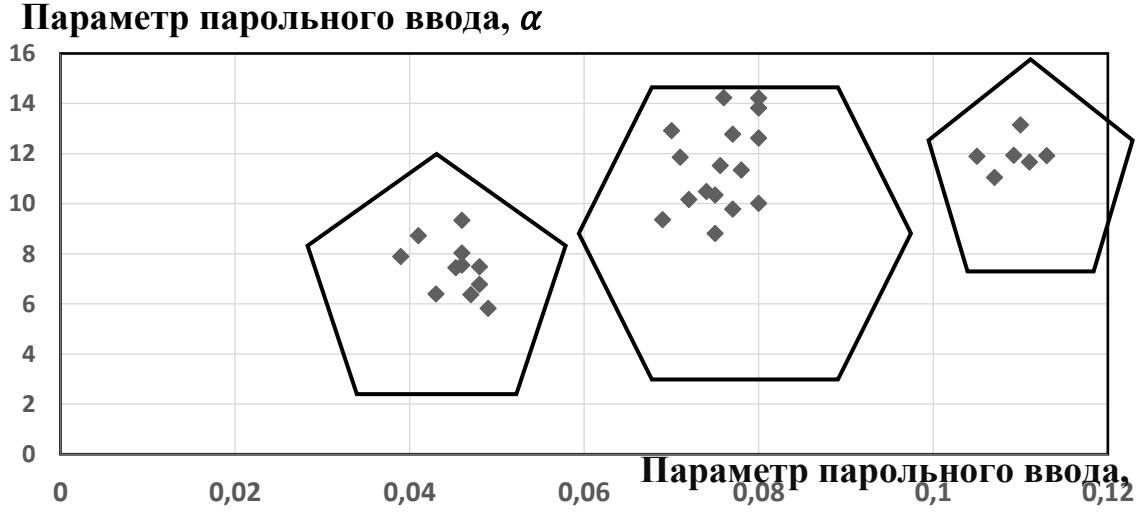

Рис. 3. Типологические группы пользователей по параметрам ввода пароля

Анализ участников эксперимента, вошедших в первую группу, показал, что в ней преобладают женщины. На основе анализа индивидуальных особенностей, определяющих поведение и психические процессы участников данной группы, выяснено, что в ней преобладает холерический темперамент, характеризующий участников сильной впечатлительностью и большой импульсивностью, а также резко меняющимся настроением. В меньшей степени в ней присутствует меланхолический темперамент, характеризующий участников склонностью к переживанию различных событий и наличием неустойчивого настроения.

Во вторую группу вошли участники, характеризующиеся малой импульсивностью, устойчивым настроением. Участники группы обладают флегматичным и сангвиническим типами личности, проявляют упорство и настойчивость в работе, оставаясь уравновешенными, рассудительными, осмотрительными.

В третью группу вошли участники, которые имеют сравнительно высокие параметры α и β. В большей степени – это мужской пол, быстрее адаптирующегося к работе. В группе преобладают участники с сангвиническим и холерическим темпераментом. К этому типу относятся открытые и оптимистичные люди. Они дисциплинированы, обладают хорошей

способностью к концентрации и самоконтролю,

Результаты решения задачи типологизации показали, что гипотеза о делении участников эксперимента на различающиеся однородные группы по параметрам клавиатурного почерка подтверждена.

Обсуждение и выводы

Учитывая, что при защите информации и персональных данных особую роль играет аутентификация личности, возникла необходимость разработки методов, позволяющих, с одной стороны, быстро, а, с другой стороны, качественно осуществлять указанную процедуру.

В статье показано, что среди биометрических признаков, отличающихся легкостью получения, надежностью аутентификации и низкой стоимостью реализации является технология парольного входа, совмещенная с оценкой параметров модели клавиатурного почерка.

Параметры модели, характеризующие величину скорости ввода в начальный момент и величину ее увеличения в течение времени, прошедшего с начала экспериментов, устойчивы для каждого конкретного пользователя. Именно, этой устойчивостью параметров следует руководствоваться при аутентификации.

Необходимо также учитывать типологизацию пользователей, разделенных на однородные группы, с тем, чтобы иметь дополнительную информацию об их психотипических, гендерных и иных характеристиках.

Как показали эксперименты, такая дополнительная информация дает возможность с б*о*льшей точностью аутентифицировать пользователя.

Заключение

Разработанная авторами модель является важным шагом в области совершенствования аутентификации и способствует повышению надежности и достоверности проверки подлинности субъектов доступа.

Технология парольного входа среди биометрических признаков отличается надежностью аутентификации и низкой стоимостью реализации.

Проведенное исследование типологизации пользователей по параметрам клавиатурного почерка при парольном вводе в компьютерную систему позволяет получить дополнительную информацию о психологических характеристиках, позволяющих более точно аутентифицировать пользователя.

Перспективы развития результатов исследования связывается с изучением характеристик парольного ввода в различных стрессовых условиях работы пользователей. А также исследовать другие психологические характеристики личности.

Кроме того, целесообразно увеличение в выборке испытуемых для возможно большей дифференциации групп с целью получения дополнительной информации о пользователях при аутентификации.

Список литературы

1. Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646 // Собрание законодательства РФ.

2. ГОСТ Р ИСО/МЭК 19794-5-2013. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. М.: Стандартинформ, 2013. – 36 с.

3. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. М.: Стандартинформ, 2020. – 32 с.

4. Болл Р.М., Коннел Дж.Х., Панканти Ш., Рахта Н.К., Сеньор Э.О. Руководство по биометрии. М.: Техносфера, 2007. – 386 с.

5. Минаев В. А., Королев И. Д., Сабанов А. Г. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия // Вестник УрФУ. Безопасность в информационной сфере. 2018. № 3 (30). – С. 43-49.

6. Сабанов А. Г. Особенности аутентификации при доступе к облачным сервисам // Вестник Нижегородского университета им. Н.И. Лобачевского. 2013. № 2-1. – С. 47-52.

7. Брагина Е.К., Соколова С.С. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития // Вестник

Астраханского государственного технического университета. 2016. № 1 (61). – С. 40-45.

8. Сабанов А. Г. Классификация процессов аутентификации // Вопросы защиты информации. 2013. № 3. – С. 49-58.

9. Эббингауз Г. Основы психологии / Перевод с немецкого Г.А. Котляра; под редакцией В.С. Серебреникова, Э.Л. Радлова. Санкт-Петербург: Типография товарищества «Общественная польза», 1911-1912. – 660 с.

Московский университет МВД РФ им. В.Я. Кикотя
Moscow University of the Internal Affairs Ministry of Russia

Поступила в редакцию 10.05.23

Информация об авторах

Минаев Владимир Александрович – д-р техн. наук, профессор, профессор кафедры специальных информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: m1va@yandex.ru

Стручков Илья Сергеевич – старший преподаватель кафедры специальных информационных технологий учебно-научного комплекса информационных технологий, Московский университет МВД РФ им. В.Я. Кикотя, Москва, e-mail: pikia91@mail.ru

PASSWORD ENTRY BIOMETRICS: NEW AUTHENTICATION MODEL

V.A. Minaev, **I.S. Struchkov**

The article discusses the possibility of strengthening the authentication method by combining a password and a user's keyboard handwriting at the entrance to a computer system. To substantiate the new biometric authentication model, the results of experiments on measurements of forgetting information obtained in the XIX century by the German psychologist G. Ebbinghaus are considered. The hypothesis is put forward and tested that the process of entering a password by the user from the keyboard is characterized by an exponential curve, when at first the input speed is minimal, respectively, the input time is maximal, and then as new repetitions occur, the input speed increases and the input time decreases, tending to a certain limit. At the same time, for each user, the exponential curve parameters characteristic only of him are observed. To build a model of keyboard handwriting, experiments were conducted with 30 participants to study its dynamic parameters. The value of the determination coefficient R2 serves as a measure of the correspondence between the theoretical and experimental curve, as well as the user authentication criterion. Analysis of the simulation results showed that the participants of the experiment are divided into three typological groups in the space of keyboard handwriting parameters. The groups differ significantly in gender and psychological characteristics reflecting the type of character of the user.

Keywords: biometric method, authentication, keyboard handwriting, information forgetting curve, mathematical model, typology.

Submitted 10.05.23

Information about the authors

Vladimir A. Minaev – Dr. Sc. (Technical), Professor, Professor of the Special Information Technologies Department, Moscow University of the Internal Affairs Ministry of Russia, Moscow, Russian Federation, e-mail: m1va@yandex.ru

Ilya S. Struchkov – Senior Lecturer of the Special Information Technologies Department of the Educational and Scientific Complex of Information Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, Moscow, Russian Federation, e-mail: pikia91@mail.ru