УДК 681.324

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ

Погорелов Д.Н.
Научный руководитель – к.т.н., доцент Валеев С.С.
Уфимский государственный авиационный технический университет

Объектом исследования является информационная система предприятия, разрабатывающего сложные технические объекты (СТО). Особенностями автоматизированных систем обработки данных (АСОД) на таких предприятиях являются:

- распределенность АСОД;
- длительность жизненного цикла разрабатываемых СТО порядка 10-15 лет.

Целями создания системы управления защитой информации (ЗИ) на предприятии являются: оптимизация расходов на информационную безопасность, повышение эффективности ЗИ.

Защита информации является слабо формализуемой областью, поэтому при создании системы управления ЗИ использовались стохастические методы управления.

При разработке системы управления ЗИ с учетом особенности распределенности АСОД была выбрана двухуровневая архитектура, где первым уровнем (стратегическим) является интеллектуальная подсистема принятия решений, функциями которой являются: анализ событий безопасности в АСОД, анализ состояния АСОД, прогнозирование состояния АСОД. На основании результатов анализа подсистема принятия решений формирует новое задание по безопасности и передает его на второй (тактический) уровень. Тактический уровень представлен программными агентами, которые размещены во всех узлах АСОД и специализированы в соответствии с функциями, которые этот узел выполняет. Функциями агентов являются: регистрация событий, влияющих на информационную безопасность, передача данных о зарегистрированных событиях в базу данных подсистемы принятия решений, оперативный анализ состояния узла и принятие мер по его защите в случае атаки. Метод принятия решений о наличии атаки на узел строится на основе байесовских сетей доверия и метода анализа иерархий.

Подсистема принятия решений так же содержит информацию о СТО, которые разрабатываются на предприятии. За столь длительный срок (10-15 лет), которые составляют жизненный цикл СТО, ценность информации изменяется, информация стареет. Для учета этих изменений с использованием метода анализа иерархий определяются коэффициенты старения для каждого изделия на каждом этапе ЖЦ. Эти коэффициенты учитываются при формировании задания по безопасности.

Для отображения проанализированных данных о состоянии АСОД в меры по защите информации используется аппарат нечеткой логики.

Использование интеллектуальной системы управления ЗИ на предприятии позволяет обеспечить регистрацию событий, влияющих на безопасность, их анализ в соответствии с заложенной логикой, оперативное противодействие атакам, прогнозирование состояния АСОД, минимизацию расхождений между требуемым и существующим уровнями ЗИ. Так же данные о безопасности могут предоставляться для анализа специалистам по ЗИ.