С. Ж. Симаворян (Сочи, СГУТиКД)**. Понятие неопределенности в задачах защиты информации.**

К настоящему времени стал совершенно очевидным и получил всеобщее признание тот факт, что на решение задач защиты информации в автоматизированных системах обработки данных (АСОД) большое влияние оказывают неопределенности, связанные со злоумышленными действиями людей-нарушителей. Анализ задач защиты информации показывает, что многие параметры задач невозможно описать количественно, поскольку они носят лингвистический, качественный характер [1], [2], [4]. Классификация неопределенностей, встречающихся в задачах защиты информации в АСОД, приводится в работах [1], [2].

Неопределенности: неизвестность, неполнота, недостаточность, неадекватность и недостоверность характеризуют качественное описание количества отсутствующей информации об элементах задач защиты информации. Например, неизвестность планов противника, связанных со злоумышленными действиями; неадекватность имеющихся моделей защиты информации применительно к АСОД; недостаточность требований по защите информации и т. д. Недостоверность делится на физическую и лингвистическую неопределенности. Источником физической неопределенности является внешняя среда, а именно, наличие неточностей при определении величин с помощью вычислений (измерений) физическими приборами и наличие случайных событий связанных со злоумышленными действиями. Источником лингвистической неопределенности является язык используемый лицами принимающими решения для управления защитой информации. Лингвистическая неопределенность порождается, с одной стороны, многозначностью значений слов (понятий и отношений) в языке, т.е. полисемией, а с другой стороны — неоднозначностью смысла фраз. Если отображаемые одним и тем же словом объекты системы защиты информации различны, то имеет место ситуация омонимии, если сходны, то ситуация нечеткости (расплывчатости, размытости, неясности). Неоднозначность смысла фраз может быть синтаксической или семантической.

В подобных ситуациях задачи защиты информации трудноформализуемы и хорошо развитые методы анализа строго или полностью определенных процессов не всегда эффективны. Опыт применения методов классической теории систем к задачам такого типа показывает их недостаточность для адекватного моделирования процессов существенно зависящих от воздействия трудно предсказуемых факторов. Для решения таких задач наиболее подходящими являются методы нечетких множеств [5], лингвистических переменных [3], неформального оценивания и неформального поиска оптимальных решений [1], [2].

Основные положения названных методов необходимо включить в курсы лекций по предметам по защите информации и информационной безопасности. Эффективность использования вышеназванных методов подтверждается результатами положительного восприятия студентами СГУТиКД материала по защите информации в целом и практической значимостью использования лингвистических переменных при вычислении вероятностей уязвимости информации, полноты и эффективности решения задач защиты информации, оценки качества и надежности средств защиты информации, адаптируемости систем защиты информации, а также определения таких функций, как принадлежность нечеткому множеству каналов несанкционированного получения информации, нечеткому множеству злоумышленников,

СПИСОК ЛИТЕРАТУРЫ

1. *Герасименко В. А.*, *Малюк А. А.* Основы защиты информации. М: 1997, 540 с.
2. *Симаворян С.Ж.* Проектирование систем защиты информации в АСУ специального назначения. Автореферат на соискание уч. ст. канд. техн. наук. М: РГГУ, 1991.

3. *Заде Л.* Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: Мир, 1976.
4. *Корченко А.* Построение систем защиты информации на нечетких множествах. Теория и практика. Изд-во «МК-ПРЕСС», 2006, 320 с.
5. *Орловский С. А.* Проблемы принятия решений при нечеткой исходной информации. М.: Наука, 1981, 208 с.