DOI: 10.18372/2410-7840.18.11084
УДК 621.396:534

МОДИФИЦИРОВАННЫЙ МЕТОД ДИГРАФОВ В ЗАДАЧЕ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Василий Алексеев, Юлия Синица, Денис Горелов

Анализ динамики клавиатурного почерка человека является достаточно быстро развивающимся сегментом исследований, что обусловлено необходимостью обеспечения безопасности большого парка приложений и адаптации к изменяющимся технологиям. В данной статье предложен метод аутентификации пользователя на основании анализа его клавиатурного почерка с использованием модифицированного метода диграфов. В рамках предложенного подхода к аутентификации оператора реализовано разделение клавиш клавиатуры по их функциональному назначению. Работа с каждой зоной формирует собственные события клавиатуры (парные и одиночные), которые анализируются отдельно. Конечное решение о допуске оператора к ресурсам системы принимается на основании всех данных со всех функциональных зон клавиатуры. Для парных событий клавиатуры используются отношения временных параметров диграфов, что позволяет учесть не только статические особенности клавиатурного почерка, но и динамические. Обработка одиночных событий клавиатуры, где основным вычисляемым параметром является время удержания конкретной клавиши, позволяет дополнить профиль пользователя уникальными признаками. Такой комплексный подход позволяет повысить точность процедуры аутентификации без необходимости увеличения объема обрабатываемых данных.

Ключевые слова: *клавиатурный почерк, биометрические алгоритмы, метод диграфов, время удержания клавиши, биоэталон пользователя.*

Введение. В настоящий момент особую важность и значение приобретают задачи защиты информации. Одним из ключевых аспектов информационной безопасности телекоммуникационных систем является разграничение доступа к управлению компьютером и его ресурсам. В решении этих задач все чаще используются биометрические методы разграничения и контроля доступа, в частности анализ клавиатурного почерка пользователя.

Использование динамики клавиатурного почерка для реализации процедуры верификации и идентификации пользователя было впервые исследовано в середине 70-х годов прошлого века [1]. Ранние исследовательские работы [2, 3] по клавиатурному почерку в основном содержали в себе методы, использующие фиксированный (детерминированный) текст, такой как специальная парольная фраза [4] или совокупность цифр [5], анализ набора которых, производился в течение определенного времени, например, во время регистрации оператора в системе [6]. Ключевой идеей в данных работах являлся поиск схожести статистических данных, полученных при анализе параметров введенного фрагмента, по отношению к его эталонным значениям. Основными недостатками данных методов являются существенная зависимость почерка от последовательности букв, малое количество обрабатываемых данных и, как следствие, невысокий уровень достоверности при аутентификации.

Наряду с анализом фиксированного текста в последующих работах исследователей [7, 8, 9] акцент сместился в область идентификации пользователя по произвольному набору текста, что позволяет проводить непрерывную во времени аутентификацию и соответственно формировать дополнительные индивидуальные признаки, повышающие точность в принятии оконечного решения. В настоящий момент системы анализа характеристик субъекта по его клавиатурному почерку используют как статический, так и свободный текст, а также различные их комбинации.

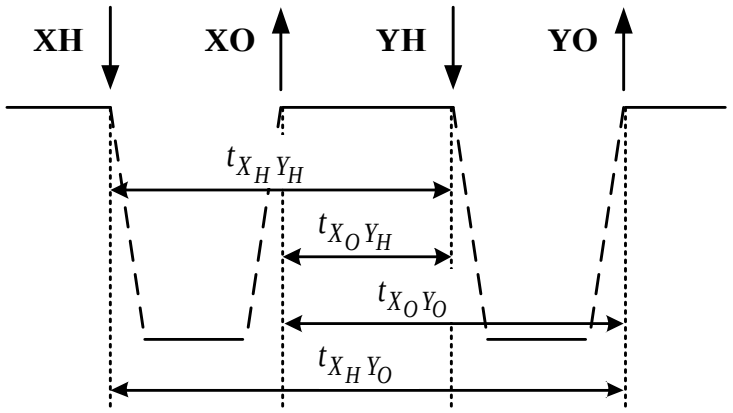
В основу многочисленных авторских работ по изучению особенностей клавиатурного почерка пользователя [10] положены такое понятие как n-граф клавиатуры – комбинация нажатых буквосочетаний, т.е. комбинация событий клавиатуры, последовательного нажатия/отпускания n клавиш.

Цель данной статьи – разработка усовершенствованного алгоритма аутентификации пользователя по клавиатурному почерку, на основании модифицированного метода диграфов, который позволит повысить точность процедуры принятия решения с минимальным набором вычислительных операций.

Метод диграфов. Предложенные в [11, 12] методы биометрической аутентификации пользователей по клавиатурному почерку базируются на статистическом анализе диграфов клавиатуры, которые не требует набора фиксированного образца

текста, так как накопление статистики происходит при любых событиях клавиатуры.

Основными биометрическими параметрами диграфа являются времена выполнения двух последовательных событий клавиш, отдельные комбинации которых изображены на рис. 1. Здесь $t_{X_HY_H}$ – время между нажатиями клавиш «X» и «Y», $t_{X_0Y_H}$ – время между отпусканием клавиши «X» и нажатием клавиши «Y», $t_{X_OY_O}$ – время между отпусканием клавиши «X» и отпусканием клавиши «Y», $t_{X_HY_O}$ – время между нажатием клавиши «X» и отпусканием клавиши «Y».



XH – клавиша «X» нажата;
XO – клавиша «X» отпущена;
YH – клавиша «Y» нажата;
YO – клавиша «Y» отпущена.

Рис. 1. Пример диграфа клавиатуры

Задача идентификации состоит из нескольких этапов: обучение системы и распознавание. Для организации процесса распознавания система определяет и запоминает в базе данных значение временных характеристик зарегистрированных пользователей. На основе значений этих параметров создаются биоэталоны почерка пользователей компьютера. Для идентификации объекта система сравнивает образец почерка на основе введенных данных с биоэталоном, сохраненным в базе данных.

Формирование профиля клавиатурного набора пользователя происходит путем накопления статистических данных о временных интервалах каждого выделенного диграфа во введенном пользователем тексте:

$$T_1 = \begin{vmatrix} t_{1X_HY_H} \\ t_{2X_HY_H} \\ \dots \\ t_{NX_HY_H} \end{vmatrix},\ T_2 = \begin{vmatrix} t_{1X_0Y_H} \\ t_{2X_0Y_H} \\ \dots \\ t_{NX_0Y_H} \end{vmatrix},\ T_3 = \begin{vmatrix} t_{1X_0Y_0} \\ t_{2X_0Y_0} \\ \dots \\ t_{NX_0Y_0} \end{vmatrix},\ T_4 = \begin{vmatrix} t_{1X_HY_0} \\ t_{2X_HY_0} \\ \dots \\ t_{NX_HY_0} \end{vmatrix}, \quad (1)$$

где N – количество повторений определенного диграфа.

Для построения системы аутентификации могут быть использованы любые векторы из (1). Так, например, в [13] входными параметрами каждого диграфа являются времена $t_{X_HY_O}$.

Обычно в процессе набора диграфы повторяются, поэтому в качестве характеристики каждого диграфа целесообразно использовать математическое ожидание и дисперсию временных интервалов (2):

$$m = \frac{1}{N}\sum_{j=1}^{N} t_j, \quad (2)$$

$$\sigma^2 = \frac{1}{N-1}\sum_{j=1}^{N}(t_j - m)^2. \quad (3)$$

Таким образом, эталон пользователя представляет собой некоторый вектор, который состоит из набора пар математического ожидания и дисперсии, характеризующих определенный диграф:

$$Etalon = \begin{vmatrix} m_1 & \sigma_1 \\ m_2 & \sigma_2 \\ \dots & \dots \\ m_L & \sigma_L \end{vmatrix}, \quad (4)$$

где L – количество анализируемых диграфов.

Входными значениями для системы аутентификации являются векторы фактических значений временных интервалов каждого введенного диграфа P_i (допустим, что M_i – количество повторений i-го диграфа), которые затем преобразуются в вектор $Profile$:

$$P_i = \begin{vmatrix} t_{1X_HY_0} \\ t_{2X_HY_0} \\ \dots \\ t_{M_iX_HY_0} \end{vmatrix}, \quad (5)$$

$$Profile = \begin{vmatrix} P_1 \\ P_2 \\ \dots \\ P_K \end{vmatrix}, \quad (6)$$

где K – количество диграфов, участвующих в процедуре аутентификации.

В теории вероятности среднее квадратическое отклонение – индикатор изменчивости объекта, показывающий, на сколько в среднем отклоняются индивидуальные значения признака объекта от их математического ожидания. Каждый определенный диграф является случайной величиной, имеющей нормальный закон распределения. Согласно правилу «трех сигм», не менее чем 99.7% всех значений нормальной случайной величины лежат в интервале:

$$[m - 3\sigma;\ m + 3\sigma]. \qquad (7)$$

Таким образом, решающее правило аутентификации может быть определено следующим образом: при сравнении с эталоном (4) для каждой компоненты вектора (6) проверяются условия согласно правилу (7). Для прохождения аутентификации достаточно, чтобы система распознала не менее 75% диграфов, причем не мене 60% из которых должны удовлетворять условию (7).

Модифицированный метод диграфов. В ходе мониторинга событий клавиатуры должны учитываться как алфавитные символы, так и служебные, которые вместе несут уникальную характеристику клавиатурного почерка каждого пользователя, однако имеют значительные различия между собой во временных параметрах.

В рамках предложенного алгоритма клавиши клавиатуры условно делятся по их назначению на четыре группы – блок алфавитно-цифровых клавиш (рис. 2, а), блок клавиш-модификаторов (рис. 2, б), блок функциональных клавиш (рис. 2, в) и зона клавиш из дополнительного цифрового блока (рис. 2, г), которые ввиду малой частоты использования (или отсутствия в случае «ноутбучного» исполнения) из анализа исключены. Конечное решение об аутентификации пользователя принимается на основании всех данных со всех функциональных зон клавиатуры.

Рис. 2. Деление клавиш клавиатуры на функциональные зоны

В зависимости от функциональной группы клавиатуры, события делятся на парные и одиночные. Если зафиксировано двойное (парное) событие клавиатуры, то для него строится соответствующий диграф, и вычисляются временные характеристики. Такие события формируются клавишами из алфавитно-цифрового блока и клавишами модификаторами, которые, как правило, отдельно не используются. Использование функциональных клавиш анализируется как одиночное событие, где основным вычисляемым параметром является время удержания клавиши $t_{X_H X_O}$ (см. рис. 1).

Алгоритм аутентификации для блока алфавитно-цифровых клавиш. Повысить точность аутентификации личности без увеличения объема обрабатываемых данных (т.е. без перехода к триграфам/n-графам) возможно при анализе отношений временных параметров диграфов, т.е. вместо одного из параметров $t_{X_H Y_H}$, $t_{X_O Y_H}$, $t_{X_O Y_O}$, $t_{X_H Y_O}$ (см. рис. 1) диграфа «XY» использовать их отношения, характеризующие динамику набора текста:

$$\Delta t_{HH\_OH} = \frac{t_{X_H Y_H}}{t_{X_O Y_H}} \quad \text{и} \quad \Delta t_{OO\_OH} = \frac{t_{X_O Y_O}}{t_{X_O Y_H}}. \qquad (8)$$

В данном случае профиль клавиатурного почерка субъекта для диграфа «XY», который повторился при наборе M раз, будет иметь следующий вид:

$$T_1 = \begin{vmatrix} \Delta t_{1\ HH\_OH} \\ \Delta t_{1\ HH\_OH} \\ \dots \\ \Delta t_{M\ HH\_OH} \end{vmatrix},\ T_2 = \begin{vmatrix} \Delta t_{1\ OO\_OH} \\ \Delta t_{2\ OO\_OH} \\ \dots \\ \Delta t_{M\ OO\_OH} \end{vmatrix}. \qquad (9)$$

Далее вычисляются статистические параметры: математические ожидания $m_{T1,}m_{T2,}$ и дисперсии $\sigma_{T1,}^2\ \sigma_{T2}^2$ диграфа.

Итоговый эталон пользователя представляет собой некоторый вектор, который состоит из наборов четырех параметров, характеризующих определенное двойное событие клавиатуры:

$$Etalon = \begin{vmatrix} m_{1\,T1} & \sigma_{1\,T1} & m_{1\,T2} & \sigma_{1\,T2} \\ m_{2\,T1} & \sigma_{2\,T1} & m_{2\,T2} & \sigma_{2\,T2} \\ \dots & \dots & \dots & \dots \\ m_{L\,T1} & \sigma_{L\,T1} & m_{L\,T2} & \sigma_{L\,T2} \end{vmatrix}, \quad (10)$$

где L – количество анализируемых диграфов.

В формировании эталона участвуют только те диграфы, время введения которых не превышает предельное значение, определяемое для каждого пользователя индивидуально. Это необходимо делать для того, чтобы незапланированные долгие паузы во время набора текста не влияли на профиль.

Аналогично (5) и (6) формируется вектор профиля пользователя, проходящего аутентификацию:

$$P_{1i} = \begin{vmatrix} \Delta t_{1\,HH\_OH} \\ \Delta t_{2\,HH\_OH} \\ \dots \\ \Delta t_{M_i\ HH\_OH} \end{vmatrix}, \quad P_{2i} = \begin{vmatrix} \Delta t_{1\,OO\_OH} \\ \Delta t_{2\,OO\_OH} \\ \dots \\ \Delta t_{M_i\ OO\_OH} \end{vmatrix}, \quad Profile = \begin{vmatrix} P_{11} \\ P_{12} \\ \dots \\ P_{1K} \\ P_{21} \\ P_{22} \\ \dots \\ P_{2K} \end{vmatrix}. \quad (11)$$

В результате проверки условия (7) для каждого компонента вектора $Profile$ (11) и вектора $Etalon$ (10) рассчитывается вектор верификации V:

$$V = \begin{vmatrix} V_{11} \\ V_{12} \\ \dots \\ V_{1K} \\ V_{21} \\ V_{22} \\ \dots \\ V_{2K} \end{vmatrix}, \quad V_{1s_j} = \begin{cases} 1, \text{если } m_{s\,T1_j} - 3\sigma_{s\,T1_j} \le \Delta t_{j\,HH\_OH_s} \le m_{s\,T1_j} + 3\sigma_{s\,T1_j}; \\ 0, \quad \text{иначе;} \end{cases}$$
$$V_{2s_j} = \begin{cases} 1, \text{если } m_{s\,T2_j} - 3\sigma_{s\,T2_j} \le \Delta t_{j\,OO\_OH_s} \le m_{s\,T2_j} + 3\sigma_{s\,T2_j}; \\ 0, \quad \text{иначе,} \end{cases} \quad (12)$$

где $s = 1,2, \dots K$ – порядковый номер анализируемого диграфа; $j = 1,2, \dots M_{\langle s \rangle}$ – порядковый номер временного параметра (Δt_{HH_OH} или Δt_{OO_OH}) в векторах P_{1s} и P_{2s} (см. (11)) для s-го диграфа; $M_{\langle s \rangle}$ – количество повторений s-го диграфа.

По норме вектора согласованности V принимается решение R_1 о подлинности субъекта:

$$R_1 = \begin{cases} \|V\| \le Z_{OTK} - \text{отказ;} \\ \|V\| \ge Z_{\text{ДОП}} - \text{допуск;} \\ Z_{OTK} < \|V\| < Z_{\text{ДОП}} - \text{дальнейший анализ.} \end{cases} \quad (12)$$

Значения порогов отказа и допуска принимаются равными $Z_{OTK} = 0.5$ (50 % единиц в векторе V) и $Z_{\text{ДОП}} = 0.6$ (60 % единиц в векторе V). Также для прохождения аутентификации необходимо, чтобы система распознала не менее 75 % диграфов.

Алгоритм аутентификации для блока клавиш-модификаторов. В данном случае алгоритм аутентификации и решающее правило R_2 полностью повторяют шаги (8)-(12). Единственное отличие – диграф всегда начинается с клавиши-модификатора, т.е. «Shift», «Ctrl», «Alt» и «Fn». Если при анализе возникает ситуация, когда клавиша-модификатор является заключительной в диграфе, то предыдущая ей клавиша анализируется как одиночное событие клавиатуры, а диграф строится, начиная с клавиши-модификатора.

Алгоритм аутентификации для блока функциональных клавиш. В случае анализа и обработки одиночных событий клавиатуры производится статистическая обработка времен удержания клавиш. В этом случае векторы входных данных, эталона и профиля формируются аналогично (1), (4) и (6) с той лишь разницей, что исходными параметрами являются интервалы времени $t_{X_H X_O}$. Аналогичным (12) является и решающее правило. В данном случае вектор верификации:

$$V = \begin{vmatrix} V_1 \\ V_2 \\ \cdots \\ V_K \end{vmatrix},\ V_{1_j} = \begin{cases} 1, \text{ если } m_{1_j} - 3\sigma_{1_j} \le t_{X_H X_{O_j}} \le m_{1_j} + 3\sigma_{1_j}; \\ 0, \quad \text{иначе}, \end{cases} \tag{13}$$

где K – количество анализируемых клавиш; $j = 1,2, \ldots M_{\langle s \rangle}$ – порядковый номер временного параметра в векторе P_s (см. (5)); $M_{\langle s \rangle}$ – количество нажатий s-ой клавиши.

Решение R_3 о подлинности субъекта:

$$R_3 = \begin{cases} \|V\| \le Z_{OTK} - \text{отказ}; \\ \|V\| \ge Z_{\text{ДОП}} - \text{допуск}; \\ Z_{OTK} < \|V\| < Z_{\text{ДОП}} - \text{дальнейший анализ}. \end{cases} \tag{14}$$

Значения порогов отказа и допуска также принимаются равными $Z_{OTK} = 0.5$ и $Z_{\text{ДОП}} = 0.6$.

Общее решение RA о подлинности субъекта принимается на основе выполнения условия:

$$RA = \begin{cases} 0.6R_1 + 0.2R_2 + 0.2R_3 \le 0.5 - \text{отказ}; \\ 0.6R_1 + 0.2R_2 + 0.2R_3 \ge 0.6 - \text{допуск}; \\ 0.5 < 0.6R_1 + 0.2R_2 + 0.2R_3 < 0.6 - \text{дальнейший анализ}. \end{cases} \tag{15}$$

С каждой успешной аутентификацией субъекта выполняется обновление эталона, что позволяет учесть изменения клавиатурного почерка и соответствующим образом адаптировать систему аутентификации.

Значения порогов отказа Z_{OTK} и допуска $Z_{\text{ДОП}}$ в выражениях (12) и (14), а также весовых коэффициентов в выражении (15) являются первичными и опытным путем в дальнейшем будут уточняться.

Алгоритмы формирования биоэталона и процесса аутентификации. При аутентификации пользователь вводит произвольный текст. Программно рассчитываются временные события клавиатуры и сравниваются с сохраненными в базе данных параметрами того или иного биоэталона согласно решающему правилу. По истечению определенного интервала времени происходит проверка выполнения условия (15).

Если аутентификация пройдена успешно, то эталон дополняется новыми значениями и пересчитывается, ввод текста и мониторинг продолжается. В противном случае – система блокируется. В случае неопределенности ввод текста проводится до следующей проверки на выполнение условий выражения (15). Обновление профиля позволяет учесть изменение клавиатурного почерка и соответствующим образом адаптировать систему аутентификации. Таким образом, осуществляется непрерывная аутентификация пользователей, которая позволяет проводить скрытую аутентификацию в течение всего времени активности клавиатуры.

Процедура формирования эталона. В режиме регистрации проходит обучение системы – ввод имени пользователя и его биометрического эталона. Формирование биоэталона является важной составляющей алгоритма программы, так как эта процедура выполняется как в режиме обучения, так и частично в режиме аутентификации. Процесс регистрации пользователя изображен на рис. 3.

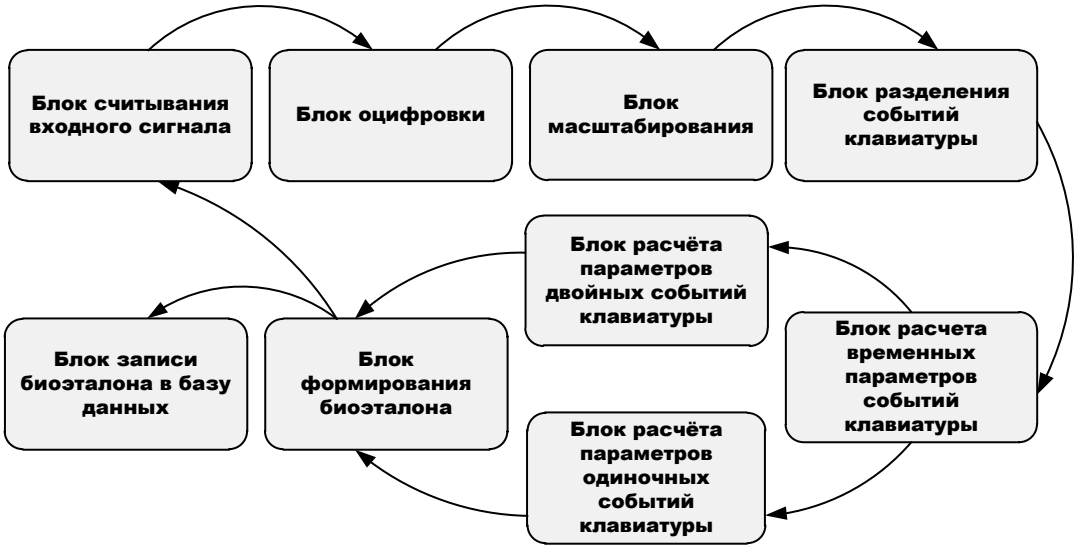


Рис. 3. Структурная схема процесса регистрации пользователя

После считывания входного сигнала происходит его оцифровка. Затем сигнал масштабируется. Далее производится разделение событий клавиатуры, вычисление их основных временных параметров и сохранение в базу данных.

Общая блок-схема алгоритма формирования биометрического эталона приведена на рис. 4. При формировании биометрического эталона постоянно происходит мониторинг клавиатуры. В случае появления какого-либо события клавиатуры проводится анализ событий: «клавиша нажата» или «клавиша отпущена». Для двух приведенных событий обработка данных является идентичной, но также зависит от обработки предыдущего события. После распознавания события клавиатуры выполняется обработка кода клавиши и уточнение, из какой функциональной зоны поступило событие. Если клавиша зафиксирована как «одиночная», то производится вычисление временного интервала удержания клавиши. Из «тика» события «клавиша отпущена» вычитается «тик» события «клавиша нажата» и делится на частоту счетчика высокого разрешения для получения значения времени удержания в миллисекундах. «Тики» событий и частота счетчика определяются системными функциями операционной системы. Далее полученные значения времени вместе с кодом клавиши помещаются в массив «HoldKeyArray». На следующем этапе вызывается функция подсчета вероятностно-статистических данных. После того, как ввод будет закончен, производится формирование шаблона пользователя.

Если клавиша определена как «парная», то фиксируется ее код и устанавливается флаг состояния. После чего производится формирование парных событий клавиатуры, где элементами выборки являются временные интервалы между нажатиями двух клавиш. Если условие парности выполняется, то строится соответствующий диграф. Если полученный диграф заканчивается клавишей-модификатором, он не анализируется, а событие предыдущей клавиши интерпретируется системой как «одиночное». Следующий диграф строится, начиная с клавиши-модификатора. Далее рассчитываются временные характеристики диграфов. Таким образом, формируется два массива DigraphArr_1 и DigraphArr_2. В первый попадают значения соотношений временных интервалов диграфов, при фиксации которых были определены наложения клавиш (т.е. в какой-то момент времени обе клавиши были нажаты одновременно), во второй массив попадают временные значения событий, при появлении которых наложений не было. Это обстоятельство также может учитываться как дополнительный признак клавиатурного почерка пользователя. Параллельно вводу текста производится расчёт статистических параметров диграфов, которые в последующем вместе с их идентификаторами сохраняются в ассоциативный массив, являющийся основой эталона пользователя.

Процедура аутентификации. Пользователь набирает произвольный текст, пользуется клавишами различного назначения: клавишами навигации или системными клавишами. Программно вычисляются временные параметры диграфов. Далее в соответствии с решающим правилом (15) полученные данные сравниваются с сохранёнными биоэталонами. Функциональная схема реализации процедуры аутентификации показана на рис. 5.

Основная блок-схема алгоритма аутентификации во многом повторяет блок-схему алгоритма формирования биоэталона (см. рис. 4). Основное отличие состоит в том, что после вычисления временных параметров событий клавиатуры не происходит расчета вероятностных характеристик, их запись в ассоциативный массив и формирование эталона профиля, а выполняется загрузка и считывание существующего в базе данных биоэталона и последующее сравнение его с текущими полученными значениями.

Фрагмент алгоритма, дополняющий работу программы во время процедуры аутентификации, приведен на рис. 6. Сначала загружается файл, содержащий биоэталон пользователя. Затем выполняется считывание файла и проверка условия: присутствует ли в данной выборке анализируемая клавиша и/или диграф (в зависимости от того является ли данное событие одиночным или парным). Если присутствует, то далее рассчитываются элементы векторов (11) и (13). Если элемент равен единице, то значение счетчика, отвечающего за положительную аутентификацию, увеличивается на 1, в противном случае на 1 увеличивается значение счетчика, отвечающего за отрицательную аутентификацию. Данная часть алгоритма работает зеркально как с парными событиями клавиатуры, так и с одиночными.

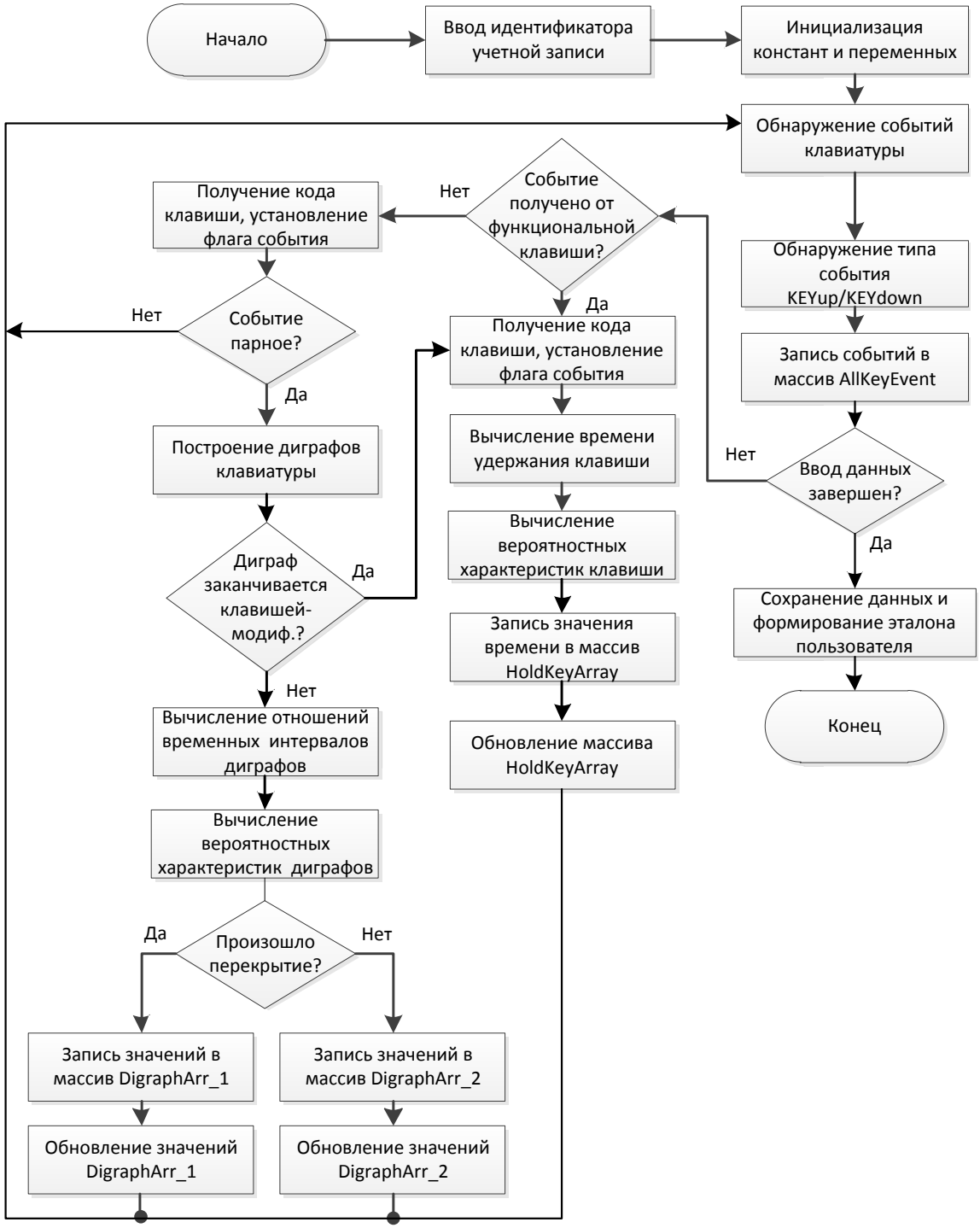


Рис. 4. Блок-схема алгоритма формирования биометрического эталона

Рис. 5. Структурная схема процесса аутентификации пользователя

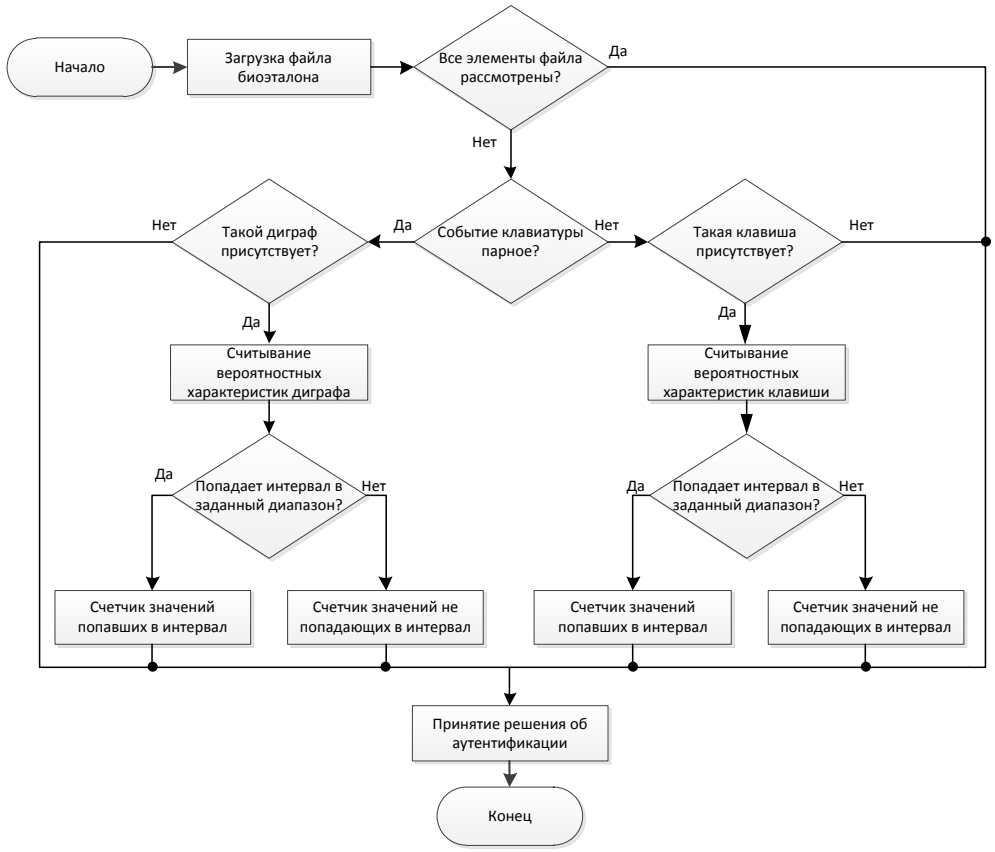


Рис. 6. Фрагмент блок-схемы алгоритма аутентификации пользователя

Выводы. Предложенный подход к аутентификации пользователей по клавиатурному почерку отличается от известных раздельным анализом функциональных зон клавиатуры. Для алфавитно-цифровых клавиш и клавиш-модификаторов используются отношения временных параметров диграфов, что позволяет учесть не только статические особенности клавиатурного почерка, но и динамические. Введение в анализ функциональных клавиш, как одиночных событий клавиатуры, позволяет учесть недоступные методу диграфов информативные признаки клавиатурного почерка.

Использование как статистических, так и динамических оценок одиночных и двойных событий клавиатуры, а также выделение в отельную группу диграфов с клавишами-модификаторами в сравнении с другими статистическими методами дает существенно более высокую точность клавиатурной аутентификации.

ЛИТЕРАТУРА

[1]. R.Spillane. Keyboard apparatus for personal identification. IBM Technical Disclosure Bulltin, 17(11), 1975.

[2]. R. Gaines, W. Lisowski, S. Press, and N. Shapiro. Authentication by keystroke timing: some preliminary results. Technical Report Rand Rep. R-2560-NSF, RAND Corporation, p. 51, 1980.

[3]. D. Umphress and G. Williams. Identity verification through keyboard characteristics. International Journal of Man-Machine Studies, Vol. 23(3), pp. 263–273, 1985.

[4]. K.S. Balagani, Vir V. Phoha, A.Ray, and S. Phoha. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. Pattern Recognition Letters, Vol. 32(7), pp. 1070–1080, 2011.

[5]. R.A. Maxion and K.S. Killourhy. Keystroke biometrics with number-pad input. In IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 201–210, 2010.

[6]. J.A. Robinson, V.W. Liang, J.A.M. Chambers, and C.L. MacKenzie. Computer user verification using login string keystroke dynamics. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, Vol. 28(2), pp. 236–241, 1998.

[7]. D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM Transactions on Information and System Security, Vol. 8(3), pp.312–347, 2005.

[8]. F. Bergadano, D. Gunetti, and C. Picardi. User authentication through keystroke dynamics. ACM Transactions on Information and System Security, Vol. 5(4), pp. 367–397, 2002.

[9]. D. El Menshawy, H.M.O. Mokhtar, and O. Hegazy. A keystroke dynamics based approach for continuous authentication. In 10th International Conference on Beyond Databases, Architectures, and Structures (BDAS), Vol. 424 of CCIS, pp. 415–424, 2014.

[10]. T. Sim and R. Janakiraman. Are digraphs good for free-text keystroke dynamics? In IEEE Conference on

Computer Vision and Pattern Recognition (CVPR), pp. 1–6, 2007.
[11]. A. Messerman, T. Mustafic, S.A. Camtepe, and S. Albayrak. Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In International Joint Conference on Biometrics (IJCB), pp. 1–8, 2011.
[12]. S.Z.S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours. Soft biometrics for keystroke dynamics. In 10th International Conference on Image Analysis and Recognition (ICIAR), Vol. 7950 of LNCS, pp. 11–18, 2013.
[13]. Синиця Ю.О. Автентифікація суб'єктів за клавіатурним почерком з використанням диграфів // Международная конференция "Интернет-технологии и программирование компьютерных мобильных систем": Материалы XVII Международного молодежного форума "Радиоэлектроника и молодежь в XXI веке ", том 5. — Харьков, 2013. — с. 167-168.

REFERENCE

[1]. R.Spillane. Keyboard apparatus for personal identification. IBM Technical Disclosure Bulltin, 17(11), 1975.
[2]. R. Gaines, W. Lisowski, S. Press, and N. Shapiro. Authentication by keystroke timing: some preliminary results. Technical Report Rand Rep. R-2560-NSF, RAND Corporation, p. 51, 1980.
[3]. D. Umphress and G. Williams. Identity verification through keyboard characteristics. International Journal of Man-Machine Studies, Vol. 23(3), pp. 263–273, 1985.
[4]. K.S. Balagani, Vir V. Phoha, A.Ray, and S. Phoha. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. Pattern Recognition Letters, Vol. 32(7), pp. 1070–1080, 2011.
[5]. R.A. Maxion and K.S. Killourhy. Keystroke biometrics with number-pad input. In IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 201–210, 2010.
[6]. J.A. Robinson, V.W. Liang, J.A.M. Chambers, and C.L. MacKenzie. Computer user verification using login string keystroke dynamics. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, Vol. 28(2), pp. 236–241, 1998.
[7]. D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM Transactions on Information and System Security, Vol. 8(3), pp. 312–347, 2005.
[8]. F. Bergadano, D. Gunetti, and C. Picardi. User authentication through keystroke dynamics. ACM Transactions on Information and System Security, Vol. 5(4), pp.367–397, 2002.
[9]. D. El Menshawy, H.M.O. Mokhtar, and O. Hegazy. A keystroke dynamics based approach for continuous authentication. In 10th International Conference on Beyond Databases, Architectures, and Structures (BDAS), Vol. 424 of CCIS, pp. 415–424, 2014.
[10]. T. Sim and R. Janakiraman. Are digraphs good for free-text keystroke dynamics? In IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1–6, 2007.
[11]. A. Messerman, T. Mustafic, S.A. Camtepe, and S. Albayrak. Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In International Joint Conference on Biometrics (IJCB), pp. 1–8, 2011.
[12]. S.Z.S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours. Soft biometrics for keystroke dynamics. In 10th International Conference on Image Analysis and Recognition (ICIAR), Vol. 7950 of LNCS, pp. 11–18, 2013.
[13]. Sinytsa YU.O. Authentication subjects by keystroke dynamics using digraphs// International conference "Internet technologies and computer programming mobile systems": Materials of the VII International Youth Forum "Radio electronics and youth in XXI century", Volume 5. — Kharkov, 2013, pp. 167-168.

MODIFIED DIGRAPHS METHOD IN THE PROBLEM OF AUTHENTICATING USERS USING KEYSTROKE DYNAMICS

Keystroke dynamics analysis is fairly fast growing direction of research that is due to need to ensure the security of a large park of applications and adaptation to the changing technologies. In this article proposed keystroke dynamics user authentication method which uses modified method of digraphs. In this case, it suggested the division of the keyboard keys on their functional purpose. Each zone generates its own events (double and single) which are analyzed separately. The final decision of authentication is made on the basis of all the data from all functional areas of the keyboard. For paired keyboard events is used the ratio of time parameters of digraphs. This makes it possible to analyze both static and dynamic features keystroke rhythms of a user. The main calculated parameter in a single event is hold time of key. Processing of such events gives the possibility to add unique additional user profile attributes. This integrated approach allows to improve the accuracy of authentication using keystroke dynamics without increasing the volume of data being processed.
Keywords: keystroke dynamics, biometric algorithms, hold time, digraphs method, biometric standart.

МОДИФІКОВАНИЙ МЕТОД ДИГРАФІВ В ЗАДАЧІ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ

Аналіз динаміки клавіатурного почерку людини є сегментом досліджень, який швидко розвивається, що обумовлено необхідністю забезпечення безпеки великого парку додатків і адаптації до постійно змінюваних технологій. У даній статті запропоновано метод автентифікації користувача на підставі аналізу його клавіатурного почерку з використанням модифікованого методу диграфів. В межах запропонованого підходу до автентифікації оператора реалізовано розмежування клавіш клавіатури за їх функціональним призначен-

ням. Робота з кожною зоною формує власні події клавіатури (парні та непарні), які аналізуються окремо. Кінцеве рішення про допуск оператора до ресурсів системи приймається на підставі всіх даних з усіх функціональних зон клавіатури. Для парних подій клавіатури використовуються відносини часових параметрів дирафів, що дозволяє врахувати не тільки статичні особливості клавіатурного почерку, а й динамічні. Обробка поодиноких подій клавіатури, де головним обчислюваним параметром є час утримання конкретної клавіші, дозволяє доповнити профіль користувача унікальними ознаками. Такий комплексний підхід дозволяє підвищити точність процедури автентифікації без необхідності збільшення обсягу оброблюваних даних.
Ключові слова: клавіатурний почерк, біометричні алгоритми, метод дирафів, час утримання клавіші, біоеталон користувача.

Алексеев Василий Александрович, аспирант кафедры основ радиотехники харьковского Национального университета радиоэлектроники.
E-mail: vasyl.alieksieiev@nure.ua.
Алексеєв Василь Олександрович, аспірант кафедри основ радіотехніки харківського Національного університету радіоелектроніки.
Alieksieiev Vasyl, postgraduate student of Radio Engineering Fundamentals Academic Dept in Kharkiv National University of Radioelectronics.

Синица Юлия Александровна, магистр технических наук ХНУРЭ, инженер по автоматизации программных продуктов в "Marvell Semiconductor Inc.", Санта Клара, штат Калифорния, США.
E-mail: lm.julia92@gmail.com.
Синиця Юля Олександрівна, магістр технічних наук ХНУРЕ, інженер з автоматизації програмних продуктів в "Marvell Semiconductor Inc.", Санта Клара, штат Каліфорнія, США.
Synytsia Yuliia, M.Eng. KNURE, Ukraine, Software Automation Engineer in Marvell Semiconductor Inc., Santa Clara, CA, USA.

Горелов Денис Юрьевич, кандидат технических наук, доцент кафедры основ радиотехники харьковского Национального университета радиоэлектроники.
E-mail: denis.gorelov@nure.ua
Горелов Денис Юрійович, кандидат технічних наук, доцент кафедри основ радіотехніки харківського Національного університету радіоелектроніки.
Gorelov Denis, PhD in Eng, Associate Professor of Radio Engineering Fundamentals Academic Dept in Kharkiv National University of Radioelectronics.

DOI: 10.18372/2410-7840.18.11087
УДК 621.391:519.7

ДОСТАТНЯ УМОВА СТІЙКОСТІ SNOW 2.0-ПОДІБНИХ ПОТОКОВИХ ШИФРІВ ВІДНОСНО ПЕВНИХ АТАК ЗІ ЗВ'ЯЗАНИМИ КЛЮЧАМИ

Антон Олексійчук

Досліджується клас потокових шифрів, аналогічних відомому шифру SNOW 2.0. Наведено формальне означення шифрів з цього класу та встановлено взаємозв'язок між процесами гамоутворення у схемі SNOW 2.0-подібного потокового шифру і зашифровування повідомлень за допомогою схеми Івена-Мансура. Проаналізовано стійкість SNOW 2.0-подібних потокових шифрів відносно атак, що базуються на існуванні ключів, еквівалентних із затримкою. Зазначені атаки відносяться до класу атак зі зв'язаними ключами та є застосовними до широкого кола потокових шифрів, зокрема, SNOW 2.0. Головним результатом статті є достатня умова стійкості SNOW 2.0-подібних шифрів відносно зазначених атак. Ця умова є зручною для практичного застосування і дозволяє будувати афінні відображення (за допомогою яких здійснюється запис ключа та вектора ініціалізації у накопичувач генератора гами), які гарантують стійкість відповідного шифру відносно зазначених атак. Наведено два приклади таких відображень, які можуть бути використані при побудові нових SNOW 2.0-подібних шифрів.
Ключові слова: *потоковий шифр, схема Івнга-Мансура, еквівалентьність ключів із затримкою, атаки зі зв'язаними ключами, обгрунтована стійкість, SNOW 2.0.*

Вступ. Потоковий шифр SNOW 2.0 [3] запропонований у 2002 році як альтернатива попередньої (більш слабкої) версії – SNOW. На сьогодні цей шифр є стандартизованим [6] та являє собою один з найбільш швидких програмно орієнтованих потокових шифрів. Не відомо атак на повну версію шифру SNOW 2.0, спрямованих на відновлення єдиного ключа (single key recovery attacks), більш ефективних ніж повний перебір ключів. Поряд з тим, відомі ефективні атаки зі зв'язаними ключами (related key attacks), які базуються