Д. В. Соколов

КОМПЬЮТЕРНАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ «ПОЛЬЗОВАТЕЛЬ – МЫШЬ»

Цель исследования состоит в разработке компьютерной модели работы пользователя с манипулятором мышь; объектом исследования является компьютерный образ системы «пользователь — мышь».

В работе принцип сбора информации основывается на записи координат указателя мыши.

Основные положения:

1) производится анализ не только движения мыши, но также и нажатия кнопок пользователем (время, частота нажатия);

2) время снятия характеристик — 0,279 мс;

3) фиксируются все манипуляции с мышью;

4) анализируются не просто движения, но и объекты, с которыми эти движения происходят (анализ активных окон).

В результате работы была составлена модель, состоящая из: T — время движения манипулятора до остановки; L — длина (погонная) траектории; $V_{ср}$ — средняя скорость движения указателя; δ — время между остановкой указателя и подтверждающим нажатием кнопки манипулятора.

Данное количество анализируемых параметров создает меньшую нагрузку на компьютерную систему.

СПИСОК ЛИТЕРАТУРЫ:

1. *Болл Р. М., Коннен Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У.* Руководство по биометрии. М.: Техносфера, 2007.
2. *Zach Jorgensen, Ting Yu*. On Mouse Dynamics as a Behavioral Biometric for Authentication. Proceedings of the Sixth ACM Symposium on Information, Computer, and Communications Security (AsiaCCS). 2011. С. 476—482.

Е. С. Степанова

МЕТОДИКА ОЦЕНКИ СТОИМОСТИ ИНФОРМАЦИИ НА ОБЪЕКТЕ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ АППАРАТА НЕЧЕТКОЙ ЛОГИКИ

Оценка риска заключается в качественном или количественном определении его уровня. Величина риска, связанного с реализацией угрозы нарушения безопасности информационного актива, определяется как функция двух величин: вероятности успешной реализации угрозы с использованием уязвимостей и его стоимости. Количественная оценка более предпочтительна при решении задач выбора рациональных наборов средств защиты, так как позволяет судить об адекватности инвестиций в информационную безопасность.

Проведенный обзор известных публикаций в данной предметной области, в том числе [1], показал отсутствие методик количественного оценивания стоимости информации; программные продукты, автоматизирующие оценку риска нарушения ИБ, решают лишь проблему оценки уровня угроз и также не содержат таких методик.