

## РАЗДЕЛ III

# МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ. СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ

УДК 004.93

## ОЦЕНКА ИДЕНТИФИКАЦИОННЫХ ВОЗМОЖНОСТЕЙ ОСОБЕННОСТЕЙ РАБОТЫ ПОЛЬЗОВАТЕЛЯ С КОМПЬЮТЕРНОЙ МЫШЬЮ

Р.В. Борисов<sup>1</sup>, Д.Н. Зверев<sup>2</sup>, А.Е. Сулавко<sup>3</sup>, В.Ю. Писаренко<sup>3</sup>

<sup>1</sup>ООО "Люксофт Профешнл", Филиал ООО "Люксофт Профешнл" в городе Омск, Россия, Омск; <sup>2</sup>ООО «Интрокод», Россия, Омск;

<sup>3</sup> Омский государственный технический университет «ОмГТУ», Россия, Омск;

**Аннотация.** В статье рассматривается проблема защиты конфиденциальных данных от несанкционированного доступа в компьютерной системе. Предложен метод идентификации пользователей по особенностям работы с мышью, основанный на мониторинге деятельности субъекта во время работы за компьютером и применении сетей Байеса для принятия идентификационных решений.

**Ключевые слова:** распознавание образов, биометрические системы, идентификация, аутентификация, нарушитель, идентифицирующие признаки, особенности работы с мышью.

### Введение

Повсеместная информатизация и введение компьютеров в различные сферы деятельности приводит к массовому переходу на электронный документооборот. Поэтому актуализация вопросов защиты компьютерных ресурсов от несанкционированного доступа является закономерным явлением. Потеря, искажение, нарушение конфиденциальности информации наносит финансовый ущерб ее собственнику. Финансовые потери мировой экономики исчисляются десятками миллиардов долларов в год [1]. По данным аналитических исследований компании *InfoWatch* основная доля этого ущерба (55%) обусловлена деятельностью инсайдеров – внутренних неloyальных по отношению к организации сотрудников [2]. В связи с этим требуется проводить скрытый мониторинг деятельности пользователя за компьютером, его непрерывную аутентификацию и распознавание опасных с точки зрения информационной безопасности действий. Современные средства аутентификации основаны на проверке паролей, смарт-карт и биометрических характеристик. Последний вариант позволяет привязать аутентификатор к личности человека, поэтому является предпочтительным. Основная проблема создания биометрических систем идентификации/аутентификации состоит в выделении информативных признаков.

Наиболее надежными в этом плане являются открытые биометрические образы – отпечатки пальцев, радужная оболочка. Однако они находятся «на виду», существует множество способов их хищения незаметно для владельца. Реализовать скрытую процедуру аутентификации с их использованием проблематично (если вообще возможно). В рамках данной работы предлагается подход для разграничения доступа в компьютерной системе на основе особенностей работы пользователя с мышью. Данные, полученные при работе пользователя с мышью, используются для дополнительной непрерывной во времени аутентификации пользователя (в процессе его работы за компьютером), получившего доступ к компьютерной системе. Это возможно в связи с тем, что у каждого пользователя существует собственная манера управления манипулятором «мышь» [3-4].

### Достигнутые результаты в области распознавания пользователей по особенностям работы с мышью.

В работах [3-4] определено множество параметров траектории курсора при манипулировании мышью. Предложено каждую траекторию отображать вектором из пяти параметров: время движения манипулятора до его остановки, длина траектории, скорость разгона курсора, время между остановкой указателя и подтверждающим нажатием кнопки ма-

нипулятора, угол направления начального движения. Большинство из этих параметров определяет скоростные характеристики (динамику) работы пользователя с компьютерной мышью и мало учитывают параметры траекторий движения. Автором работы [4] также предложены: компьютерная модель информационного почерка пользователя на базе манипулятора «мышь»; метод распознавания состояния системы «пользователь-мышь» посредством выявленных информативных параметров и нейронной сети радиального типа с вероятностью 0,9-0,95; программный комплекс, реализующий указанный метод. Достигнутые результаты в области распознавания пользователей по особенностям работы с мышью не достаточно показательны для внедрения на практике. Масштабные исследования в данном направлении только начинают проводиться. Особенности работы с манипулятором «мышь» часто используют в сочетании с клавиатурным почерком для распознавания пользователя, находящегося за компьютером [5], а также определения нежелательного поведения и предотвращения утечки конфиденциальных данных [6]. В одной из последних работ в данной области [6] приводится вероятность правильной идентификации пользователей по особенностям работы с мышью порядка 0,8, при этом вероятность правильной идентификации по клавиатурному почерку при аналогичных условиях с использованием тех же методик составила 0,83, что незначительно выше. Можно предположить, что информативность временных характеристик клавиатурного почерка несущественно выше информативности особенностей работы с мышью. Но если при распознавании по клавиатурному почерку удалось подойти к пределу надежности (после 2007-2009 годов не удалось получить достоверный результат по снижению коэффициента равновероятной ошибки менее чем до 1% [7-8]), то идентификационный потенциал особенностей работы с мышью полностью не исследован. В работе [6] указывается, что признаки мыши менее стабильны и сильно зависят от используемых пользователем устройств по сравнению с признаками клавиатурного почерка. Вероятность правильной идентификации при использовании клавиатурного почерка совместно с признаками мыши, достигнутая в [6], составила более 0,92. Известен результат, при котором вероятность правильной идентификации 14 субъектов только по особенностям работы с мышью равна 0,93 [4]. Настоящее исследование направлено на то, чтобы повысить надежность

распознавания пользователя по характеру работы с мышью, используя для этого не только временные характеристики перемещений курсора, но и параметры его траекторий. Цель работы: дать обобщенную оценку идентификационных возможностей особенностей работы с мышью.

#### Идентификационные признаки

Прежде всего, необходимо выделить устойчивые идентификационные признаки и создать эталон пользователя. Эталонные значения признаков должны быть характерно различимы у разных людей, а образцы признаков одного человека, должны быть схожи. Для выявления информативных признаков разработан программный модуль. Элементы интерфейса, относительно которых производится измерение признаков – кнопки различных размеров, появляющиеся в случайно определенных областях экрана (рис.1). Пользователю предлагается нажимать на данные кнопки. Один из потенциальных признаков основан на оценке среднего времени перемещения курсора мыши между элементами интерфейса при помощи адаптированной для данной задачи формулы (1) закона Фиттса [9]. Закон связывает время движения к наблюдаемой цели с точностью движения и с расстоянием до наблюдаемой цели. Чем дальше или точнее выполняется движение руки (кисти, ноги и др.) субъекта, тем больше коррекции необходимо для его выполнения, и соответственно, больше времени требуется субъекту для внесения этой коррекции. Одна из высказанных в работе [10] гипотез заключается в том, что при внесении коррекции движений проявляются индивидуальные особенности человека, работающего с манипулятором «мышь». Таким образом, фактическое время перемещения не должно совпадать с оценкой, вычисляемой по формуле (1), а должно отличаться на величину  $\Delta T$ , которую решено использовать как один из идентифицирующих признаков в настоящей работе. Другими признаками, предложенными в работе [10], которые использованы в настоящей работе, являются максимальное  $C_{max}$  и среднее  $C_{mid}$  отклонения (в пикселях) от кратчайшего пути  $s_{min}$  перемещения курсора между двумя элементами интерфейса.

$$T = b \cdot \log_2 \left( \frac{D}{W} + 1 \right), \quad (1)$$

где  $b$  — величина, зависящая от типичной скорости движения курсора мыши (вычисляется как отношение средней скорости движения мыши по экрану, осуществляемого субъектом, к установленному в операционной сис-

теме коэффициенту чувствительности мыши),  $D$  — дистанция перемещения курсора между элементами интерфейса (в пикселях),  $W$  — ширина элемента интерфейса, к которому направляется курсор (в пикселях).

Также в качестве признаков предлагается использовать амплитуды первых десяти низкочастотных гармоник функции скорости перемещения курсора мыши по экрану  $V_{xy}(t)$ , вычисляемой по формуле (2). Разложение функции производится с помощью быстрого преобразования Фурье, тем самым достигается нормирование участков пути курсора по времени. Каждый участок приводится к длительности в 0,5 секунд. Амплитуды нормируются  $A^* = A/E_s$  по энергии функции  $V_{xy}(t)$ , вычисляемой в соответствии с формулой (3), данная операция осуществляется для того, чтобы привести все траектории перемещений курсора между элементами интерфейса к единому масштабу. Аналогичные операции осуществляются по отношению к функциям координат курсора  $x(t)$  и  $y(t)$ , однако предварительно данные функции переводятся в другую систему координат, где началом координат

является центр элемента интерфейса, на который было произведено нажатие, ось абсцисс располагается в направлении центра элемента интерфейса, по отношению к которому производится перемещение курсора (рис. 1). Это необходимо выполнять, чтобы избавиться от наклона линий, связывающих элементы интерфейса, относительно исходной координатной плоскости (т.е. зависимости координат от угла наклона).

$$V_{xy}(t) = \sqrt{(x(t_{i+1}) - x(t_i))^2 + (y(t_{i+1}) - y(t_i))^2}, \quad (2)$$

где  $x$  и  $y$  — координаты курсора,  $t_i$  —  $i$ -ый момент времени регистрации координат курсора (регистрация координат курсора осуществляется разработанным программным модулем и зависит от производительности компьютера).

$$E_s = \int_{-\infty}^{\infty} A^2(\omega) dt, \quad (3)$$

где  $A(\omega)$  — амплитуды гармоники с частотой  $\omega$  функции  $V_{xy}(t)$ .

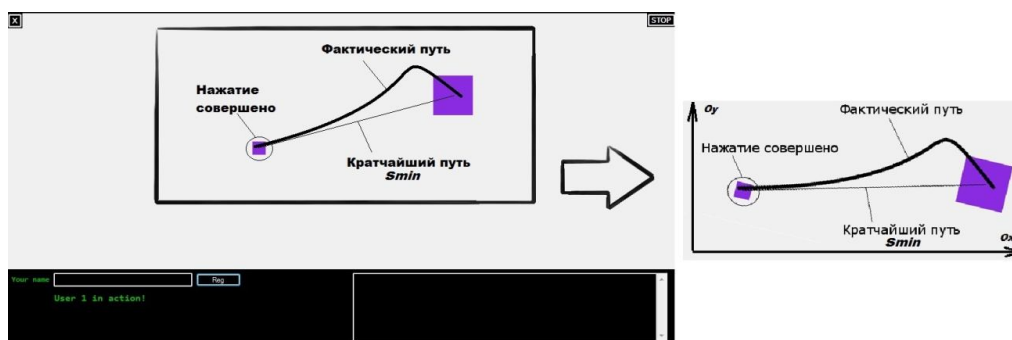


Рис. 1. Ввод пользователем данных о перемещении курсора между элементами интерфейса (слева); Перевод траектории движения курсора между парой элементов интерфейса в другую систему координат (справа)

### Создание эталонов и оценка информативности признаков

На основании критерия Хи-квадрат установлено, что законы распределения значений описанных признаков наиболее близки к нормальному (хотя для некоторых испытуемых характерно также логнормальное распределение отдельных признаков). Поэтому для создания эталонов были рассчитаны параметры нормального закона распределения — математические ожидания и среднеквадратичные отклонения значений каждого признака. Эти параметры представляют собой эталон. При помощи разработанного программного модуля была собрана база, состоящая из набора не менее чем 100 значений каждого признака для 18 испытуемых, т.е. создано 18 эталонов по данным не менее чем о 100

перемещениях курсора для каждого пользователя. Так как скорость реакций субъекта существенно зависит от его темперамента, то испытуемые подбирались таким образом, чтобы среди них было примерно равное количество представителей каждого типа темперамента: 5 сангвиников, 4 холерика, 5 меланхоликов и 4 флегматика (что определялось с помощью теста Айзенка).

Анализ выявленных идентификационных характеристик показал, что признаки  $C_{max}$  и  $C_{mid}$  очень зависимы, коэффициент корреляции между значениями данных признаков близок к единице практически у всех испытуемых (рис. 2). Площади пересечения функций плотностей вероятности данных признаков для всех испытуемых значительны, нормирование значений  $C_{max}$  и  $C_{mid}$  по величине

кратчайшего пути между целевыми элементами интерфейса не исправляет положение (рис. 3). Аналогичные заключения были сделаны относительно признака  $\Delta T$ . Таким образом, данные  $C_{max}$ ,  $C_{mid}$  и  $\Delta T$  не являются информативными, по крайней мере, при используемой в данной работе методике измерения признаков. В работе [11] постулируется снижение ошибок идентификации субъектов по клавиатурному почерку на 9% за счет ис-

пользования особенностей работы с мышью совместно с клавиатурным почерком. Можно заключить, что это достигается благодаря применению скоростных характеристик мыши в качестве признаков, также в [11] регистрировалось время задержки перед перемещением курсора к другому элементу интерфейса (в настоящей работе этого не производилось).

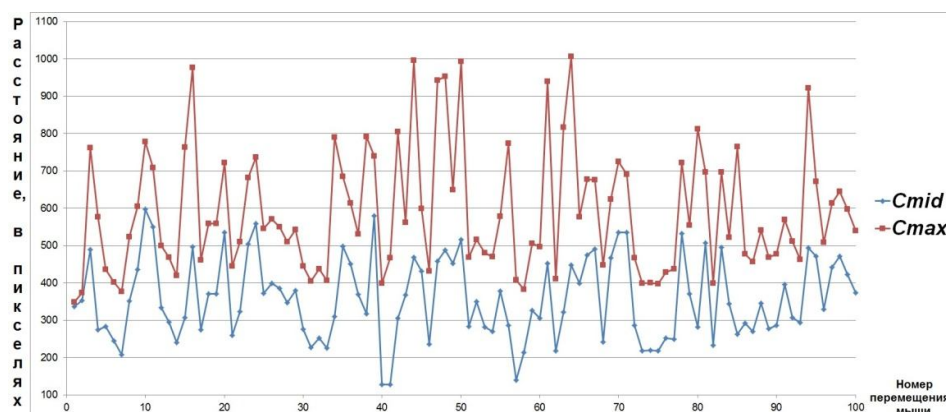


Рис. 2. Значения признаков  $C_{max}$  и  $C_{mid}$  одного из испытуемых

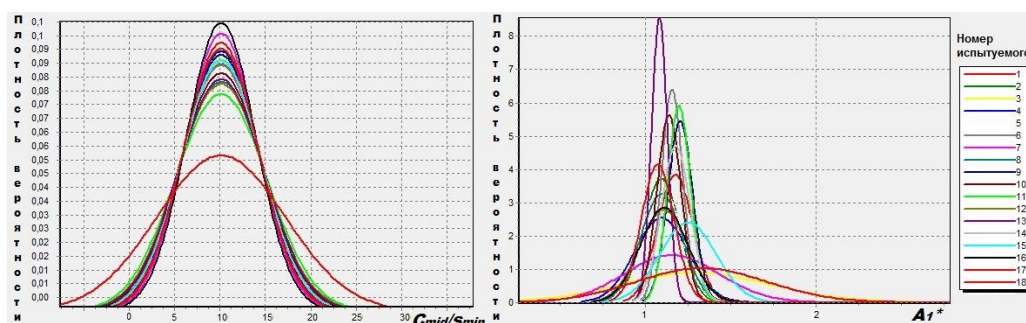


Рис. 3. Распределения неинформативного (слева) и наиболее информативного (справа) из рассматриваемых признаков: плотности вероятности значений  $C_{mid}$ , нормированных по  $S_{min}$ ; плотности вероятности значений амплитуд первой гармоники функции  $V_{mid}(t)$

Анализ амплитудного спектра функций  $V_{mid}(t)$ ,  $x(t)$  и  $y(t)$  показал, что наиболее информативной является амплитуда первой гармоники функции  $V_{mid}(t)$  (см. рис. 3). Решено в качестве признаков использовать только амплитуды первых четырех гармоник указанных функций (с частотами 2, 4, 8 и 16 Гц), т.к. колебания руки испытуемого с большей частотой во время работы с мышью являются шумом.

Таким образом, решено использовать 12 признаков для идентификации, которые вычисляются из координат пути перемещения курсора между каждой парой элементов интерфейса. Корреляция между данными признаками значительно меньше единицы, но как видно из рисунка 3 даже для наиболее информативного признака площади пересече-

ния функций плотностей вероятности значительны, что говорит о том, что признаки мыши малоинформативны [12]. Однако при многократном измерении признаков в процессе совершения пользователем перемещений мышью разделение известных классов все же возможно. Нужно найти алгоритм, который по малым информационным порциям даст интегральную оценку о различии образов пользователей.

**Принятие идентификационных решений и оценка вычислительного эксперимента.** В качестве способа принятия решений решено использовать классическую стратегию Байеса [13], основанную на последовательном применении формулы гипотез Байеса (4). Каждая гипотеза подразумевает, что данные о движениях принадлежат опреде-

ленному пользователю, то есть каждая гипотеза ассоциируется с определенным эталоном. Стратегия Байеса дает несколько меньший процент ошибочных решений в пространстве малоинформативных признаков.

$$P_j(H_i / A) = \frac{P_{j-1}(H_i / A)P(A_j / H_i)}{\sum_{i=1}^n P_{j-1}(H_i / A)P(A_j / H_i)},$$

где  $P_j(H_i / A)$  – апостериорная вероятность  $i$ -ой гипотезы, вычисляемая при поступлении  $j$ -ого признака,  $P(A_j / H_i)$  – условная вероятность  $i$ -ой гипотезы при поступлении  $j$ -ого признака. Таким образом, на каждом шаге за

априорную вероятность принимается апостериорная вероятность, вычисленная на предыдущем шаге. При каждом перемещении курсора измеряются значения признаков и рассчитываются апостериорные вероятности гипотез по формуле (4) за 12 шагов (рис. 4). До осуществления перемещений курсора (на нулевом шаге) все гипотезы равновероятны, то есть,  $P_0(H_i / A) = 1/n$ , где  $n$  – количество гипотез (пользователей). Условные вероятности вычисляются исходя из закона распределения признаков (в данном случае нормального), как плотности вероятности поступающих значений признаков.

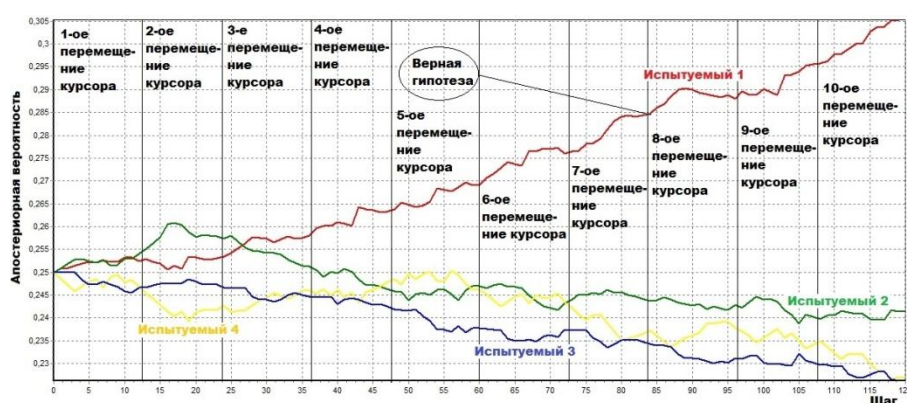


Рис. 4. Расчет интегральных показателей о различии пользователей в пространстве предложенных признаков на основе стратегии Байеса

Каков предел надежности распознавания в заданном пространстве признаков и сколько перемещений необходимо совершить пользователю для его идентификации? Чем выше данное количество перемещений, тем больше времени потребуется для распознавания пользователя на практике.

Для ответа на поставленный вопрос проведен вычислительный эксперимент, в ходе которого имитировался процесс осуществления пользователем перемещений мыши между появляющимися на экране элементами интерфейса. Для этого генерировались значения признаков под имеющиеся эталонные распределения, и производился расчет апостериорных вероятностей на основе стратегии Байеса. Для генерации нормальных случайных величин использовался метод Монте-Карло [14]. Разыгрывание нормальной случайной величины при помощи метода Монте-Карло можно реализовать следующим образом. Известно, что если случайная величина  $R$  распределена равномерно в интервале  $(0, 1)$ , то ее математическое ожидание и дисперсия соответственно равны [14]:

$$M(R) = 1/2; D(R) = 1/12 \quad (5)$$

Сгенерируем  $g$  независимых случайных величин, распределенных равномерно на интервале  $(0;1)$ . Вычисляются математическое ожидание и дисперсия суммы этих величин, которые в силу (5) равны  $g/2$  и  $g/12$  соответственно. Таким образом, среднеквадратичное отклонение вычисляется как квадратный корень из  $g/12$ . Далее сумма случайных величин  $R$  нормируется по формуле (6) [14]. В силу центральной предельной теоремы при  $g \rightarrow \infty$  распределение этой нормированной случайной величины стремится к нормальному с параметрами  $M = 0$  и  $S = 1$  (математическим ожиданием и среднеквадратичным отклонением) [14].

$$\frac{\sum_{j=1}^g R_j - (g/2)}{\sqrt{g/12}} \quad (6)$$

Полученные результаты иллюстрируются на рисунке 5.



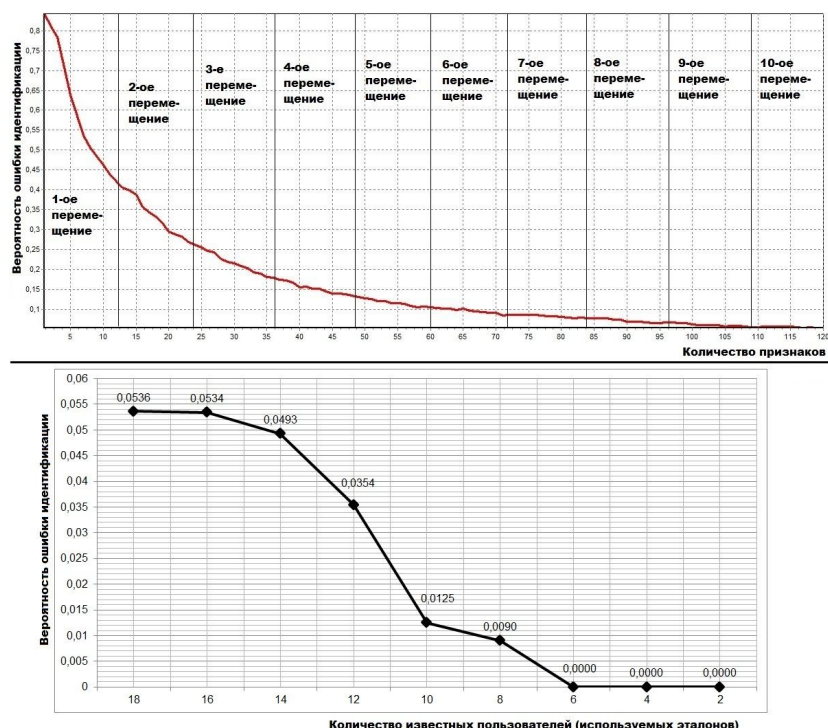


Рис. 5. Результаты эксперимента: вероятность ошибки идентификации 18 пользователей при различном количестве признаков (перемещений) – вверх; вероятность идентификации различного количества пользователей при осуществлении 10 перемещений (120 признаках) – вниз

Имитировалось по 10 перемещений курсора для каждого пользователя, количество имитаций составило 1000 (т.е. было сгенерировано 10000 значений каждого признака для каждого эталона, при этом за одну идентификационную процедуру на вход стратегии Байеса поставлялось по 120 признаков, характеризующих 10 перемещений). Решение о верной гипотезе на каждом шаге принималось по максимальной апостериорной вероятности. За ошибку идентификации принималась ситуация, при которой максимальная вероятность была у неверной гипотезы (рис. 4). Вероятность ошибки в каждом случае (для каждого количества эталонов) рассчитывалась как отношение числа неверных решений к произведению общего количества проведенных имитаций и количества используемых эталонов (см. рис. 5). При максимальном количестве эталонов (в данном исследовании оно составляет 18) после 10 перемещений курсора дальнейшее снижение вероятности ошибки идентификации практически не осуществляется, что свидетельствует о потенциальном пределе надежности распознавания (рис. 5).

#### Заключение

Подводя итоги, можно констатировать, что при количестве известных системе пользователей более 10 и до 20 (среди испытуемых было равное количество представителей

каждого типа темперамента) возможная вероятность правильного распознавания в заданном пространстве признаков превышает 0,95, т.е. сумма ошибок 1-ого и 2-ого рода может быть ниже 5%. При меньшем количестве идентифицируемых образов теоретически возможно осуществить правильное распознавание с вероятностью более 0,99. Однако на практике для достижения указанных показателей количество перемещений курсора между элементами интерфейса потребуется увеличить в несколько раз (как и время на идентификацию), в зависимости от используемого алгоритма принятия решений. Это обусловлено тем, что в задачах идентификации в пространстве малоинформативных признаков часто происходят сбои в измерении признака, вследствие чего на этапе идентификации значение признака может «не попасть» в свое распределение [15]. Поэтому на практике целесообразно использовать модифицированную стратегию Байеса с контролем приращения вероятностей гипотез, описанную в работе [15].

**Работа выполнена при финансовой поддержке РФФИ (грант № 15-37-50269).**

#### Библиографический список

1. Утечки конфиденциальной информации. Предварительные итоги 2014 года. Zecurion Analytics. 2015 г. – Режим доступа:

[http://www.zecurion.ru/upload/iblock/fe3/Zecurion\\_Data\\_leaks\\_2015.pdf](http://www.zecurion.ru/upload/iblock/fe3/Zecurion_Data_leaks_2015.pdf). (дата обращения: 16.03.2015).

2. Глобальное исследование утечек конфиденциальной информации в 2014 году. Аналитический центр InfoWatch. 2015 г. – Режим доступа: [http://www.infowatch.ru/sites/default/files/report/analytcs/russ/InfoWatch\\_global\\_report\\_2014.pdf](http://www.infowatch.ru/sites/default/files/report/analytcs/russ/InfoWatch_global_report_2014.pdf). (дата обращения: 20.03.2015).

3. Диденко С.М. Исследование динамики работы пользователя с манипулятором мышь / С.М. Диденко, В.А. Шапцев // Математическое и информационное моделирование. – Тюмень: Изд-во Тюм. ун-та, 2004. – С. 295–304.

4. Диденко, С.М. Разработка и исследование компьютерной модели динамики системы «пользователь – мышь»: автореф. дис. ... канд техн. наук: 05.13.19 / С.М. Диденко. – Тюмень, ТюмГУ, 2007. – 18 с.

5. Monika Bhatnagar, Raina K Jain and Nilam S Khairnar. Article: A Survey on Behavioral Biometric Techniques: Mouse vs Keyboard Dynamics // IJCA Proceedings on International Conference on Recent Trends in Engineering and Technology 2013 ICRTET(5), May 2013. – P. 22-25.

6. Jain-Shing Wu, Chih-Ta Lin, Yuh-Jye Lee, Song-Kong Chong. Keystroke and Mouse Movement Profiling for Data Loss Prevention // Journal of Information Science and Engineering, 2015, no 31, P. 23-42.

7. Salil P. Banerjee, Damon L. Woodard. Biometric Authentication and Identification using Keystroke Dynamics: A Survey // Journal of Pattern Recognition Research, 2012, no 7. P. 116-139

8. Margit Antal, László Zsolt Szabó, Izabella László. Keystroke Dynamics on Android Platform // 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Tirgu Mures, Romania. – P. 1-7

9. Раскин, Д. Интерфейс: новые направления в проектировании компьютерных систем / Д. Раскин. – СПб: Символ-плюс, 2010. – 272 с.

10. Еременко А.В.. Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: скрытая идентификация / А.В. Еременко, Е.А. Левитская, А.Е. Сулаво // Вестник СибАДИ. – 2014. – № 6(40). – С. 92-102.

11. Сулаво А.Е. Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: портрет нечестного сотрудника / А.Е. Сулаво, А.В. Еременко, Е.А. Левитская // Известия Трансба / ОмГУПС. – 2015. – № 1(21). – С. 80-89.

12. Ложников, П.С. Аналитическое исследование проблемы распознавания образов в пространстве малоинформативных признаков / П.С. Ложников, А.Е. Сулаво // Межотраслевая информационная служба. – 2014. – №2 (167). – С. 11-18.

13. Епифанцев, Б.Н. Сравнение алгоритмов комплексирования признаков в задачах распознавания образов / Б.Н. Епифанцев, П.С. Ложников, А.Е. Сулаво // Вопросы защиты информации ФГУП «ВИМИ». – 2012. – № 1. – С. 60-66.

14. Гмурман, В.Е. Теория вероятностей и математическая статистика: учеб. Пособие для вузов / В.Е. Гмурман. – М.: Высш. шк., 2003. – 479 с.

15. Епифанцев, Б.Н. Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса / Б.Н. Епифанцев, П.С. Ложников, А.Е. Сулаво // Межотраслевая информационная служба / ФГУП «ВИМИ». – 2013. – № 2. – С. 57-62.

#### THE ASSESMENT OF THE IDENTIFICATION CAPABILITIES OF FEATURES OF THE USER INTERACTS WITH A COMPUTER MOUTH

R.V. Borisov, D.N. Zverev,  
A.Ye. Sulavko, V.Yu. Pisarenko

**Abstract.** This article discusses the problem of Identity Theft Protection from unauthorized access in computer system. The method of user identification by features of user interacts with computer mouse based on a monitoring of subject activities and using Bayesian networks for identification decision making.

**Keywords.** pattern recognition, biometric systems, identification, authentication, intruder, identification features, computer mouse interacts features, keystroke dynamic.

#### References

1. Confidential information leaks. The preliminary results of the 2014. Zecurion Analytics, 2015. Available at : [http://www.zecurion.ru/upload/iblock/fe3/Zecurion\\_Data\\_leaks\\_2015.pdf](http://www.zecurion.ru/upload/iblock/fe3/Zecurion_Data_leaks_2015.pdf). (accessed 16.03.2015).

2. Global data leakage report 2015. InfoWatch analytic center, 2015. Available at: [http://www.infowatch.ru/sites/default/files/report/analytcs/russ/InfoWatch\\_global\\_report\\_2014.pdf](http://www.infowatch.ru/sites/default/files/report/analytcs/russ/InfoWatch_global_report_2014.pdf). (accessed 20.03.2015).

3. Didenko S.M., Shapcev V.A. Issledovanie dinamiki rabo-ty pol'zovatelja s manipuljatorom mysh' [The research of dynamics of user interacts with manipulator the mouse]. *Matematicheskoe i informacionnoe modelirovanie*, Tjumen': Izd-vo Tjum. un-ta, 2004. pp. 295–304.

4. Didenko S.M. Razrabotka i issledovanie komp'juternoj modeli dinamiki sistemy «pol'zovatel' - mysh'»: avtoref. dis. kand tehn. nauk [The development and research of computer model of system “user-mouse” dynamics dis. cand. technical science]. Tjumen', TjumGU, 2007. 18 p.

5. Monika Bhatnagar, Raina K Jain and Nilam S Khairnar. Article: A Survey on Behavioral Biometric Techniques: Mouse vs Keyboard Dynamics // IJCA Proceedings on International Conference on Recent Trends in Engineering and Technology 2013 ICRTET(5), May 2013. pp. 22-25.

6. Jain-Shing Wu, Chih-Ta Lin, Yuh-Jye Lee, Song-Kong Chong. Keystroke and Mouse Movement Profiling for Data Loss Prevention // Journal of Information Science and Engineering, 2015, № 31. pp. 23-42.

7. Salil P. Banerjee, Damon L. Woodard. Biometric Authentication and Identification using Key-

stroke Dynamics: A Survey // Journal of Pattern Recognition Research, 2012, №7. pp. 116-139

8. Margit Antal, László Zsolt Szabó, Izabella László. Keystroke Dynamics on Android Platform // 8th International Conference Interdisciplinarity in Engineering, INTER-ENG 2014, 9-10 October 2014, Tirgu Mures, Romania. pp. 1-7

9. Raskin D. *Interfejs: novye napravlenija v proektirovanii komp'juternyh sistem* [The interface: new directions in designing of computer systems]. St. Petersburg, Simvolpljus, 2010. 272 p.

10. Eremenko A.V., Levitskaja A.E., Sulavko A.E. Samotuga Razgranichenie dostupa k informacii na osnove skrytogo monitoringa dejstvij pol'zovatelej v informacionnyh sistemah: skrytaja identifikacija [Access control to information on the basis of hidden monitoring user activity in information systems: hidden identification]. *Vestnik SibADI*, 2014, no 6(40). pp. 92-102.

11. Sulavko A.E., Eremenko A.V., Levitskaja E.A. Razgranichenie dostupa k informacii na osnove skrytogo monitoringa dejstvij pol'zovatelej v informacionnyh sistemah: portret neloyal'nogo sotrudnika [Access control to information on the basis of hidden monitoring user activity in information systems: Portrait of a disloyal employee]. *Izvestija Transiba*, 2015, no 1(21). pp. 80-89.

12. Lozhnikov P.S., Sulavko A.E. Analiticheskoe issledovanie problemy raspoznavaniya obrazov v prostranstve maloinformativnyh priznakov [Analytical research of problems of pattern recognition in space of uninformative signs]. *Mezhotraslevaja informacionnaja sluzhba*, 2014, no 2 (167). pp.11-18.

13. Epifancev B.N., Lozhnikov P.S., Sulavko A.E. Sravnenie algoritmov kom-pleksirovaniya priznakov v zadachah raspoznavaniya obrazov [Comparison of algorithms of sings complexing in image recognition problems]. *Voprosy zashhity informacii FGUP «VIMI»*, 2012, no 1. pp. 60-66.

14. Gmurman V.E. *Teorija verojatnostej i matematicheskaja statistika* [Probability theory and mathematical statistics]. Moscow, Vyssh. shk., 2003. 479 p.

15. Epifancev B.N., Lozhnikov P.S., Sulavko A.E. Algoritm identifikacii gipotez v prostranstve maloinformativnyh priznakov na osnove

posledovatel'nogo primenenija formuly Bajesa [An algorithm of hypotheses identification in an uninformative attribute space based on consistent bayes' law]. *Mezhotraslevaja informacionnaja sluzhba*, 2013, no 2. pp. 57-62.

Борисов Роман Владимирович (Россия, Омск) – инженер-программист ООО "Люксофт Профешнл", Филиал ООО "Люксофт Профешнл" в городе Омск (644010, г.Омск, Учебная 83, к.1, e-mail: brv1986@yandex.ru).

Зверев Дмитрий Николаевич (Россия, Москва) – инженер-программист ООО «Интрокод» (127083, г. Москва, ул. Масловка Верхняя, д.20, строение 1).

Сулавко Алексей Евгеньевич (Россия, Омск) – кандидат технических наук, научный сотрудник кафедры комплексной защиты информации ФГБОУ ВПО ОмГТУ (644050, г. Омск, пр-кт Мира, 11, e-mail: sulavich@mail.ru).

Писаренко Виктор Юрьевич (Омск, Россия) – студент ФГБОУ ВПО ОмГТУ (644050, г. Омск, пр. Мира, 11, e-mail: j-e-d-y@mail.ru).

Roman V. Borisov (Russian Federation, Omsk) – engineer-programmer "Luxoft Professional" (644010, Omsk, Uchebnaya 83, b.1, e-mail: brv1986@yandex.ru).

Dmitriy Nikolaevich Zverev (Russian Federation, Moscow) – software engineer LLC "Introkod" (127083, Moscow, st. Maslivka top, d.20, Building 1).

Sulavko Alexey Borisov (Russian Federation, Omsk) – candidate technical sciences, Omsk State Technical University (OmSTU) (644050, Omsk, Prospect Mira, 11, e-mail: sulavich@mail.ru).

Pisarenko Viktor Yurievich (Russian Federation, Omsk) – student of Omsk State Technical University (OmSTU) (644046, Omsk, pr. Mira, 11, e-mail: j-e-d-y@mail.ru).

УДК 621.926

## ОБОБЩЕННАЯ МЕТОДИКА РАСЧЕТА БАКА ОТСТОЙНИКА ДЛЯ СИСТЕМЫ СМАЗКИ ДРОБИЛЬНО-РАЗМОЛЬНОГО ОБОРУДОВАНИЯ

С.В. Корнеев, Я.В. Ярмович, В.Н. Кузнецова

Омский государственный технический университет (ОмГТУ), Россия, г. Омск.

**Аннотация.** В данной статье рассматривается проблема сокращения затрат при эксплуатации дробильно-размольного оборудования (ДРО), связанная с большим расходом смазочного материала, так как объем систем смазки ДРО может составлять до 60 м<sup>3</sup>. Для сокращения расходов связанных с заменой смазочного материала в системе смазки ДРО, необходимо создать такой бак, в котором процесс очистки смазочного материала проходил бы постоянно, и в узел трения поступало масло необходимой чистоты. Для этого необходимо установить в бак системы смазки переливную перегородку, тем самым разделив его на две части, на отстойник и сам бак. В настоящее время нет обоснованной методики установки переливной перегородки, обычно ее устанавливают посередине бака. В данной статье предлагается обобщенная методика расчета бака