

МОДЕЛЬ СИСТЕМЫ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНОГО ЗДАНИЯ НА ОСНОВЕ БАЙЕСОВСКОГО ПОДХОДА

Ширшова Е.Ю.

Научный руководитель – к.т.н., доцент Валеев С.С.

Уфимский государственный авиационный технический университет

Мировой опыт эксплуатации зданий свидетельствует о том, что подсистемы здания нельзя рассматривать как обособленные. Взаимосвязь подсистем становится особенно важной при возникновении критических ситуаций (например, пожар, несанкционированный доступ на объект и т.д.). Органичное объединение систем жизнеобеспечения-безопасности-информатизации привело к появлению так называемых интеллектуальных зданий.

Проектирование такого сложного объекта требует определенного концептуального подхода. Он должен быть направлен на обеспечение экономичности, комфортности и безопасности. Неоспоримую значимость имеет система безопасности, являющаяся также сложной системой, которая характеризуется многоуровневостью, сложностью информационно-логических связей, наличием большого количества неопределенностей, параллельностью процессов протекающих в этой системе. Для создания и обеспечения функционирования системы безопасности необходимо построение моделей, которые соответствовали бы реально существующей системе и с достаточной полнотой описывали бы процесс защиты информации.

Исходя из того, что процесс защиты довольно трудно представить аналитически, предпочтительнее имитационные методы. В процессе имитации фиксируются определенные события и состояния, по которым можно определить количественные характеристики эффективности системы.

При формализации процессов обеспечения безопасности информации целесообразно использовать свойства байесовских сетей. С помощью байесовских сетей можно описать процесс обеспечения безопасности с достаточной степенью детализации.

Ацикличность вычислений и возможность переоценки тех или иных следствий их априорной информации является важным практическим преимуществом и отличает байесовские сети от других методик моделирования.

На основе байесовского подхода разработана модель системы безопасности интеллектуального здания. Моделирование наиболее распространенных угроз, таких как пожар и несанкционированное проникновение, позволили выявить недостатки системы, коррекция которых на этапе проектирования имеет принципиальное значение. В качестве вероятностей в первом случае соответственно использовалась вероятность реагирования системы, во втором - вероятность срабатывания систем на несанкционированное проникновение в интеллектуальное здание.