

С. М. Иванова, канд. техн. наук, доц., e-mail: sm-ivanova@yandex.ru,
З. В. Ильиченкова, канд. техн. наук, доц., e-mail: zilyichenkova@yandex.ru,
А. А. Антонова, канд. техн. наук, доц., e-mail: antonova.an.an@gmail.com,
Федеральное государственное бюджетное образовательное учреждение
"МИРЭА — Российский технологический университет", Москва

Проверка подлинности пользователя при работе в обучающих системах

Рассматривается проблема проверки подлинности личности обучающегося, работающего в образовательной среде. Анализ проводится на основе сформированного кластерного клавиатурного почерка. Рассматриваются способы посимвольного и общего контроля, проверки отдельных символов и средних значений при различных комбинациях символов. Представлены экспериментальные данные, показавшие работоспособность предложенного метода проверки.

Ключевые слова: *клавиатурный почерк, обучающие системы, кластеризация символов, контроль пользователя*

Введение. Подходы к проверке подлинности обучающихся

На сегодняшний день дистанционные образовательные технологии становятся все более популярными. Возможность изучать весь материал или его часть удаленно позволяет повысить эффективность занятий за счет наиболее удобного распределения времени обучения в соответствии с собственными образовательными потребностями [1, 2]. К несомненным достоинствам использования дистанционных образовательных технологий относятся:

- возможность планирования времени обучения, отводящегося на тот или иной раздел курса, согласно индивидуальной скорости овладения материалом;
- допустимость выбора тем для изучения или их последовательности в процессе обучения;
- возможность организации обучения по личному, а не групповому графику;
- мобильность за счет индивидуализации стратегии взаимодействия с преподавателем;
- возможность использования современных образовательных технологий;
- равные образовательные возможности вне зависимости от объективных возможностей, связанных с полом обучающегося, удаленностью места жительства от места обучения, состоянием его здоровья и т.д.;
- повышение объективности в силу использования формального оценивания и отсутствия персонализированного отношения к обучающемуся.

К недостаткам использования дистанционных образовательных технологий следует отнести:

- возможность подмены легитимного обучающегося сторонним пользователем на этапе обучения в случае, когда доступ к курсу организуется с применением разграничения полномочий (например, по логину и паролю);
- возможность подмены экзаменуемого на этапе проведения аттестации по курсу;
- невозможность осуществления непосредственного общения для получения ответов на возникающие вопросы при некоторых формах организации обучения [3, 4].

Данные проблемы заметным образом нивелируют значительные достоинства обучения в дистанционном режиме. Поэтому необходимо разрабатывать такие вспомогательные методы при организации образовательного процесса, которые позволят исключить перечисленные недостатки.

В связи с тем, что достоинства использования дистанционных образовательных технологий значительны, необходимо направить усилия на сглаживание или ликвидацию перечисленных выше недостатков.

В настоящее время уже существуют различные механизмы контроля обучающихся при проведении итоговой аттестации [5, 6]. Однако в связи с тем, что данные мероприятия требуют хотя и удаленного, но присутствия человека-проктора, осуществляющего визуальный контроль за учащимся, непосредственно процесс обучения и выполнение текущих заданий остается без внимания организаторов курса и

требует создания автоматических методов проверки подлинности.

Существующие методы прокторинга дают возможность лишь сигнализировать о возможном нарушении, но не позволяют принять взвешенное решение о доступе к среде обучения.

1. Формирование клавиатурного почерка.

Кластерный подход

Так как обучающие системы всегда содержат информацию об обучающихся, имеющих право на прохождение курса, представляется целесообразным при разработке способа контроля подлинности использовать данные, хранящиеся в системе.

Поскольку чаще всего аутентификация в среде обучения осуществляется с использованием логина и пароля, то имеет смысл использовать при организации контроля какой-либо механизм, основанный на тех же данных. Например, для указанной цели можно сформировать на этапе регистрации пользователя его клавиатурный почерк, основанный, например, на длительности нажатия на клавиатурные символы. Тогда при занятиях ученика в образовательной среде появляется возможность опираться на полученные данные [7–9].

Использование компьютерного почерка в процессе обучения предполагает периодический ввод какой-либо информации, который осуществляется либо в постоянном режиме (при выполнении заданий), либо может быть инициирован при переходе от одного блока обучения к другому. Таким образом, использование биометрических характеристик позволит проводить мониторинг учащихся в автоматическом режиме в течение всего периода обучения [10].

Однако работа с использованием всех символов клавиатуры, характерная для выполнения различного рода заданий во время обучения, не позволяет ограничиться только парольной фразой для формирования компьютерного почерка.

Недостаточность этого определяется различными характеристиками почерка, создаваемого при использовании различных знаков. Также нельзя характеристики почерка, сформированного по ограниченному набору символов, применять для проверки подлинности по любой другой фразе.

Поэтому предлагается при исходном определении почерка использовать кластерный подход, т. е. символы с похожими характеристиками объединить в наборы и хранить информацию о среднем значении и среднеквадратичном отклонении для знаков каждого из сформированных кластеров. Данный метод является

эффективным в силу того, что проведение экспериментов показало различие в длительности нажатия на часто используемые символы клавиатуры и прочие знаки. Иными словами, использование ограниченного набора символов или создание единого почерка, полученного при использовании всей клавиатуры, не является целесообразным для решаемой задачи.

При формировании клавиатурного почерка учащегося с формированием кластеров все символы клавиатуры объединяются в группы согласно близости их статистических характеристик. Если говорить о вводе в процессе обучения данных, содержащих только слова, состоящие из букв русского алфавита, то требуется распределить по кластерам 31 соответствующий знак (без букв "ё" и "ь"). Сформированный подобным образом клавиатурный почерк будет хранить информацию о числе кластеров, наборе символов в каждом кластере, среднем значении и среднеквадратичной ошибке. Данная информация является достаточной для характеристики индивидуальных особенностей клавиатурного почерка конкретного пользователя.

Например, для данных, полученных в процессе формирования клавиатурного почерка пользователя, представленных в табл. 1, при делении на 5 кластеров по формуле минимизации расстояния между двумя символами

Таблица 1

Символ	Число нажатий	Среднее значение длительности (10^{-6} с)	Среднеквадратичное отклонение (10^{-6} с)	Символ	Число нажатий	Среднее значение длительности (10^{-6} с)	Среднеквадратичное отклонение (10^{-6} с)
й	6	46483,83	280,807	р	2	46819,50	123,744
ц	3	46289,67	334,378	о	5	47112,20	235,093
у	6	46467,83	296,569	л	5	46049,40	265,168
к	2	46968,50	402,344	д	6	45951,67	186,370
е	4	47063,25	273,778	ж	4	46182,00	166,775
н	4	46892,75	386,125	э	2	46201,00	295,571
г	5	46953,20	355,546	я	4	46607,75	433,556
ш	2	45793,50	382,545	ч	5	46556,20	330,595
щ	4	46016,75	398,044	с	2	46152,00	197,990
з	2	46273,00	229,103	м	4	47134,75	390,416
х	6	45908,33	338,797	и	3	46843,33	314,475
ф	6	46495,67	369,703	т	5	47020,40	247,824
ы	4	46395,00	422,176	ь	4	46035,75	124,759
в	6	46660,83	341,338	б	6	46003,50	158,054
а	2	46204,00	203,647	ю	5	46127,40	354,528
п	6	46987,00	345,979				

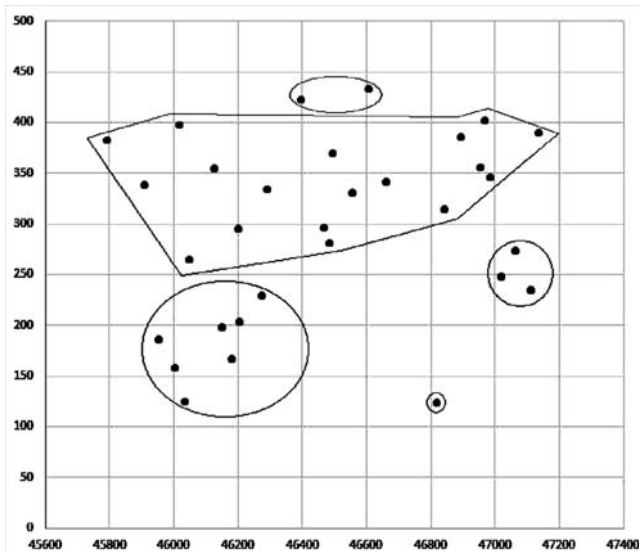


Рис. 1. Распределение символов по кластерам (по оси x расположены длительности, по оси y — СКО)

$$\rho_{ij} = \sqrt{(d_i - d_j)^2 + (s_i - s_j)^2},$$

где d_i — среднее значение длительности нажатия на i -й символ; s_i — значение среднеквадратичного отклонения (СКО) для i -й символа, получаются кластер 1 "й у в ч ф к н г п м и ц ю э л щ ш х", кластер 2 "е о т", кластер 3 "з а с ж д б ь", кластер 4 "ы я", кластер 5 "р" (рис. 1).

Средние значения и СКО, рассчитанные согласно данным табл. 1, для кластеров 1—5 соответственно равны 46499,43 и 489,121 (кластер 1), 47065,43 и 234,143 (кластер 2), 46071,54 и 189,172 (кластер 3), 46501,38 и 412,160 (кластер 4), 46819,50 и 123,744 (кластер 5).

2. Проверка почерка пользователя при кластерном подходе

Имея сформированный клавиатурный почерк, необходимо определить подлинность обучающихся в процессе работы. Иными словами, требуется проверить, соответствуют ли характеристики вводимой фразы сформированному клавиатурному почерку. В данном случае нет необходимости пытаться отнести находящегося в системе ученика к тому или иному пользователю, так как он авторизовался на сайте. Следовательно, необходимо принять решение, является ли ученик именно тем субъектом, за которого он себя выдает.

На основании общих принципов проверки клавиатурного почерка задача сводится к отнесению текущих характеристик к ранее сформированному классу почерка. Нужно определить, попадают ли длительности символов \tilde{x} , вводимых с клавиатуры в процессе работы

в системе, в некоторый допустимый интервал $(x_{k,\min}, x_{k,\max})$, формируемый согласно статистической модели для соответствующего кластера k . Указанные диапазоны предварительно формируются для каждого кластера согласно его статистическим характеристикам. Одним из хорошо зарекомендовавших себя способов является определение границ диапазона с помощью функции Лапласа, которая дает возможность учитывать имеющуюся информацию о среднем значении длительности нажатия на соответствующие символы, входящие в кластер, и среднеквадратичном отклонении:

$$P(x_{k,\min} < \tilde{x} < x_{k,\max}) = \Phi\left(\frac{x_{k,\max} - \bar{x}_k}{\sigma_k}\right) - \Phi\left(\frac{\bar{x}_k - x_{k,\min}}{\sigma_k}\right),$$

где $\Phi(\cdot)$ — функция Лапласа; \bar{x}_k — среднее значение длительности нажатия на символы кластера k ; σ_k — СКО для кластера k .

В зависимости от необходимой жесткости принятия решения можно варьировать значение вероятности. Его увеличение позволяет принимать решение в пользу находящегося в системе ученика (увеличивается число ошибок второго рода — постороннее лицо может быть принято за авторизованного пользователя). Снижение вероятности повышает число отказов добросовестному пользователю (увеличивается число ошибок первого рода).

Так как искомый диапазон должен быть симметричным, то вероятность можно записать в виде

$$P(x_{k,\min} < \tilde{x} < x_{k,\max}) = 2\Phi\left(\frac{x_{k,\max} - \bar{x}_k}{\sigma_k}\right).$$

Для заранее определенного значения вероятности при заданных среднем и среднеквадратичном отклонении определяются границы диапазона.

В классическом варианте проверки подлинности пользователя решение о его добросовестности принимается на основе информации о том, попадают ли текущие значения в найденный диапазон. При кластерном подходе может возникнуть ситуация, когда по некоторым кластерам решение положительное, а по другим — отрицательное. В этом случае необходимо определить механизм, определяющий, считать обучающегося подлинным или злоумышленником.

Существуют несколько подходов к решению данной проблемы. К наиболее перспективным можно отнести принятие решения:

- по всем результатам (личность подтверждается, только когда по всем кластерам принято положительное решение);

- по большинству результатов (если кластеров, подтверждающих почерк, не меньше, чем остальных, то личность пользователя подтверждается).

Так как решение принимается по разным наборам, то оно может также зависеть от частоты проверки, т. е. от той комбинации символов, которые проверяются одновременно. Контроль может идти после:

- ввода каждого символа;
- ввода одного ответа, являющегося словом.

В первом случае учитывается длительность нажатия на каждый знак. Во втором случае определяется среднее значение для разных нажатий на один и тот же символ или на все символы одного кластера.

Различные подходы к принятию решения предлагается рассмотреть на конкретных экспериментальных данных, полученных при анализе информации о работе добросовестного и постороннего пользователей в системе.

3. Принятие решения о подлинности пользователя

В обоих случаях пользователям предлагалось ввести слово "сложносочиненное", являющиеся ответом на вопрос задания. В данном слове содержатся символы только из трех первых кластеров, поэтому статистическую информацию (допустимый диапазон длительности нажатия) будем рассматривать только для них.

Согласно среднему значению и СКО, рассчитанному для каждого из наборов данных, допустимые интервалы при вероятностях попадания, равных 0,95 и 0,85 соответственно, представлены в табл. 2.

Рассмотрим соотношение экспериментальных данных с полученными диапазонами при разных подходах к анализу статистической информации.

Для добросовестного пользователя были получены данные о длительности нажатия на клавиши, представленные в табл. 3.

Упорядочивание по кластерам для облегчения обработки данных показано в табл. 4.

Средние длительности нажатий на каждый символ показаны в табл. 5, а на все символы одного кластера целиком — в табл. 6.

Рассмотрим попадание в требуемые диапазоны всех нажатых символов ответа согласно полученным значениям длительности в зависимости от выбранного допустимого диапазона вероятности (0,85 и 0,95).

Как видно из диаграммы (рис. 2), все символы, кроме одного, попали в требуемые интервалы для обоих значений вероятности. Зна-

Таблица 2

Кластеры	Вероятность			
	0,85		0,95	
	Минимум	Максимум	Минимум	Максимум
1	46450,53	46548,33	46432,88	46565,98
2	46973,31	47157,55	46940,05	47190,81
3	46028,36	46114,72	46012,77	46130,31

Таблица 3

Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)
с	46142,0	с	46277,0	е	48004,25
л	46246,4	о	46915,2	н	46812,75
о	47164,2	ч	46480,2	н	46902,75
ж	45998,0	и	46943,33	о	47360,2
н	46666,75	н	46675,75	е	46828,25
о	46914,2				

Таблицы 4

Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)
л	46246,4	и	46943,33	е	48004,25
н	46666,75	о	47164,2	е	46828,25
н	46675,75	о	46914,2	с	46142,0
н	46812,75	о	46915,2	с	46277,0
н	46902,75	о	47360,2	ж	45998,0
ч	46480,2				

Таблица 5

Символ	Число нажатий	Среднее значение длительности (10^{-6} с)
л	1	46246,4
н	4	46764,5
ч	1	46480,2
и	1	46943,33
о	4	47088,45
е	2	47416,25
с	2	46209,5
ж	1	45998,0

Таблица 6

Символ кластера	Число нажатий	Среднее значение длительности (10^{-6} с)
Кластер 1	7	46675,4
Кластер 2	6	47197,7
Кластер 3	3	46139,0

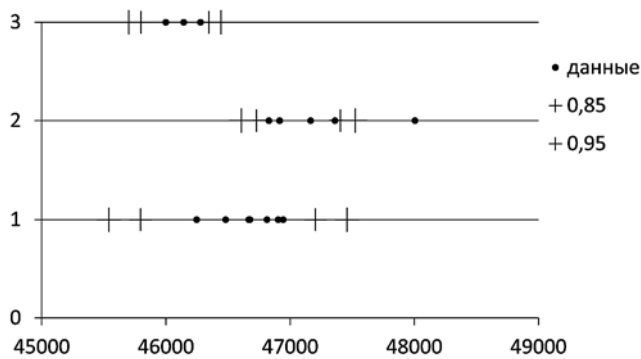


Рис. 2. Диаграмма попадания длительности нажатия на символы добросовестным пользователем в доверительный интервал (по оси x расположены длительности, по оси y — кластеры)

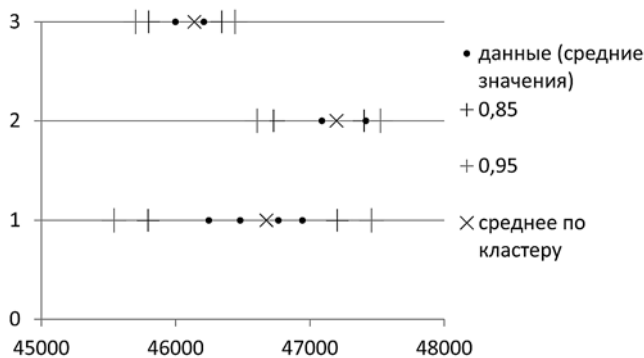


Рис. 3. Диаграмма попадания средних значений длительности нажатия на символы добросовестным пользователем в доверительный интервал (по оси x расположены длительности, по оси y — кластеры)

чение, не попавшее в интервал, может быть отнесено к "грубой ошибке", так как значение сильно отличается (по абсолютной величине) ото всех данных по длительности. Таким образом, подтвердить подлинность обучающегося можно только при условии игнорирования данного выброса. Данный анализ позволяет говорить о нецелесообразности контроля почерка после ввода каждого символа в ответе, так как случайные выбросы будут приводить к принятию неправильного решения для добросовестного пользователя.

Анализ данных по каждому символу позволяет принять правильное решение при условии игнорирования "грубых ошибок". Альтернативой данному методу является анализ средних значений, полученных для одних и тех же символов или для знаков всего кластера в целом.

На диаграмме (рис. 3) отражены значения, полученные при нахождении указанных средних. Почерк можно идентифицировать как соответствующий добросовестному пользователю при условии построения доверительного интервала с вероятностью 0,95 для средних значений по символам или при рассмотрении средних значений по всему кластеру.

Для того чтобы принять решение о наиболее адекватном способе принятия решения, необходимо проанализировать данные "злоумышленника" (другого пользователя) относительно характеристик почерка исследуемого обучающегося.

Для злоумышленника были получены данные о длительности нажатия на клавиши, представленные в табл. 7.

Упорядочивание по кластерам для облегчения обработки данных показано в табл. 8.

Так же, как и для добросовестного пользователя, вычислим необходимые для анализа средние длительности нажатий на каждый символ (табл. 9) и на все символы одного кластера целиком (табл. 10).

Диаграмма попадания в требуемые диапазоны (они сформированы относительно данных

Таблица 7

Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)
с	46104,0	с	46259,0	е	46500,2
л	46237,4	о	47258,2	н	46758,75
о	47077,2	ч	47177,25	н	46698,75
ж	46225,0	и	46668,33	о	46888,2
н	46695,75	н	47044,75	е	46704,2
о	46868,2				

Таблица 8

Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)	Символ	Значение длительности (10^{-6} с)
л	46237,4	и	46668,33	е	46500,2
н	46695,75	о	47077,2	е	46704,2
н	47044,75	о	46868,2	с	46104,0
н	46758,75	о	47258,2	с	46259,0
н	46698,75	о	46888,2	ж	46225,0
ч	47177,25				

Таблица 9

Символ	Число нажатий	Среднее значение длительности (10^{-6} с)
л	1	46237,4
н	4	46799,5
ч	1	47177,25
и	1	46668,33
о	4	47022,95
е	2	46602,2
с	2	46181,5
ж	1	46225,0

Таблица 10

Символ кластера	Число нажатий	Среднее значение длительности (10^{-6} с)
Кластер 1	7	46754,4
Кластер 2	6	46882,7
Кластер 3	3	46196

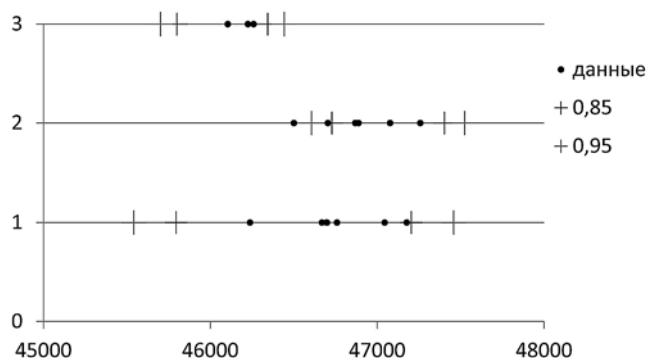


Рис. 4. Диаграмма попадания длительности нажатия на символы "злоумышленником" в доверительный интервал (по оси x расположены длительности, по оси y — кластеры)

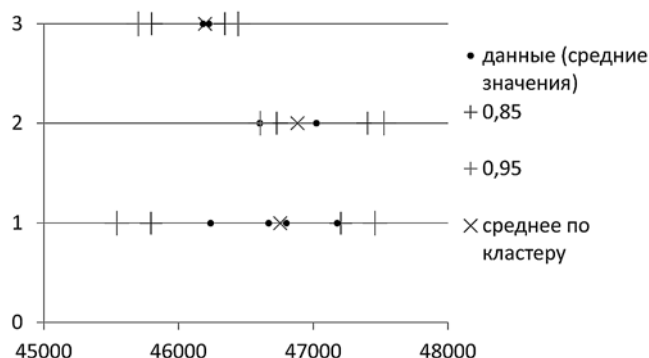


Рис. 5. Диаграмма попадания средних значений длительности нажатия на символы "злоумышленником" в доверительный интервал (по оси x расположены длительности, по оси y — кластеры)

почерка добросовестного пользователя) представлена на рис. 4.

"Грубые ошибки" при вводе отсутствуют (или можно считать таковой одно значение из кластера 1 — значение для символа "л", — которое, тем не менее, попало в требуемый диапазон). Одно из значений второго кластера не попало в диапазон при вероятности 0,95, и два значения — при вероятности 0,85. Таким образом, как и в случае добросовестного пользователя, в кластере 2 присутствуют посторонние значения, однако их характер отличается от ошибок, наблюдаемых в первом случае.

Анализ средних значений, полученных для одних и тех же символов или для знаков всего кластера в целом (рис. 5) дает непопадание одного среднего значения (по символу "е") ни в один, ни в другой доверительный интервалы в кластере 2. Средние значения по кластерам

позволяют сделать неверный вывод о том, что "злоумышленник" является добросовестным пользователем.

Заключение

Проанализировав все полученные данные, можно сделать вывод о возможности проверки подлинности пользователя по кластерному клавиатурному почерку.

Из рассмотренных методов не является удовлетворительным способ оценивания по среднему значению по всем символам кластера. Вероятнее всего, это определяется тем, что комбинация нескольких различных символов дает значительный разброс данных и увеличивает, тем самым, СКО. Поэтому допустимый интервал получается большим и включает усредненные значения практически любого пользователя.

Также, видимо, следует исключить способ принятия окончательного решения по наибольшему числу принятых решений для кластеров в отдельности. Пример показывает, что и в том, и в другом случае почерк подтверждается только по кластерам 1 и 3 и не подтверждается только по кластеру 2, что составляет меньшую часть, т. е. будет принято неверное решение относительно "злоумышленника".

Принятие решения по среднему для нескольких одинаковых символов возможно при использовании доверительного интервала, полученного для вероятности 0,95. Однако следует понимать, что для символов, употребляемых однократно, средние значения будут совпадать с исходными данными, и "грубые ошибки", попадающие на такие знаки, не будут нивелированы.

Использование всех знаков как самостоятельных позволяет принять верное решение при игнорировании "грубых ошибок". Для этого необходимо проводить анализ после ввода ответа целиком, чтобы иметь возможность оценить характер значения, не попавшего в диапазон. Также в этом случае отрицательное решение может быть принято, если в доверительный интервал не попало более одного значения длительности.

Таким образом, достоинством предложенного метода проверки подлинности пользователя является повышение точности принятия решения в автоматическом режиме. Недостатком метода является необходимость хранения большего объема данных по каждому обучающемуся, характеризующих его клавиатурный почерк. Однако возможность использования предложенного метода для проверки подлинности обучаемого во время его работы в образовательной среде дает возможность сделать вывод о перспективности его использования.

Список литературы

1. Антонова И. И., Магомедов Ш. Г., Сумкин К. С., Кобыш А. Н. Повышение качества электронного образования методами бенчмаркинга // Развитие современного образования: теория, методика и практика. 2017. № 1 (11). С. 38–41.
2. Саркисова И. О. Использование специализированной ЭОС для повышения эффективности обучения мультиязычных групп // Ученые записки института социальных и гуманитарных знаний. 2019. № 1(17). С. 439–443.
3. Мотозов А. В., Иванова И. А. Проблемы реализации и работы с пиринговыми сетями // Телекоммуникации и информационные технологии. 2018. Т. 5, № 1. С. 122–125.
4. Ефромеева Е. В., Смирнова И. А. Автоматизированная система для управления работой по поиску информации на основе анализа обработанных обращений // Вестник МГТУ Станкин. 2019. № 1 (48). С. 118–121.
5. Бахвалова Т. Н., Белкин М. Е., Гладышев И. В., Кудж С. А., Сигов А. С. Фотонная технология как способ совершенствования ключевых технических показателей устройств задержки радиосигналов // Российский технологический журнал. 2017. Т. 5, № 3 (17). С. 4–21.
6. Иванова С. М., Ильиченкова З. В. Идентификация аттестационных работ при реализации электронного обучения с применением дистанционных образовательных технологий // Вестник МГТУ Станкин. 2015. № 2 (33). С. 116–118.
7. Брюхомицкий Ю. А. Гистограммный метод распознавания клавиатурного почерка. // Известия ЮФУ. Технические науки. Тематический выпуск. С. 55–62. URL: <https://cyberleninka.ru/article/v/gistogrammnyy-metod-raspoznavaniya-klaviaturnogo-pocherka>.
8. Иванова С. М., Ильиченкова З. В. Аутентификация пользователей мобильных устройств по клавиатурному почерку // Вестник МГТУ Станкин. 2018. № 2 (45). С. 85–89.
9. Шарипов Р. Р., Ситников А. Н. Проблемы при разработке систем распознавания пользователей по клавиатурному почерку // Вестник технологического университета, 2019. Т. 22, № 10. С. 143–147.
10. Алешникова Е. А., Чадина Ю. А. Аксиологизация работы с текстом на уроках русского языка в старшей школе // Русский язык в школе. 2019. Т. 80, № 1. С. 46–49.

S. M. Ivanova, Assistant Professor, e-mail: sm-ivanova@yandex.ru,
Z. V. Ilyichenkova, Assistant Professor, e-mail: zilyichenkova@yandex.ru,
A. A. Antonova, Assistant Professor, e-mail: antonova.an.an@gmail.com,
MIREA — Russian Technological University, Moscow

User Authentication in Training Systems

The problem of verifying the identity of a student who works in an online educational system is discussed in the article. This is necessary to prohibit the substitution of one user for another upon receipt of information or in the process of performing certification work. Verification is carried out on the basis of the student's keyboard handwriting, formed according to the cluster principle. Symbols with similar characteristics are clustered. For each cluster, statistical characteristics are calculated. The authentication method in the process is very important. It is proposed to consider the methods of character-by-character data control or verification after entering the entire answer in order to ensure the correct decision. For this, approaches were used to analyze each symbol individually or average values for various combinations of symbols. During the study, a number of experiments were carried out and the data obtained are presented in the work. Studies have shown efficiency of the proposed user authentication method. Monitoring cluster average values was considered impractical, since large confidence intervals almost always include the average. The most successful is checking after entering the whole word. Next, you should remove the "glaring errors" or calculate the average values for each character, if there are several of them in the answer. In the latter case, the confidence interval must be constructed, based on the probability of occurrence, equal to 0.95.

Keywords: keyboard handwriting, learning systems, character clustering, user control

DOI: 10.17587/it.26.648-654

References

1. Antonova I. I., Magomedov Sh.G., Sumkin K. S., Kobyshev A. N. Improving the quality of electronic education using benchmarking methods, *Development of modern education: theory, methodology and practice*, 2017, no. 1 (11), pp. 38–41 (in Russian).
2. Sarkisova I. O. The use of specialized EOS to increase the effectiveness of teaching multilingual groups, *Scientific notes of the Institute of Social and Humanitarian Knowledge*, 2019, no. 1(17), pp. 439–443 (in Russian).
3. Motozov A. V., Ivanova I. A. Problems of implementation and work with peer-to-peer networks, *Telecommunications and Information Technologies*, 2018, vol. 5, no. 1, pp. 122–125 (in Russian).
4. Efromeeva E. V., Smirnova I. A. Automated system for managing information retrieval based on the analysis of processed calls, *Vestnik MGTU Stankin*, 2019, no. 1 (48), pp. 118–121 (in Russian).
5. Bakhvalova T. N., Belkin M. E., Gladyshev I. V., Kuj S. A., Sigov A. S. Photon technology as a way to improve key technical indicators of radio signal delay devices, *Russian Technology Journal*, 2017, vol. 5, no. 3 (17), pp. 4–21 (in Russian).
6. Ivanova S. M., Ilyichenkova Z. V. Identification of certification work in the implementation of e-learning using distance educational technologies, *Vestnik MGTU Stankin*, 2015, no. 2 (33), pp. 116–118 (in Russian).
7. Bryukhomitsky Yu. A. Histogram method of recognition of keyboard handwriting, *News of SFU. Technical science*, Thematic issue, pp. 55–62, available at: <https://cyberleninka.ru/article/v/gistogrammnyy-metod-raspoznavaniya-klaviaturnogo-pocherka/> (in Russian).
8. Ivanova S. M., Ilyichenkova Z. V. Authentication of users of mobile devices by keyboard handwriting, *Vestnik MSTU Stankin*, 2018, no. 2 (45), pp. 85–89 (in Russian).
9. Sharipov R. R., Sitenkov A. N. Problems in the development of user recognition systems by keyboard handwriting, *Bulletin of the Technological University*, 2019, vol. 22, no. 10, pp. 143–147 (in Russian).
10. Alekhnikova E. A., Chadina Y. A. Axiological working with text on lessons of the Russian language in high school, *Russian language in school*, 2019, vol. 80, no. 1, pp. 46–49 (in Russian).