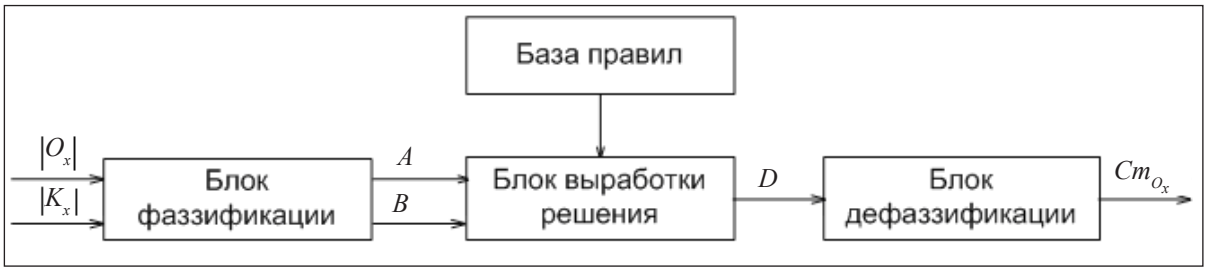

Рис. 1. Система нечеткого вывода

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.

СПИСОК ЛИТЕРАТУРЫ:

1. *Чуканов В. О.* Надежность программного обеспечения и аппаратных средств систем передачи данных атомных электростанций: Учебное пособие. М.: МИФИ, 2008. — 180 с.
2. ГОСТ Р МЭК 61508-4-2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения».
3. *Rubino G., Tuffin B.* Rare Event Simulation Using Monte Carlo Methods. John Willey & Sons Ltd., 2009. — 271 p.
4. *Durairaj G., Koren I. and Krishna C.M.* Importance Sampling to Evaluate Real-Time System Reliability: A Case Study // Simulation. Vol. 76. № 3. March 2001. P. 172–183.

А. А. Тихомиров, А. И. Труфанов, В. Н. Дмитриенко, А. Россодивита, Е. В. Шубников

КЛАССИФИКАЦИЯ АТАК В ИМИТАЦИОННЫХ ИССЛЕДОВАНИЯХ УЯЗВИМОСТИ КОМПЛЕКСНЫХ СЕТЕЙ

Большинство социальных, биологических и технологических сетей демонстрируют свои существенные нетривиальные топологические особенности, со связями между их элементами, которые невозможно определить однозначно как регулярные или случайные. Такие особенности включают в себя тяжелые хвосты распределений связующего, высокие значения коэффициента кластеризации, ассортативность и диссортативность узлов, общинные и иерархические структуры. Подобные сети называют комплексными сетями (КС) [1–3].

Устойчивость сетевой архитектуры является одной из важнейших проблем построения любых систем. Оценке стойкости комплексных сетей при воздействии дестабилизирующих угроз в рамках имитационных исследований посвящен значительный объем научных публикаций, в том числе [4–15]. Моделирование (генерация) атаки в КС заключается, как правило, в удалении элементов сети в соответствии с заранее заявленными алгоритмами угроз и уязвимостей и последующем анализе изменений сети. Выбор угроз и уязвимостей во многих работах определяется информированностью и предпочтениями авторов, причем зачастую слабо аргументирован или не аргументирован вовсе. При этом характерно, что область комплексных сетей является междисциплинарной площадкой, где базовые позиции занимают физики, математики и специалисты ИТ. Таковые обычно либо не принимают во внимание, либо принимают лишь на уровне интуиции известное определение теории информационной безопасности, утверждающее, что атака — это пара «источник угрозы — уязвимость», реализующая угрозу и приводящая к ущербу. С учетом данного определения в настоящей работе предлагается краткий обзор основных атакующих действий, значимых при моделировании деградации сетей, имеющих комплексную структуру, и следующая классификация атак.

1. Защищенность элемента сети. Как правило, исследователи изначально рассматривали незащищенные, полностью уязвимые элементы, а угрозы в таком случае тождественны атакам [4]. Учет защиты элементов сети наблюдается в работах нынешнего десятилетия [5–6].

2. Атакуемый элемент. Таким элементом может быть как узел, так и связь. Основной мишенью с первых работ по имитации атак на КС является узел [7]. Связь как мишень используется реже [8].

3. Принадлежность к антропогенному источнику угроз. Большинство обзоров КС классифицирует угрозы по единственному признаку и делит на две группы: случайные и преднамеренные (зачастую соответствующие реализации называют «сбоями» и непосредственно «атаками» [9]) .