

ции). Такое ее рассмотрение открывает широкие возможности для формальных преобразований аннотированных программ и формальных доказательств свойств программ, что является основной для верификации и оптимизации программ. Аннотированные программы являются также ценным компонентом документации и могут эффективно использоваться в процессах отладки (тестирования) и контроля работы программы.

## **2.5. ОСНОВЫ МЕТОДИКИ ЛОГИЧЕСКОЙ СПЕЦИФИКАЦИИ ПРОГРАММ**

Логический язык спецификаций дает формальные средства для выражения отношений между программными переменными в виде логических инвариантов. Остановимся теперь на методологических вопросах использования этих средств при спецификации свойств программ. Возникающие здесь задачи можно разделить на две группы:

- 1) разработка аксиоматических теорий проблемных областей, объекты которых представляются переменными программы;
- 2) разработка индуктивных утверждений для соответствующих точек или регионов программы в виде формул созданной в п. 1 аксиоматической теории.

Первая задача является наиболее важной при спецификации, так как по существу определяет обобщенные знания, используемые при спецификации некоторого класса программ. Прежде чем записывать формулы для тех или иных утверждений о программных объектах, необходимо иметь используемую в них систему понятий (функций) вместе с аксиомами, характеризующими семантику этих понятий. Вопросы состоят в том, как выбирать эти понятия и как их аксиоматизировать. Для ответа на эти вопросы требуется соответствующая методика, так как они не решаются (в достаточно общих постановках) автоматически.

При выборе системы понятий для спецификации следует прежде всего стремиться к естественности понятий и их выразительности. Удачная система понятий во многом определяет успех как спецификации программы, так и последующей верификации. Число понятий, относящихся к одному уровню иерархии, должно быть ограничено для удобства манипулирования ими. Здесь в полную меру действует известный в психологии принцип (закон Миллера): число одновременно используемых объектов не должно превышать семи. Это означает, что каждое выбираемое понятие должно быть достаточно «емким», представительным. В то же время понятия должны характеризоваться по возможности малым числом аксиом, что предъявляет требования к их выбору. Выбор, таким образом, есть компромисс между выразительностью и сложностью понятия.