Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 9, Пенза-2014, с.76-78 (http://www.pniei.penza.ru/RV-conf/T9/C19)

НЕПРЕРЫВНАЯ ИДЕНТИФИКАЦИЯ СУБЪЕКТОВ НА ОСНОВЕ СКРЫТОГО МОНИТОРИНГА ПЕРИФЕРИЙНОГО ОБОРУДОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ[1]

Левитская Е.А. (г. Снежинск),
Ложников П.С., Сулавко А.Е., Еременко А.В. (г. Омск)

Мы живем в условиях постоянной информатизации общества, информационные технологии и сама информация играют все большую роль в жизни людей, ценность информации возрастает. Поэтому вопросы защиты информации от несанкционированных воздействий всегда остаются актуальными. В соответствии с The Global Stateof Information Security Survey 2014 – глобальным исследованием информационной безопасности, проведенным фирмой PwC и журналами CIO и CSO, основной причиной инцидентов, связанных с нарушением безопасности, являются сотрудники (31%) и бывшие сотрудники компаний (27%). По данным Zecurion Analytics суммарный ущерб от деятельности внутренних нарушителей в мире за 2013 и 2014 годы составил более 42 млрд. долл., и с каждым годом оценки ущерба растут. Использующиеся на практике процедуры аутентификации выполняют функцию разграничения понятий “Свой” и “Чужой”, не учитывая, что авторизованный пользователь, являющийся штатным сотрудником, может также оказаться нарушителем. Выше изложенная информация стимулирует исследователей и ученых на проведение научно-исследовательских и опытно-конструкторских работ по созданию систем защиты информации нового поколения от любого несанкционированного использования, в том числе, и от несанкционированных действий авторизованного пользователя информационной системы.

Предлагается подход к разграничению доступа, основанный на проведении непрерывной скрытой идентификации пользователя компьютерной системы в процессе его работы с электронным документом. В качестве идентификационных характеристик используются клавиатурный почерки особенности работы пользователя с мышью. Клавиатурный почерк характеризуется временами удержания и паузами между нажатием клавиш во время работы на компьютере. Сделана попытка адаптации закона Фиттса [1] для его использования в целях получения количественных оценок особенностей работы субъектов с мышью [2]. Данный закон касается сенсорно-моторных процессов человека и связывает время движения субъекта к наблюдаемой цели с точностью движения и с расстоянием перемещения. 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. При внесении коррекции движений проявляются индивидуальные особенности человека. В качестве признаков, формируемых при работе с мышью, решено использовать следующие: скорость перемещения курсора мыши между элементами интерфейса, максимальное и среднее отклонения в пикселях от кратчайшего пути

1 - Работа выполнена в рамках проекта РФФИ № 15-37-21109

перемещения курсора мыши между элементами интерфейса (C_{max} и C_{mid} на рис. 1), тремор курсора мыши. Нормирование скорости перемещения курсора мыши между элементами интерфейса производится по формуле (1), заимствованной из [2]. Указанные величины, характеризующие индивидуальность клавиатурного почерка и особенностей работы с мышью субъекта имеют нормальное распределение. Проверка гипотезы о распределении выполнялась с помощью критерия хи-квадрат.

$$V_{\text{mid}} = \frac{T}{\log_2(\frac{D}{W}+1)}, \qquad (1)$$

где T — время, которое было затрачено на перемещение курсора мыши от одного элемента интерфейса к другому в миллисекундах, D — дистанция от точки начала движения до центра элемента интерфейса, к которому направляется курсор (в пикселях), W — ширина элемента интерфейса, к которому направляется курсор, измеренная вдоль оси движения в пикселях.

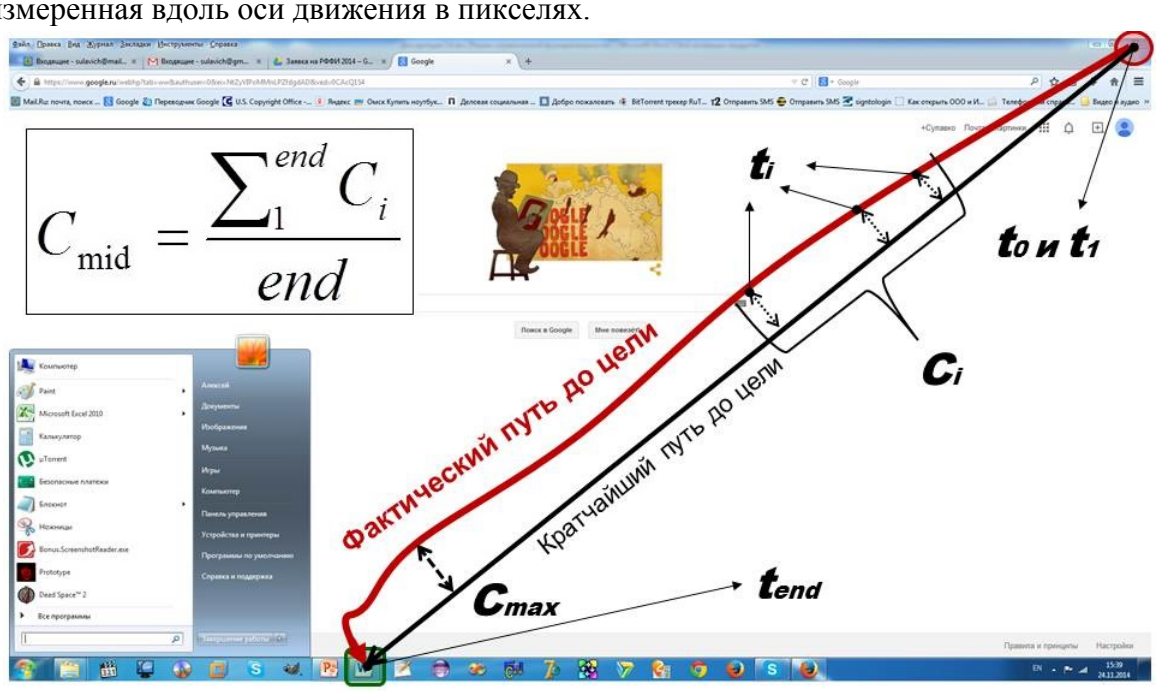

Рис.1.Принцип вычисления значений признаков, сформированных особенностями работы с мышью

Формирование эталона субъекта осуществляется в процессе работы за компьютером. При увеличении базы данных признаков хранение всех значений указанных величин становится нецелесообразным. Поэтому более удобным при реализации процедуры создания эталона является рекуррентное вычисление оценочных значений параметров нормального закона распределения – математического ожидания и среднеквадратичного отклонения по формулам (2) и (3) [3], соответственно. При формировании эталона в реальном времени вычисляются значения признаков, но сохраняется только общее число уже использованных примеров и текущее значение математического ожидания.

$$M_K = \frac{K-1}{K} \cdot M_{K-1} + \frac{X_K}{K}, \qquad (2)$$

где X – значение биометрического признака, K – количество значений признака, использованных ранее для обучения.

$$\sigma_K = \sqrt{\frac{K-2}{K-1} \cdot \sigma_{K-1}^2 + \frac{(X_K - M_K)^2}{K-1}}, \qquad (3)$$

где X – значение биометрического признака, K – количество значений признака, использованных ранее для обучения, M_K – оценка математического ожидания на основании K значений признака. Решения о предоставлении доступа принимаются в процессе работы субъекта на компьютере на основе усовершенствованной стратегии Байеса, учитывающей параметры и взаимное расположение функций плотностей вероятности значений признаков [2].

Предлагаемый подход включает не только процедуру идентификации в реальном времени, но и оценку лояльности действий, воспроизводимых субъектом в системе. Если действия пользователя классифицируются как опасные, доступ к отдельным фрагментам документа будет ограничен. На данный момент ведутся исследования с целью разработки методики автоматического определения нелояльного поведения субъекта. Были сделаны следующие выводы касательно возможности определения нелояльного поведения пользователя:

1. Чем выше дисперсия фактических показателей количества произошедших событий безопасности (операции с файлами, запуск программ, использование “горячих” клавиш) в определенное время суток от их среднего числа, полученного в результате многократных наблюдений в это же время суток, тем выше степень неопределенности действий пользователя. Спонтанное изменение данной дисперсии может указывать на нелояльность действий или изменение выполняемых задач.
2. При реализации нарушений режима доступа к информации нестабильность клавиатурного почерка и особенностей работы субъекта с мышью возрастает. Увеличение дисперсии регистрируемых значений признаков может свидетельствовать о совершении пользователем противоправных действий.
3. При разработке методики распознавания нелояльного поведения пользователя в компьютерной системе целесообразно учитывать его психоэмоциональное состояние, которое можно оценить дистанционно [4].

ЛИТЕРАТУРА:

1. Раскин Д. Интерфейс: новые направления в проектировании компьютерных систем. — СПб: Символ-плюс, 2010. — 272 с.
2. Еременко А.В., Левитская Е.А., Сулавко А.Е., Самотуга А.Е. Разграничение доступа к информации на основе скрытого мониторинга действий пользователей в информационных системах: скрытая идентификация // Вестник СибАДИ. – 2014, №6 (40). - С. 92-102.
3. Брюхомицкий Ю. А. Учебно-методическое пособие к циклу лабораторных работ «Исследование биометрических систем динамической аутентификации пользователей ПК по рукописному и клавиатурному почеркам» по курсу: «Защита информационных процессов в компьютерных системах» / Ю. А. Брюхомицкий, М. Н. Казарин. − Таганрог: Изд-во ТРТУ, 2004. – 38 с.
4. Epifantsev B.N., Lozhnikov P.S., Kovalchuk A.S. Hidden identification for operators of information-processing systems by heart rate variability in the course of professional activity / Dynamics of Systems, Mechanisms and Machines (Dynamics), 11-13 November 2014, Omsk, Russia – p.1-4.

Материал поступил 19.12.2015. Публикуется по положительной рецензии к.т.н. Егорова В.Ю.