

ПРИНЦИПЫ ОПТИМИЗАЦИИ УПРАВЛЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИЕЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В работе рассмотрены принципы оптимизации управления технической эксплуатацией систем защиты информации, которые заключаются в оптимизации систем технической эксплуатации при минимальной целевой функции и выполнении ограничений по обеспечению безопасности. На основании проведенных исследований предлагается использовать имитационную модель.

Ключевые слова: система защиты информации, теория графов, оптимальная система технической эксплуатации, критериальный анализ.

Введение. Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых является массовое применение ПЭВМ; усложнение информационных технологий; необходимость защиты не только государственной и военной тайн, но и промышленной, коммерческой и финансовой тайн, расширяющие возможности несанкционированных действий над информацией.

Кроме того, следует учитывать, что современный этап развития автоматически характеризуется значительным усложнением задач управления системами защиты в связи с переходом от автоматизации отдельных объектов и подсистем к комплексной автоматизации управления всей системой. Вследствие этого традиционное содержание теории автоматического управления и регулирования стало слишком простым. Возникла необходимость включения в эту теорию ряда новых вопросов, связанных с эксплуатацией и управлением эксплуатацией систем защиты. Особенно это важно для систем, которые представляют из себя сложные многофункциональные системы.

Основная часть. Очевидно, что основной совершенствования технической эксплуатации (ТЭ) систем защиты информации (СЗИ) является комплексный подход к концепции эксплуатации СЗИ по техническому состоянию, базирующейся на организационно-технической структуре системы. В частности, создание такой высокоэффективной системы требует решения комплекса оптимизационных задач и выбор соответствующих критериев оптимизации. Исследования [1,2,3] и др., обосновавшие ряд критериев оптимальности системы ТЭ СЗИ, и анализ организационно-технической структуры позволяют в качестве экономического критерия

$$\Phi = f(\min a_c), \quad (1)$$

где $a_c = \sum_{k=1}^N c_k$.

Многокомпонентный критерий Φ является целевой функцией и требует соблюдения ограничения по обеспечению безопасности:

$$F(R_i) \leq F^*(R_i) \quad (2)$$

Здесь $F(R_i)$ вероятность появления особых ситуаций в обеспечении защиты информации, нормирующихся нормативными документами (при $i = 1, \dots, 4$);

* - индекс нормировки.

Тогда основные экономические принципы управления системами ТЭ СЗ определяется следующим образом:

- 1) минимизация затрат при обеспечении нормированного уровня защиты;
- 2) минимизация затрат, соответствующих заданному изменению уровня защиты.

Ввиду многокритериальности оценки системы ТЭ СЗИ оптимальные управляющие воздействия всегда являются комплексными и улучшение одного критерия оптимизации сопровождается ухудшением другого.

Составляющие из критерия (I) в свою очередь зависят от этапов процесса эксплуатации СЗИ, таких, как хранение, подготовка к применению, работа по назначению, техническое обслуживание и ремонт.

При эксплуатации СЗИ происходит как процесс изменения технического состояния (изнашивание, физико-технические изменения материалов), так и целенаправленный управляемый процесс восстановления СЗИ при техническом обслуживании и ремонте. Текущее состояние СЗИ определяется совокупностью этих процессов и описывается вектором в n -мерном пространстве. Таким образом, основой для принятия решения по эксплуатации СЗИ является ее техническое состояние, определяемое, в первую очередь, при диагностировании объекта с использованием системы – выявление (распознавание) состояний объекта с целью выработки управляющих решений, определяющих этап (состояние) эксплуатации обеспечивающих выполнение условий (2).

Обозначим символом «А» объект СЗИ, а этап его эксплуатации: B - применение по назначению; C - оперативное обслуживание; d - периодическое техническое обслуживание (ТО); e - направление на капитальный ремонт; f - ремонт и т.д. Тогда для жизненного цикла объекта в общем виде имеем:

$$\dot{Y}_a = \{b, c, d, e, f, \dots\}. \quad (3)$$

Этому выражению соответствует граф, представленный на рисунке.

Аналогичный граф может быть построен для различных состояний СЗИ, соответствующих этапов ее эксплуатации [1,2]. Причем, как показано в [2], состояние СЗИ однозначно связаны с вероятностью появления особых ситуаций при эксплуатации. В свою очередь состояние СЗИ может быть определено путем оценки множества ее динамических параметров[3] и (или) апостериорных (априорных при прогнозе) множества значений при показателе надежности.

Таким образом, для процесса ТЭ выражение можно сформулировать связь множества P_0 значений v -х показателей надежности, множества D_j значений j -х диагностических признаков СЗИ, множества P_0 показателей надежности и соответствующих этапов эксплуатации СЗИ:

$$R_i \Rightarrow [P_e, D_j] \Leftrightarrow B_i \Leftrightarrow \dot{Y}_0. \quad (4)$$

Очевидно, что это соотношение должно обеспечивать выполнение условия (2).

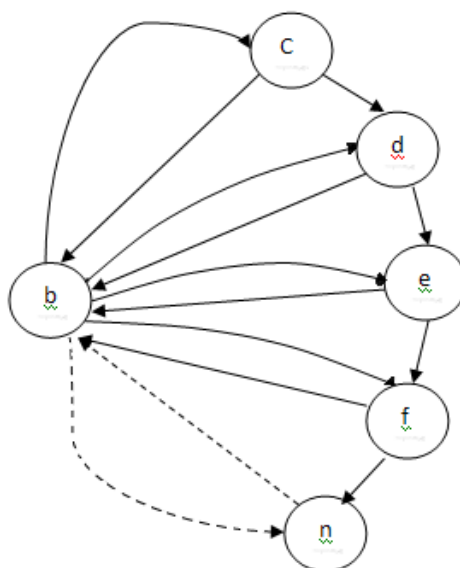


Рис. 1. Граф состояний СЗИ при эксплуатации

Выводы. Учитывая изложенное, сформулируем основной принцип соответствия оптимальной системы ТЭ СЗИ: оптимальная система ТЭ должна обеспечивать условия адекватности согласно выражению (4) при минимизации целевой функции (1) выполнении ограничения (2).

Поэтому выбор и оценку последствий управляющих воздействий предполагается выполнять на основе имитационных моделей в настоящее время уже разработанных для некоторых функциональных СЗИ.

ЛИТЕРАТУРА

1. Егоров Ф.И. – Задачи защиты информации / Егоров Ф.И., Тискина Е.О., Хорошко В.А. //Захист інформації, №1, 2009. – с.5-12.
2. Тискина Е.О. – Моделирование процесса управления комплексной системой защиты объекта / Тискина Е.О., Хорошко В.А. // Зб. наук. праць СНУЯЕП, №2(70), 2009. – с.153-160.
3. Гурина С.А. – Живучесть систем защиты информации в условиях внешних воздействий / Гурина С.А., Егоров Ф.И., Хорошко В.А. // Захист інформації, №2, 2008. – с.69-73.
4. Козлова К.В.- Кількісна оцінка захисту радіоелектронних об'єктів / Козлова К.В., Хорошко В.О. // Захист інформації, №1, 2007. – С.30-33.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Конахович Г.Ф.