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.

Таким образом, проблема численной оценки стоимости информации при анализе риска нарушения информационной безопасности является актуальной.

Методика, реализующая предложенный метод, заключается в следующем:

1. С учетом принятых в организации уровней критичности информации производится идентификация информационных активов, с указанием сегментов сети, в которых они обрабатываются.

2. Для каждого информационного актива определяется перечень возможных приемлемых видов последствий в результате нарушения его защищенности. Перечень формируется в соответствии с критериями, предложенными в [1] в качестве основы для определения ценности информационных активов.

3. Определяются значения входных переменных $|O_x|$ – количество информационных объектов, обрабатываемых в сегменте сети x, и $|K_x|$ – количество всех возможных видов последствий нарушения свойств ИБ для информационных объектов сегмента сети x.

4. Задаются функции принадлежности входных лингвистических переменных: A – нечеткая ЛП, соответствующая входной переменной $|O_x|$; B – нечеткая ЛП, соответствующая входной переменной $|K_x|$.

5. Формулируются продукционные правила, позволяющие представить опыт эксперта в формализованном виде и отражающие влияние значений входных переменных на ценность информационных объектов сегмента сети.

6. Задаются функции принадлежности выходных лингвистических переменных «ценность информационного объекта» Cm_{O_x} для активов всех уровней критичности. Область определения переменной: $Cm_{O_x} \in [0,1]$.

7. В соответствии с продукционными правилами, значениями входных лингвистических переменных определяются нечеткие значения выходных лингвистических переменных «ценность информационного объекта» D.

8. После дефаззификации – отображения нечеткой ЛП D в (четкое) значение выходной переменной Cm_{O_x} – производится нормализация полученных величин и вычисляются относительные стоимости информационных объектов, обрабатываемых в сегментах сети организации:

$$Cm_{C_n^{\text{H}}} = \frac{Cm_{O_n^H}}{Cm_{\sum}}$$

$$Cm_{C_m^{\text{C}}} = \frac{Cm_{O_m^C}}{Cm_{\sum}},$$

$$Cm_{C_l^{\text{B}}} = \frac{Cm_{O_l^B}}{Cm_{\sum}}$$

где $Cm_{\sum}$ – ценность всех информационных ресурсов, обрабатываемых во всех сегментах сети, т. е.

$$Cm_{\sum} = \sum_{n \in N} Cm_{O_n^H} + \sum_{m \in M} Cm_{O_m^C} + \sum_{l \in L} Cm_{O_l^B};$$

$Cm_{C_n^{\text{H}}}$, $Cm_{C_m^{\text{C}}}$, $Cm_{C_l^{\text{B}}}$ – относительные стоимости информационных ресурсов, обрабатываемых в сегментах C_n^H, C_m^C и C_l^B соответственно.

На рис. 1 приведена схема нечеткого вывода применительно к решению проблемы оценки стоимости информационных объектов при анализе рисков нарушения ИБ.

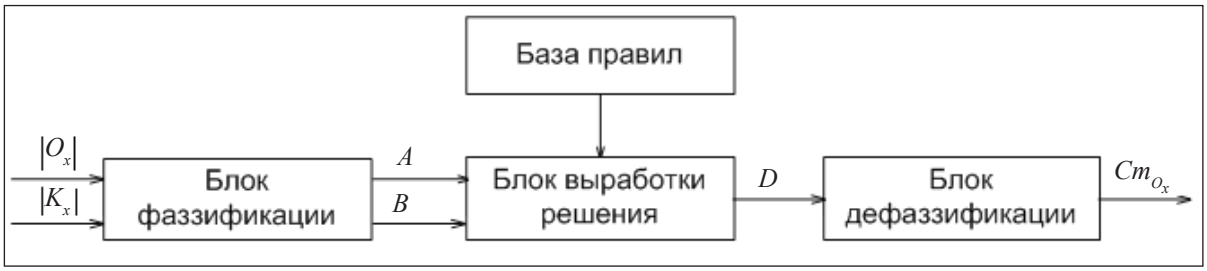

Рис. 1. Система нечеткого вывода

Метод, алгоритм которого приведен выше, апробирован с целью анализа его функциональности.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р ИСО/МЭК 27005-2010 «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

А. В. Титов, В. О. Чуканов

МЕТОДИКА ОЦЕНКИ ПАРАМЕТРОВ НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В работе предложена методика оценки параметров надежности информационных систем персональных данных при редких событиях отказов в системе. Применение методики является частью комплекса мероприятий по обеспечению функциональной безопасности таких систем.

Методика включает совокупность взаимосвязанных этапов, позволяющих оценить границы параметров надежности системы с заданной степенью точности.

На первом этапе проводится оценка параметров надежности однотипных модулей системы при условии ограниченного объема статистических данных об отказах.

На втором этапе обосновывается возможность объединения статистических данных, полученных для однотипных модулей, применяемых на разных объектах. В некоторых случаях возможно построение нескольких пересекающихся или непересекающихся объединенных серий наблюдений.

Третий этап представляет собой вычисление уточненной оценки параметров надежности системы после объединения статистических данных.

Таким образом, рассматриваемая методика позволяет производить объединения статистических данных и может быть использована при анализе отказов программных средств однотипных изолированных информационных систем персональных данных.