В работе рассматривается теория прогнозирования состояния технической системы защиты информации на основании сетей Петри.

Ключевые слова: техническая система защиты, прогнозирование состояния системы, сети Петри.

В роботі розглядається теорія прогнозування стану технічної системи захисту інформації на основі мереж Петрі.

The theory of prediction for technical system state on the basis of Petri nets is described in the article.

Рецензент:д.т.н., проф.Шелест М.Є.
Надійшла 10.09.2010

УДК 629.735.06:004.681

Пискун И.В.

МОДЕЛЬ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМ СОСТОЯНИЕМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Вступление

Модель управления техническим состоянием (ТС) систем защиты (СЗ) должна учитывать [1,2], что СЗ являются подсистемами сложной системой защиты информации (СЗИ) от утечки по одному из каналов несанкционированного получения информации, которые, в свою очередь, являются элементами комплексной системой технической защиты информации (КС ТЗИ), и что сама система управления ТС СЗ должна строиться, исходя из соблюдения принципа жизненного цикла СЗИ.

Относительно КС ТЗИ система управления ТС СЗ должна рассматриваться как система управления эффективностью и таким образом должна быть направлена на выполнения этой задачи путем выбора оптимальных решений, обеспечивающих минимизацию затрат на эксплуатацию СЗИ и обеспечения требуемого уровня защищенности объекта.

Основная часть

Применительно к ТЗИ безопасность информации характеризуется ее уровнем защиты. Таким образом, система управления состоянием СЗ должна быть направлена на поддержание требуемого уровня защищенности объекта СЗ.

Так как любая СЗ является элементом СЗИ, то система управления их состоянием должна разрабатываться от объекта – СЗИ, при этом в качестве критериев оценки оптимальности систем управления должны выбираться такие показатели, которые органически вытекают из показателей, выбранных для системы управления годностью СЗИ.

Следовательно, система управления ТС СЗ должна быть направлена на предотвращение функциональных отказов и построена таким образом, чтобы затраты на ее обслуживание и ремонт в процессе эксплуатации были минимальными.

Методологическая взаимосвязь указанных принципов организации системы управления ТС СЗ приведена в табл. 1 – 4.

Таблица 1. Методологическая взаимосвязь организации системы управления ТС СЗ в составе КСТЗИ

Объект	Характеристика	Система управления	Оценка
КСТЗИ	Эффективность эксплуатации СЗИ	Эффективностью	$С_э$, $Р_п$
СЗИ	Обеспечение требуемой защищенности	Требуемой защиты	$К_э$, $К_{тз}$
СЗ	Функциональное состояние	Технологическим состоянием	$К_{эф}$, $К_{фс}$

Таблица 2. Содержание модели управления ТС СЗ

Характеристика СЗ	Система управления СЗ	Оценка СЗ
Функциональное состояние	Управляющие воздействия	$К_{эф}$=затраты $С_с$ $Р_{эф}$ – вероятность появления состояния

Таблица 3. Формулировка модели управления ТС СЗ

Функциональные состояния	Управляющие воздействия	Затраты	Вероятности состояния
Изменение функциональных параметров $y_м = \mu(1,k)$	1.Замены: а) плановые $Т_п$; б) случайные $M[1]=T^*_{пз}$ 2. Контроль: $t_k,\ \alpha, \beta$	Весовые коэффициенты $С_з$ $С_{з,к}=С_з+С_к$	$P(T_з)$ – безотказности, $P(H)$ - работоспособности

Таблица 4. Аналитическое задание модели управления ТС СЗ

Функция модели управления	**Целевая функция**	**Ограничения**
$\Phi_i = F_i(y_1, \dots, y_m, V_1, \dots, V_m)$	$\min Э_{фс}$ $Э_{фс} = С_с(Т_{пз}, Т^*_з, t_k, С_з, С_{зк})$	$\lambda^*(S_i)$ $\lambda^*(S_i) \gg \lambda^*(\Phi_{n-1}, \dots, \Phi_i)$

Предложим, что СЗ характеризуются некоторым множеством параметров у, которые будем называть функциональными, и внешних параметров В, определяющих ожидаемые условия эксплуатации. Считаем, что любая СЗ удовлетворяет параметрам В.

Рассмотрим множество состояний СЗИ $С_i$, которые в соответствии с [3] адекватны особым ситуациям при защите объектов информации R_i (i=1, 4). При этом необходимо рассматривать множество таких состояний СЗ S_i, которые соответсвуют $С_i$, т.е. $S_i \Rightarrow С_i$.

Рассмотрим множество функциональных параметров У. Очевидно, что множеству $У_0$ соответствует условие нормального функционирования системи (состояния $S_0 \Rightarrow С_0$).

С точки зрения управления ТС СЗ множество параметров $У_0$ не представляет интереса и поэтому в дальнейшем не будут рассматриваться.

Содержание системы управления ТС СЗ должно сводится к анализу влеяния множества параметров $y_j (j = \overline{1,n})$ (отклонений от заданных значений y_0) на состояние S_i СЗ и введения управляющих воздействий $V_\mu (\mu = \overline{1,k})$ таких, которые переводят состояние S_i СЗ в состояние S_0.

Выводы

Таким образом, первая задача построения модели управления ТС СЗ заключается в определении связей вида:

$$S_1 = S_1(y_1, y_2, \dots, y_n; V_1, V_2, \dots, V_k);$$
$$S_2 = S_2(y_1, y_2, \dots, y_n; V_1, V_2, \dots, V_k);$$
$$\dots \quad \dots \quad \dots \quad \dots \quad \dots$$
$$S_m = S_m(y_1, y_2, \dots, y_n; V_1, V_2, \dots, V_k).$$

На появление состояний S_i СЗ, очевидно, должны быть положены некоторые ограничения:

$$\theta_1 >_< q_1(S_1, \dots, S_m);$$

$$\theta_p >< q_p(S_1, \dots, S_j, \dots, S_m);$$
$$\theta_m >< q_m(S_1, \dots, S_j, \dots, S_m);$$

Введем весовые оценки C_μ управляющих воздействий V_μ. Тогда можно определить функцию управления состояниями СЗ:

$$\Phi >< f\left(y_1, y_2, \dots, y_j, \dots, y_n; V_{1v}, \dots, V_{1\mu}, \dots, V_k; C_1, \dots, C_\mu, \dots, C_k\right).$$

Если функция управления состоянием сводится к минимизации (максимизации) ее значения, то она становится целевой функцией.

Так как СЗ является элементом СЗИ и управление ее ТС направлено на обеспечение требуемого уровня защищенности, которая определяется вероятностью появления особых ситуаций эксплуатации, та в качестве нормированных значений θ_p будем рассматривать вероятности появления S_i состояний системы, вызывающих появление R_i особых ситуаций эксплуатации, а каждому значению функционального параметра $У_j$ вероятность его появления P_{yi}.

Среди управляющих воздействий, определяющих ТС СЗ, можно выделить три наиболее важных, обеспечивающих не появление S_i состояний системы: резервирование элементов системы; замены элементы системы; контроль состояний системы. Первый способ управляющих воздействий применяется на этапе проектирования, а так как в статье исследуется управление ТС СЗ на этапе эксплуатации СЗИ, то этот способ не рассматривается.

Управляющие воздействия путем замен через время $T_з$ характеризуется там, что уровень безопасной работы элемента системы ограничен некоторой заданной величиной $P_э^*$:

$$P_э^* >< e^{\int_0^{T_з} \lambda(t)dt}$$

В качестве весового коэффициента при этом способе выбираются затраты на замену элемента, включающие его стоимость.

Контроль технического состояния элемента сводится к выбору значения вероятности $P_н$ (определить работоспособное состояние элемента при эксплуатации) при условии, что контроль состояния проводится через временной интервал t_k с характеристиками достоверности контроля α и β (ощибки I и II рода).

В качестве весового коэффициента в этом случае выбираются затраты на контроль и замены элементов, если они неисправны.

Таким образом, функцию управления ТС СЗ в процессе эксплуатации можно определить нам целевую функцию минимизации затрат на выполнения замен и контроля состояний элементов СЗ в процессе эксплуатации СЗИ.

При этом должны выполнятся ограничения (2), накладываемые на вероятности появления S_i состояния СЗ.

В соответствии с [1] уравнения типа (1) являются уравнениями функционально-надежных состояний.

Литература

1. Гурина С.А. – Создание информационных моделей системы управления защитой объектов/ Гурина С.А., Егоров Ф.И., Хорошко В.А. // Вісник ДУІКТ, т.6, №2, 2008. – с.147-153.

2. Козакова Н.Ф. - Повышение адаптивности и достоверности вероятностной модели оценки живучести систем защиты информации / Козомова Н.Ф., Тискина Е.О., Хорошко В.А.// Інформаційна безпека, №2, 2009. – с.69-73.

3. Дмитренко А.П. – Статистическое моделирование для оценки защищенности локальной сети / Дмитренко А.П., Сирченко Г.А., Хорошко В.А. // Вісник ДУІКТ, т.8, №1, 2010. – с.62-67.

Рецензент:д.т.н., проф.Дудикевич В.Б.
Надійшла 24.11.2010