УДК 621.369:534 **DOI:10.30837/rt.2021.4.207.15**

Д.Ю. ГОРЕЛОВ, канд. техн. наук, Е.А. ИВАНОВА канд. техн. наук,
А.В. ЛИТВИНЕНКО, А.А. ДОВБНЯ, Д.А. МИНИН

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ КЛАВИАТУРНОГО ПОЧЕРКА ДЛЯ ЗАДАЧ ИДЕНТИФИКАЦИИ СТУДЕНТОВ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

Введение

При использовании систем дистанционного образования (СДО) возникает проблема информационной безопасности учебного процесса, которая, кроме внешних, подразумевает также и внутренние угрозы. Одной из таких угроз может стать студент СДО, который заплатил мошеннику за сдачу тестов и создал видимость учебной деятельности под своим именем. Таким образом, нелегальное получение диплома или сертификата получает удобный механизм реализации.

Использование традиционных методов идентификации в СДО имеет два существенных недостатка: во-первых, неоднозначность идентифицируемого пользователя, поскольку в данном случае установление личности пользователя происходит по введенной парольной фразе; во-вторых, отсутствие возможности обнаружения подмены идентифицированного пользователя в процессе работы с системой (пользователь, заинтересованный в завышении результата оценки знаний, может авторизоваться и передать управление компьютером постороннему лицу). Указанные недостатки устраняются при использовании биометрических методов скрытного мониторинга.

В связи с пандемией коронавируса, начавшейся в 2019 году, актуальность задачи [1 – 7], решаемой в данной статье, резко возросла, поскольку СДО стали использоваться в многих странах вместо традиционного очного обучения.

Обзор методов скрытного биометрического мониторинга

Для решения проблемы распознавания пользователей в СДО необходимо проводить идентификацию не только при входе пользователя в систему, но и регулярно с некоторой периодичностью в течение всего пользовательского сеанса. Таким образом, следует использовать биометрические методы скрытного мониторинга, которые удовлетворяют следующим требованиям: отсутствие необходимости в дополнительном аппаратном оснащении компьютера (ноутбука); простота сбора и анализа биометрических признаков в процессе работы в СДО; возможность идентификации незаметно для пользователя.

Указанным требованиям соответствуют методы идентификации по геометрии лица, по голосу и по клавиатурному почерку [8].

Преимущества идентификации по геометрии лица:

− имеющиеся в личных делах студентов фотографии могут быть использованы в качестве биометрических эталонов;

− бесконтактный и ненавязчивый процесс идентификации;

– идентификацию можно осуществлять в процессе любой деятельности пользователя в СДО: при изучении учебно-методических материалов, сдаче тестов, общении с преподавателем.

Недостатки идентификации по геометрии лица:

– нарушается право на частную жизнь (в процессе идентификации важно именно незаметное использование фронтальной камеры монитора – в противном случае злоумышленникам будут известны промежутки времени, когда у экрана должен находиться студент, а когда – злоумышленник);

– высокая чувствительность алгоритмов распознавания к изменениям положения головы или ракурса, освещения (если студент предпочитает обучаться вечером при выключенном свете в комнате, то его идентификация становится затруднительной).

Преимущества идентификации по голосу – надежность, гибкость и высокие показатели точности. Технология развивается достаточно продолжительное время и сегодня существует большое количество алгоритмов [9], устойчивых к изменяющимся условиям применения – уровню шума, фонемам речи конкретного человека, техническим характеристикам микрофона и т.д.

Недостатки идентификации по голосу:

– возможное отсутствие микрофона у студента СДО;

– голос человека может кардинально измениться из-за болезней, например во время сезонной эпидемии гриппа;

– специфика контрольных тестов: идентификация применима только в случае, если проверка знаний осуществляется при помощи устных ответов на вопрос.

Клавиатурный почерк – уникальный стиль работы на клавиатуре [10], зависящий от таких параметров как: количество пальцев, задействованных во время набора текста; длительность нажатия клавиш; время между нажатиями клавиш; использование основной или дополнительной части клавиатуры; характер сдвоенных или строенных нажатий; излюбленные сочетания горячих клавиш и т.д.

Преимущества идентификации по клавиатурному почерку:

– простота реализации и внедрения (реализация исключительно программная, ввод осуществляется со стандартного устройства ввода – клавиатуры. Это самый дешевый способ аутентификации по биометрическим характеристикам);

– возможность полностью легальной скрытой аутентификации на протяжении всего пользовательского сеанса;

– простота интеграции в мультимодальные биометрические системы (клавиатурный почерк плюс динамика мыши, клавиатурный почерк плюс геометрия лица и т.д.).

Недостатки идентификации по клавиатурному почерку:

– на корректность работы алгоритма аутентификации достаточно сильно влияет психофизическое состояние пользователя;

– для корректной работы алгоритма аутентификации необходим стабильный клавиатурный почерк, который вырабатывается у пользователей, давно работающих на компьютере, следовательно, данный метод нельзя использовать для новичков.

Таким образом, с учетом того, что оценка знаний, как правило, проходит в форме тестирования, наиболее предпочтительным методом идентификации пользователей в системах дистанционного обучения является использование алгоритмов скрытного клавиатурного мониторинга.

Информативные параметры клавиатурного почерка и специфика дистанционного контроля знаний

В задаче идентификации пользователя по клавиатурному почерку основным этапом является анализ и обработка первичных данных. После данной операции входной информативный поток делится на ряд характеристик, которые отражают те или иные динамические признаки набора текста пользователем, который проходит идентификацию. Далее данные признаки позволяют получить ряд уникальных характеристик пользователя.

В настоящее время можно выделить три класса информативных параметров клавиатурного почерка [11, 12].

1. Временные характеристики отдельных событий клавиатуры (монографов), например, абсолютная длительность удержания клавиши, абсолютная длительность паузы перед клавишей, абсолютная длительность паузы после клавиши, отношение длительности паузы перед клавишей к длительности удержания клавиши, отношение среднего значения длитель-

ности удержания конкретной клавиши к среднему значению длительности удержания всех клавиш и т.д.

Информативные параметры монографов клавиатуры формируются для каждой клавиши отдельно, следовательно, обладают важным недостатком: исследуемые интервалы времени всегда связаны с конкретной клавишей и рассчитываются независимо от клавиш, которые нажимались до и после, т.е. не несут информации о динамике набора текста.

2. Временные характеристики последовательных событий клавиатуры (на рис.1 два последовательных события клавиатуры образуют дограф, три последовательных события – триграф, n последовательных событий клавиатуры – n-граф), например, абсолютное значение и распределение длительности всех диграфов в заданном тексте (параметры $t_{A_D B_U}$, $t_{B_D C_U}$ на рис. 2), абсолютные значения и распределения времен между нажатиями (параметры $t_{A_D B_D}$, $t_{B_D C_D}$ на рис. 2) и времен между отпусканиями (параметры $t_{A_U B_U}$, $t_{B_U C_U}$ на рис. 2) клавиш всех диграфов в заданном тексте и т.д.

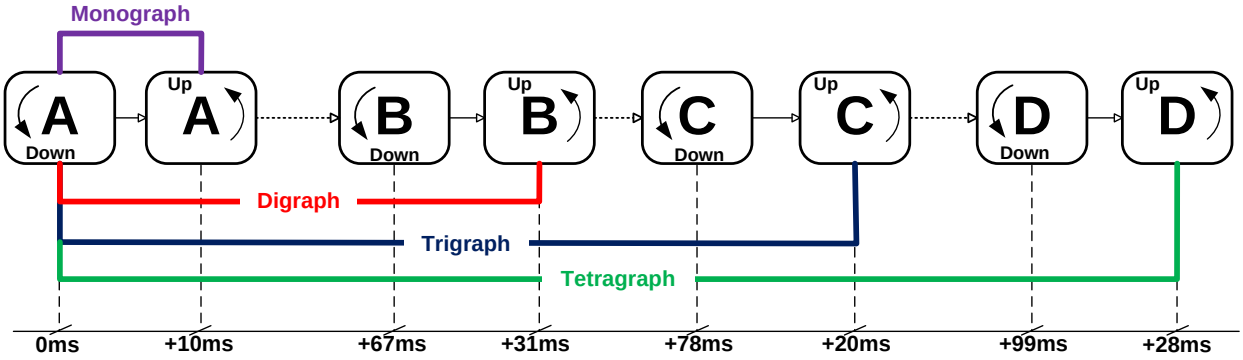

Рис. 1. *N*–графы клавиатуры

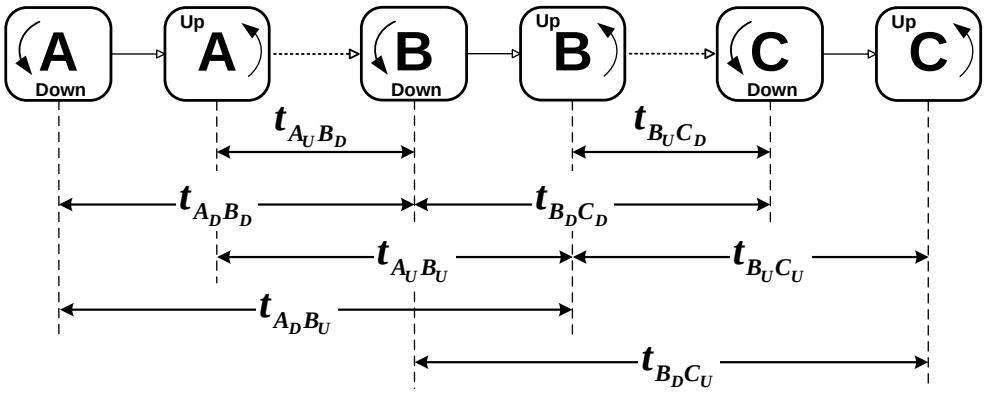

Рис. 2. Временные параметры диграфов клавиатуры

Информативные признаки последовательных событий клавиатуры точнее передают особенности клавиатурного почерка, но также имеют недостаток: для их получения необходимо иметь в несколько раз больший набор данных, чем для получения предыдущей группы характеристик. Также следует отметить, что согласно [13 – 15] переход к анализу отношений временных параметров диграфов, например, $\frac{t_{A_D B_D}}{t_{A_U B_D}}$ и $\frac{t_{A_D B_D}}{t_{A_U B_U}}$, приводит к «нормализации» закона распределения исследуемых признаков, то есть «случайность» изменения параметров клавиатурного почерка уменьшается.

3. Интегральные характеристики набора текста, например, скорость набора символов, скорость набора слов, степень аритмичности набора, количество исправлений, количество и особенности перекрытий (случай нажатия второй клавиши, когда еще не отпущена первая),

распределение частот использования клавиш изменения регистра, пропуск определенных букв в определенных буквосочетаниях/словах, опечатки определенных букв в определенных буквосочетаниях/словах и тому подобное.

Класс интегральных информативных характеристик клавиатурного почерка в сочетании с любым из первых двух классов дает максимальную точность, однако требует значительных затрат на разработку, внедрение и поддержку подобных систем.

В технологиях дистанционного обучения, которые использует мировая педагогическая практика, тестированию уделяется значительное внимание. Хотя тестирование как форма аттестации не является идеальной, однако в дистанционном обучении именно тесты чаще всего представляют собой залог качества полученных знаний.

В настоящее время используется много разновидностей тестов. Условно их можно поделить на две группы [16].

Первая группа – тесты с выбираемыми ответами, их разновидности: 1) тесты опознания – это задания, требующие альтернативного ответа: «согласен» или «не согласен», «да» или «нет» и т.п.; 2) тесты различения – содержат варианты ответов, из которых надо выбрать один или несколько; 3) тесты соотнесения – в них предлагается найти общее или отличное в объектах, соотнося их по свойствам, параметрам, классам и т.д.; 4) тесты-задачи – дается условие задачи, нужные данные и варианты ответов в цифровой или буквенной форме. Студенту нужно выбрать правильный вариант. Задача также может быть сформулирована таким образом, что студенту нужно выбрать правильную последовательность действий и операций или определить зависимость каких-то факторов.

Все эти тесты рассчитаны на проверку знаний-представлений и, отчасти, понимания материала. Такие тесты в наибольшей степени подходят для текущего контроля, а также для самоконтроля.

Вторая группа тестов не содержит вариантов ответов. Такие тесты используются для проверки понимания материала, а также некоторых умений. К ним относятся: 1) тесты-подстановки – в таких заданиях пропущены некоторые составляющие – слова, элементы схем, графиков, и студент должен заполнить пропуски; 2) конструктивные тесты не содержат подсказок и вариантов ответов и требуют от студента самостоятельного конструирования ответа: написания формулы, формулировки свойств, операционной последовательности, выполнения схемы и т.д. Эти тесты, в свою очередь, делятся на два подвида: 1) тесты-задачи – отличие от подобной разновидности первой группы в том, что в нем не предлагаются варианты ответов; тесты-процессы – предназначаются для проверки подготовленности студентов к разработке содержания и последовательности различных процессов.

Таким образом, для использования алгоритмов скрытного клавиатурного мониторинга в задаче идентификации пользователей СДО необходимо:

1) использовать тесты, не содержащие вариантов ответов;

2) использовать тесты при текущем контроле знаний, т.е. в конце каждой лекции или практического занятия (поскольку для формирования биометрического эталона нужно несколько сеансов);

3) использовать тесты с большим количеством вопросов, т.к. объемы текстов, которые вводятся при ответе на каждый вопрос весьма незначительны;

4) использовать тесты с численными ответами. В данном случае анализируются только десять клавиш (цифры от 0 до 9) и 100 возможных диграфов, следовательно, получить необходимую для расчетов «статистику» достаточно легко.

Статическая и динамическая идентификация пользователей по клавиатурному почерку

Идентификация по клавиатурному почерку может быть разделена на два типа: статическая (парольная) и динамическая (непрерывная). Статическая идентификация – это проверка и сопоставление характеристик почерка в процессе набора определенной текстовой последо-

вательности, например логина и пароля пользователя. Непрерывная идентификация направлена на постоянный анализ почерка пользователя во время работы за клавиатурой с целью выявления и сопоставления особенностей почерка.

Парольной идентификации характерен ограниченный набор данных и, как следствие, худшая по сравнению с динамической идентификацией точность. В СДО парольную идентификацию следует использовать как вспомогательное средство в двух случаях, во-первых, когда основной модуль скрытного мониторинга не дал точного идентификационного решения; во-вторых, когда факт сдачи теста третьим лицом уже установлен и по динамике набора парольной фразы проводится идентификация этого лица с целью добавления его в черный список.

Можно выделить два этапа скрытой идентификации пользователя: качественный и количественный. Первый обнаруживает различия в заранее выявленных индивидуальных особенностях работы с клавиатурой легального пользователя. Это использование альтернативных служебных клавиш (например, клавиши Backspace и Delete, CapsLock и правый/левый Shift) использование клавиш дополнительной клавиатуры и др. Эти особенности проявляются на подсознательном уровне, и попытка контролировать их неизбежно отразится на изменении динамики почерка. Второй этап предусматривает продление сбора и анализа ключевых временных характеристик клавиатурного почерка после того, как пользователь уже вошел в систему. Таким образом, мониторинг характера клавиатурной активности выполняется в течение всей рабочей сессии под конкретным аккаунтом. По мере накопления статистических данных происходит уточнение сходства эталона по вновь сформированной совокупности параметров.

Описание алгоритма формирования профиля пользователя и его идентификации

1. Сочетанием качественного и количественного подходов является анализ диграфов ответов-чисел вида «клавиша А – десятичный разделитель», «десятичный разделить – клавиша А» и «клавиша А – клавиша В».

К качественному подходу относятся:

1) распределение частот использования групп цифровых клавиш, а также знаков «плюс» и «минус» – основная или вспомогательная клавиатура (рис. 3);

2) распределение частот использования клавиш-разделителей целой и дробной части – клавиши «,» и «.» в английской раскладке, клавиши «б», «ю» и «.» в украинской раскладке, клавиша «,» на вспомогательной клавиатуре в английской/украинский раскладке.

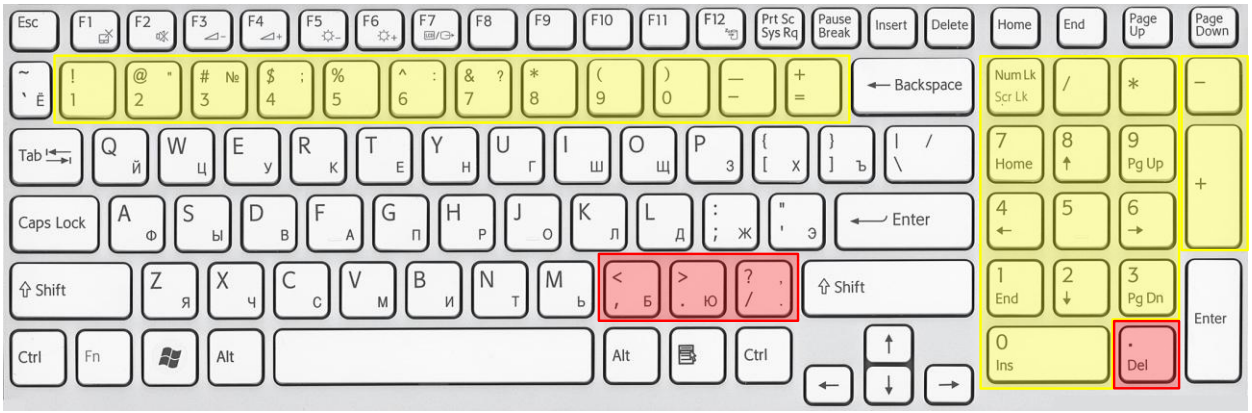

Рис. 3. Разделение клавиш клавиатуры на функциональные блоки

1. Количественный подход начинается с формирования профиля пользователя путем накопления данных о временных интервалах каждого диграфа введенных пользователем ответов-чисел:

$$T_1 = \begin{vmatrix} t_{1A_DB_D} \\ t_{2A_DB_D} \\ \dots \\ t_{N_{AB}A_DB_D} \end{vmatrix}, \quad T_2 = \begin{vmatrix} t_{1A_UB_D} \\ t_{2A_UB_D} \\ \dots \\ t_{N_{AB}A_UB_D} \end{vmatrix}, \quad T_3 = \begin{vmatrix} t_{1A_UB_U} \\ t_{2A_UB_U} \\ \dots \\ t_{N_{AB}A_UB_U} \end{vmatrix}, \quad T_4 = \begin{vmatrix} t_{1A_DB_U} \\ t_{2A_DB_U} \\ \dots \\ t_{N_{AB}A_DB_U} \end{vmatrix}, \qquad (1)$$

где N_{AB} – количество повторений диграфа «AB».

2. Пять процентов самых быстрых и пять процентов медленных диграфов изымаются из анализа. Таким образом, можно исключить случайные хаотичные нажатия клавиш – быстрые диграфы и случаи, когда пользователь отвлекся на длительное время и нажал одну кнопку – медленные диграфы.

3. ***Подалгоритм 1.*** Построение профиля и правило идентификации пользователя на основе девиации Δt_{AB} длительности диграфов (клавиши «A» и «B» принимают значения «.», «0», «1», … «9»).

3.1. Для каждого диграфа рассчитывается значение относительной девиации длительности:

$$\Delta t_{AB} = \frac{1}{N_{AB} \cdot \Delta t} \sum_{i=1}^{N_{AB}} t_{A_DB_U\,i}, \qquad (2)$$

где средняя длительность по всем возможным диграфам равна:

$$\Delta t = \frac{1}{L} \sum_{j=1}^{L} t_{X_DY_U\,j}, \qquad (3)$$

L – общее количество диграфов; клавиши «X» и «Y» принимают значения «.», «0», «1», … «9».

3.2. По результатам п. 3.1 строится табличный профиль пользователя (табл. 1), причем значения относительной девиации записываются в таком формате:

если $\Delta t_{AB} \geq 1$, то $\Delta t_{AB} = 1$;

если $\Delta t_{AB} < 1$, то $\Delta t_{AB} = -1$.

Таблица 1

Пример формирования профиля пользователя

Первая клавиша диграфа	Вторая клавиша диграфа	Параметр Δt_{AB}
.	0	1
.	1	-1
.	2	1
.	3	1
.	4	-1
.	5	-1
.	6	1
.	7	-1
.	8	1
.	9	1
0	.	-1
0	0	1
0	1	1
0	2	-1
…	…	…
9	7	-1
9	8	1
9	9	-1

3.3. На втором шаге (по окончании второго текущего контроля знаний) уточняется профиль пользователя:

1) рассчитывается новое среднее значение длительности диграфов Δt;
2) рассчитываются новые значения относительной девиации Δt_{AB};
3) строится новый табличный профиль пользователя;
4) профили объединяются по формуле (табл. 2):

$$\Delta t_{AB} = \Delta t_{AB1} + \Delta t_{AB2} = \begin{cases} 2, & \textit{если} \;\; \Delta t_{AB1} = \Delta t_{AB2} = 1, \\ -2, & \textit{если} \;\; \Delta t_{AB1} = \Delta t_{AB2} = -1, \\ 0, & \textit{ели} \;\; \Delta t_{AB1} \neq \Delta t_{AB2}. \end{cases} \qquad (4)$$

3.4. На третьем шаге (по окончании третьего текущего контроля знаний) уточняется профиль пользователя:

1) рассчитывается новое среднее значение длительности диграфов Δt;
2) рассчитываются новые значения относительной девиации Δt_{AB};
3) строится новый табличный профиль пользователя;
4) профили объединяются по формуле

$$\Delta t_{AB} = \Delta t_{AB1} + \Delta t_{AB2} + \Delta t_{AB3} = \begin{cases} \pm 3, & если \quad \Delta t_{AB1} = \Delta t_{AB2} = \Delta t_{AB3}, \\ \pm 1, & если \quad \Delta t_{AB1} \neq \Delta t_{AB2} \neq \Delta t_{AB3}. \end{cases} \quad (5)$$

3.5. На шестом шаге (по окончании шестого текущего контроля знаний) формируется табличный профиль пользователя. Значения параметров Δt_{AB} после объединения становятся равными $\{-6;\ -4;\ -2;\ 0;\ 2;\ 4;\ 6;\}$. Сформированный профиль графически (рис. 4) удобно представлять в виде двух 3D диаграмм.

Таблица 2

Пример формирования уточненного профиля пользователя

Первая клавиша диграфа	Вторая клавиша диграфа	Параметр Δt_{AB1}	Параметр Δt_{AB2}	Параметр Δt_{AB}
.	0	1	1	2
.	1	-1	1	0
.	2	1	-1	0
.	3	1	1	2
.	4	-1	-1	-2
.	5	-1	1	0
.	6	1	1	2
.	7	-1	-1	-2
.	8	1	-1	0
9	7	-1	-1	-2
9	8	1	-1	0
9	9	-1	-1	-2

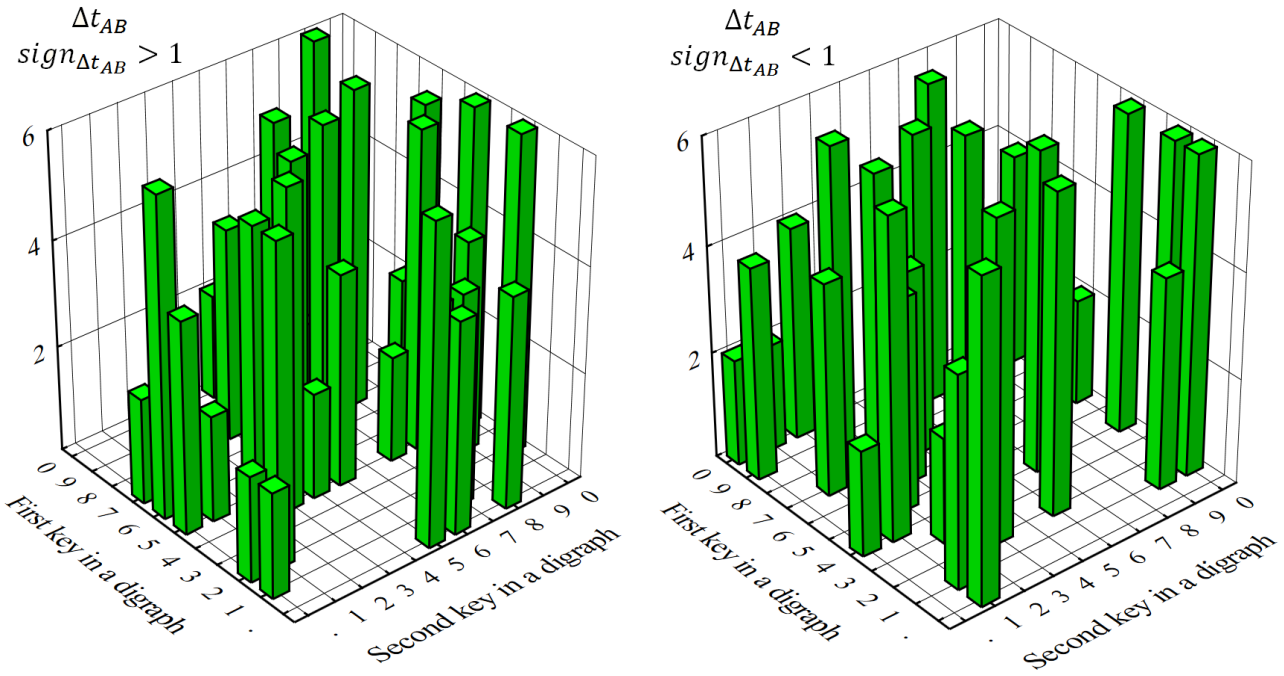

Рис. 4. Пример представления профиля пользователя в виде 3D диаграмм

3.6. Формируется вектор биометрического профиля пользователя:

$$V_{\Delta t_{AB}} = \begin{vmatrix} \Delta t_{.0} \\ \Delta t_{.1} \\ \Delta t_{.2} \\ \dots \\ \Delta t_{99} \end{vmatrix} \quad (6)$$

и рассчитывается его норма

$$n_{\Delta t_{AB}} = \sqrt{\sum_{i=1}^{119} \Delta t_{AB_i}^{\ 2}}. \quad (7)$$

Как видно из (7), все диграфы с нулевым значением Δt_{AB} не участвуют в формировании профиля пользователя.

3.7. На этапе идентификации пользователя выполняются следующие шаги.

3.7.1. Рассчитываются значения относительной девиации длительности диграфов δt_{AB} и приводятся к виду $\delta t_{AB} = \pm 1$.

3.7.2. Рассчитывается вектор идентификации:

$$V_{\delta t_{AB}} = \begin{vmatrix} v_{.0} \\ v_{.1} \\ v_{.2} \\ \dots \\ v_{99} \end{vmatrix}, \quad v_i = \begin{cases} \Delta t_{AB_i}, & \textit{если } \Delta t_{AB_i} \cdot \delta t_{AB_i} > 0, \\ 0, & \textit{если } \Delta t_{AB_i} \cdot \delta t_{AB_i} < 0; \end{cases} \quad (8)$$

и рассчитывается его норма:

$$n_{\delta t_{AB}} = \sqrt{\sum_{i=1}^{119} v_i^2}. \quad (9)$$

3.7.3. В соответствии со значениями нормы вектора идентификации $n_{\delta t_{AB}}$ и нормы вектора биометрического профиля пользователя $n_{\Delta t_{AB}}$ принимается решение о подлинности пользователя:

$$Rule_{\Delta t_{AB}} = \begin{cases} 1, & \textit{если } n_{\delta t_{AB}} \geq 0.7 n_{\Delta t_{AB}}, \\ 0, & \textit{иначе.} \end{cases} \quad (10)$$

4. Аналогично п. 3 формируются профиль (вектор $V_{\Delta t_{AB}^{pause}}$) и правило идентификации $Rule_{\Delta t_{AB}^{pause}}$ на основе относительной девиации длительности паузы в диграфах.

5. Аналогично п. 3 формируются профиль (вектор $V_{\Delta t_{AB}^{A/DD}}$) и правило идентификации $Rule_{\Delta t_{AB}^{A/DD}}$ на основе относительной девиации отношения времени нажатия первой клавиши диграфов ко времени между нажатиями клавиш в диграфах.

6. Аналогично п. 3 формируются профиль (вектор $V_{\Delta t_{AB}^{B/UU}}$) и правило идентификации $Rule_{\Delta t_{AB}^{B/UU}}$ на основе относительной девиации отношения времени нажатия второй клавиши диграфов ко времени между отжатиями клавиш в диграфах.

7. Общее решение о подлинности пользователя принимается на основе частных:

$$Rule = \begin{cases} Rule_{\Delta t_{AB}} + Rule_{\Delta t_{AB}^{pause}} + Rule_{\Delta t_{AB}^{A/DD}} + Rule_{\Delta t_{AB}^{B/UU}} \geq 3 \; - \; \text{пользователь подлинный,} \\ Rule_{\Delta t_{AB}} + Rule_{\Delta t_{AB}^{pause}} + Rule_{\Delta t_{AB}^{A/DD}} + Rule_{\Delta t_{AB}^{B/UU}} < 2 \; - \; \text{пользователь не подлинный,} \\ RA_{\Delta t_{AB}} + RA_{\Delta t_{AB}^{A}} + RA_{\Delta t_{AB}^{B}} + RA_{\Delta t_{AB}^{P}} = 2 \; - \; \text{использование качественого подхода.} \end{cases} \quad (11)$$

В третьем случае, когда $Rule = 2$, подлинность пользователя проверяется с использованием качественного подхода. Если частоты использования групп цифровых клавиш, клавиш «плюс», «минус» и клавиш разделителей целой и дробной части для более чем 75 % диграфов совпадают с эталоном, то принимается решение о положительной идентификации.

Результаты исследований и выводы

Тестовую группу составили восемь студентов и аспирантов в возрасте от 20 до 30 лет, каждый из которых ежедневно работает за компьютером и имеет стабильный клавиатурный почерк.

За время эксперимента каждый пользователь сделал по восемь подходов в привычной для него обстановке, на своей клавиатуре, что позволило снизить влияние внешних факторов на почерк и собрать более точные данные. Каждый из подходов состоял из ввода 200 цифровых диграфов, таким образом, в течение каждого подхода пользователь находился в разных психофизических состояниях: медлительность и неуверенность в первых попытках, стабильность в середине, усталость и путаность ближе к концу подхода.

В результате было собрано базу, состоящую из 51200 записей о временных параметрах $t_{A_D B_U}$, $t_{A_U B_D}$, $\frac{t_{A_D A_U}}{t_{A_D B_D}}$, $\frac{t_{B_D B_U}}{t_{A_U B_U}}$. Далее данные были разделены на две части: первую, учебную, выборку составили 38400 записей (восемь пользователей, шесть подходов, 200 диграфов в подходе); вторую, тестовую, составили 12800 записей (восемь пользователей, два подхода, 200 диграфов в подходе).

Ошибка FRR рассчитывалась следующим образом. Для каждого пользователя был сформирован эталон, который сравнивался с двумя тестовыми профилями этого же пользователя. Таким образом, было проведено 8×2=16 аутентификационных тестов. Одно аутентификационное решение было неверным, то есть ошибка FRR составила 6,25 %.

Ошибка FAR рассчитывалась следующим образом. Для каждого пользователя был сформирован эталон, который сравнивался с двумя тестовыми профилями последних семи пользователей. Таким образом, было проведено 8×2×7=112 идентификационных тестов. Пять идентификационных решений были неверными, то есть ошибка FAR составила 4,64 %.

Полученные ошибки классификации пользователей близки к таковым, например, из [1, 6, 7]. Конечно, в реальных условиях объемы данных о временных параметрах диграфов для формирования эталонных и тестовых профилей могут оказаться значительно меньшими, а следовательно, и ошибки FRR и FAR будут иметь более высокие значения. Однако на самый главный вопрос этих исследований – о принципиальной возможности использовать предложенную методику для скрытного мониторинга клавиатурного почерка слушателей СДО – проведенные исследования дали положительный ответ.

Сохранить точность предложенного метода идентификации и уменьшить необходимый объем данных о диграфах клавиатуры можно с помощью мультимодальных систем идентификации. Например, одновременно с клавиатурным почерком отслеживать динамику курсора компьютерной мыши или анализировать совокупность данных, которые сервер СДО может получить о компьютере и браузере пользователя, запросив эту информацию при загрузке веб-страницы (параметры Browser Fingerprints).

Список литературы:

1. Zamfiroiu, Alin, Diana Constantinescu, Mădălina Zurini, and Cristian Toma. Secure Learning Management System Based on User Behavior. Applied Sciences 10, no. 21 (October 2020): 7730. DOI:10.3390/app10217730.

2. Marcela Hernández de Menéndez, Ruben Morales-Menendez, Carlos A. Escobar, Jorge Arinez. Biometric applications in education. International Journal on Interactive Design and Manufacturing (IJIDeM) 15(5). September 2021 DOI:10.1007/s12008-021-00760-6.

3. Rajamanogaran, M.; Subha, S.; Baghavathi Priya, S. Contactless Attendance Management System using Artificial Intelligence. Journal of Physics: Conference Series, Volume 1714, Issue 1, article id. 012006 (2021). DOI: 10.1088/1742-6596/1714/1/012006.

4. Jack Curran, Kevin Curran. Biometric Authentication Techniques in Online Learning Environments. In book: Biometric Authentication in Online Learning Environments (pp.266-278). January 2019. DOI:10.4018/978-1-5225-7724-9.ch011.

5. Aeri Leea, Jin-young Hanb. Effective User Authentication System in an E-Learning Platform. International Journal of Innovation, Creativity and Change (pp. 1101-1113). Volume 13, Issue 3, 2020.

6. Adetoba B.T., Awodele O., Kuyoro S.O., Nwaocha O. An Improved Authentication and Monitoring System for E-Learning Examination Using Supervised Machine Learning Algorithms (pp. 235-242). International Journal of Scientific & Engineering Research Volume 11, Issue 3, March-2020.

7. Amr Jadi. New Detection Cheating Method of Online-Exams during COVID-19 Pandemic (pp. 123-130).International Journal of Computer Science and Network Security. VOL.21 No.4, April 2021. https://doi.org/10.22937/IJCSNS.2021.21.4.17

8. A.V.S. Kumar, Biometric authentication in online learning environments. IGI Global, Information Science Reference, an imprint of IGI Global, 2019.

9. Homayoon Beigi. Fundamentals of Speaker Recognition. Springer Science + Business Media; 2011.

10. Teh P S, Teoh A B J, Yue S. A Survey of Keystroke Dynamics Biometrics, The Scientific World Journal, vol. 2013, Article ID 408280, 2013, 24 pages.

11. Заяць В.М., Уліцький О.О. Алгоритмічне та програмне забезпечення системи розпізнавання людини за її рукомоторними реакціями // Вісник Держ. ун-ту «Львівська політехніка» «Комп'ютерна інженерія та інформаційні технології». 2000. № 392. С.73 – 76.

12. Тушканов Е.В. Разработка методов и алгоритмов повышения защищенности информации на основе анализа клавиатурного почерка : дис. канд. техн. наук / Санкт-Петербург. нац. исслед. ун-т информационных технологий, механики и оптики, Санкт-Петербург, 2016. 118 с.

13. Vasyl Alieksieiev, Aleksey Strelnitskiy, Dmitry Gavva, Denis Gorelov, Yuliia Synytsia. Studying of keystroke dynamics statistical properties for biometric user authentication. Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Pages 559-563, 2018.

14. Дослідження статистичних властивостей клавіатурного почерку для вирішення задач аутентифікації користувачів комп'ютерних мереж / Д. Ю. Горелов, В. О. Алєксєєв, В. М. Бублик, Д. В. Маслій // Радиотехника. 2019. Вып. 197. С. 78-85.

15. Дослідження інформативних параметрів диграфів клавіатурного почерку для задач ідентифікації користувачів комп'ютерних мереж / Д. Ю. Горелов, О. О. Іванова, О. В. Кокорін, Д. В. Маслій, О. В. Литвиненко // Радіотехніка. 2020. Вип. 201. С. 194-200.

16. Калмыков А.А., Орчаков О.А., Попов В.В Дистанционное обучение. Введение в педагогическую технологию : учеб. пособие / МГТУ МИРЭА. Москва, 2005. 196 с.

Поступила в редколлегию 07.11.2021

Сведения об авторах:

Горелов Денис Юрьевич – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры компьютерной радиоинженерии и систем технической защиты информации, Украина; email: denis.gorelov@nure.ua; ORCID: https://orcid.org/0000-0002-0845-8070.

Иванова Елена Александровна – кандидат технических наук, доцент, Харьковский национальный университет радиоэлектроники, доцент кафедры компьютерной радиоинженерии и систем технической защиты информации, Украина; email: olena.ivanova1@nure.ua; ORCID: https://orcid.org/0000-0001-9970-7951.

Литвиненко Александр Викторович – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина; email: oleksandr.lytvynenko@nure.ua.

Довбня Андрей Анатольевич – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина; email: andrii.dovbnia@nure.ua.

Минин Дмитрий Александрович – аспирант кафедры безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Украина; email: dmytro.minin@nure.ua.