ЗАХИСТ ІНФОРМАЦІЇ

УДК 621.3:004.056

Е.В. Иванченко,
В.А. Хорошко,
Ю.Е. Хохлачева

ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются задачи и стратегия технического обслуживания систем обеспечения информационной безопасности. Определены оценки и показатели технического состояния и особенности функционирования системы, а также определены эксплуатационно-технические показатели исследуемой системы.

Ключевые слова: *стратегия обслуживания, система обеспечения информационной безопасности, методика, модель, граф.*

Розглядаються завдання і стратегія технічного обслуговування систем забезпечення інформаційної безпеки. Визначено оцінки і показники технічного стану та особливості функціонування системи, а також визначені експлуатаційно-технічні показники досліджуваної системи.

Ключові слова: *стратегія обслуговування, система забезпечення інформаційної безпеки, методика, модель, граф.*

The problems and maintenance strategy of information security systems are considered. Several estimations and indicators of the technical condition and features of the functioning of the system are defined; operational and technical characteristics of the studied system are identified.

Keywords: *maintenance service strategy, information security support system, method, model, graph.*

Введение

Основной задачей технического обслуживания (ТО) систем обеспечения информационной безопасности (СИБ) является поддержание исправности системы при использовании их по назначению, а также при их хранении. Решение задач ТО СИБ определяется выбором соответствующей системы ТО как совокупности технических и программных средств, а также обслуживающего персонала, взаимодействующих с системой по правилам, установленным нормативной (НТД) и эксплуатационной технической (ЭТ) документацией [1].

В системе ТО СИБ в настоящее время используют специальные понятия стратегий, видов и методов ТО [2].

Стратегия обслуживания представляет собой систему правил управления техническим состоянием (ТС) системы в процессе его ТО. Различают:

1) стратегию ТО по наработке, предусматривающие выполнение определенных видов и операций обслуживания, перечень и периодичность выполнения которых определяется наработкой системы с начала эксплуатации или после ремонта;

2) стратегию ТО по состоянию с контролем параметров (ТОКП) или уровнем надежности (ТОУН), или совокупности правил, предусматривающих выполнение определенных работ, объем и периодичность которых для выделенного множества подсистем назначаются по результатам их технического диагностирования (ТД), или оценки уровня надежности, т.е. определения фактическим ТС системы и подсистем в момент начала ТО.

Отмеченные стратегии ТО СИБ предусматривают проведение следующих видов технического обслуживания:

а) ТО с непрерывным (ТОНК) и периодическим (ТОПК) контролем;

б) оперативное ТО (ОТО);

в) периодическое ТО (ПТО);

г) регламентное ТО (РТО);

д) специальное ТО, выполняемое по требованию или при особой необходимости.

Структура ТО и контроля СИБ предусматривает планово-предупредительный характер работ. В этом случае планируемыми являются:

а) объем регламентированных работ и интервалы наработки аппаратуры независимо от ее фактического ТС;

б) объем и периодичность проведения контролбных или диагностических операций на аппаратуре.

Внедрение в СИБ современной аппаратуры предусматривает ТО по состоянию с контролем параметров [2, 3]:

1) выбор совокупности контролируемых параметров (признаков), определяющих ТС системы в целом или подсистем;

2) оценку важности выбранных контролируемых параметров или признаков и их описание в виде номинальных, и упреждающих значений, набора соответствующих тестов и т.п.;

3) обоснование периодичности и объема проводимых контрольных и диагностических операций;

4) классификацию технических состояний СИБ путем представления различных уровней работоспособности и неисправности систем;

5) разработка регламентов ТО и ТД, алгоритмов технической диагностики и поиска неисправностей.

Основная часть

Повышение эффективности и качества функционирования СИБ требуют системного подхода при оценке их технического состояния, который предусматривает разбиение процессов функционирования и технического обслуживания системы на элементарные технологические операции, находящиеся в определенной иерархической взаимосвязи. Проведение той или иной операции связано с изменением ТС СИБ под воздействием внутренних или внешних дестабилизирующих факторов или управляющих воздействий обслуживающего персонала, пользователей или злоумышленников.

Исследование процессов функционирования и технического обслуживания СИБ связано с уровнем ее детализации, что определяется реальными требованиями к выполнению отдельных операций на соответствующих иерархических уровнях исследуемой системы.

Оценка ТС исследуемых систем производится на основании анализа эксплуатационно-технических характеристик этих систем. Различают следующие уровни ТС:

а) неработоспособное;

б) неисправное.

В ряде случаев оговаривается понятие неисправного состояния СИБ, при котором система удовлетворяет всем основным требованиям сохранения работоспособности и вспомогательным требованиям, установленным НТД.

Рассмотрим возможный перечень элементарных технологических операций, совершаемых при переводе СИБ на уровне системы из одного класса состояний в другой. Граф взаимосвязи этих состояний представлен на рис. 1.

Подготовка СИБ к использованию по назначению ($S_1^Г$) предусматривает включение, выключение, проверку правильности функционирования, установку и регулировку режимов работы, калибровку, измерение и регулировку параметров и характеристик, введение данных. Нахождение системы в состоянии готовности определяется принятой стратегией ТО и контроля надежности СИБ, наличием технического ресурса и резерва, совершенством организационной структуры и программного обеспечения. Готовность системы определяется также подготовкой подсистем, формированием очереди обслуживания, присвоением приоритета, ожиданием использования и т.п.

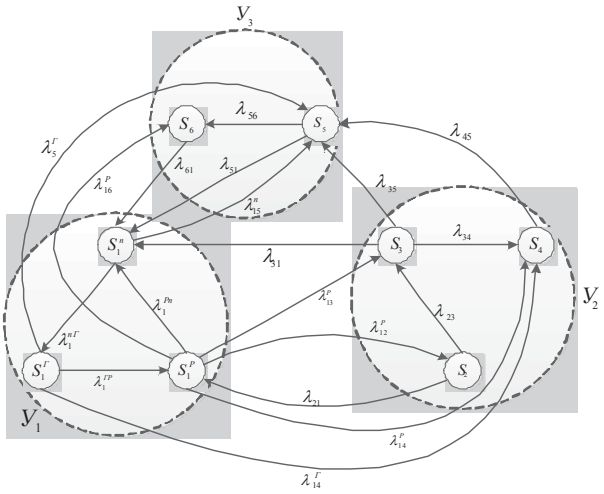

Рис. 1. Граф дискретных состояний СИБ

Режим функционирования СИБ S_1^P (использование по назначению) предусматривает: проведение работ, связанных с проверкой работоспособности подсистем и системы путем непрерывного контроля ее ТС; предотвращение отказов, неисправностей или сбоев; постройку и регулировку. Обычно при ТО СИБ с контролем параметров используются эксплуатационные допуски на контролируемые параметры двух видов – номинальные и упреждающие.

Профилактическому регулированию S_2 подвергается та часть параметров, которая в процессе функционирования системы вышла за границы упреждающих ресурсов.

Оценка работоспособности СИБ в общем случае сводится к задаче распознавания уровней ее ТС по совокупности контролируемых параметров или признаков. Нахождение системы в состояниях отказа S_4 или неисправности S_3 требует проведения восстановительных операций S_5: текущего, среднего ремонта, предупредительных замен и т.п. Переключение системы в резервное состояние S_6 иногда производится при проведении трудоемких ТО, а также после восстановительных мероприятий, проводимых вследствие появления отказов или неисправностей.

В общем случае с учетом многообразия случайных законов воздействия и атак на рассматриваемую совокупность ТС справедливо предположение о произвольном распределении длительности переходов системы в одно из анализируемых состояний.

При этом целесообразно рассмотреть следующие условия функционирования рассматриваемой модели.

В общем случае моменты возможных переходов системы из одного состояния в другое имеет случайный характер. Время пребывания системы в определенном состоянии S_i является непрерывной величиной, равной обратной величине суммарной интенсивности выходов СИБ из этого состояния, т.е.

$$T_i = \frac{1}{\sum\limits_{i=j} \lambda_{ij}}, \text{ или } T_1^{\Gamma} = \frac{1}{\lambda_1^{\Gamma P} + \lambda_{14}^{\Gamma} + \lambda_{15}^{\Gamma}}.$$

Время подготовки СИБ к использованию по назначению T_H и время восстановления T_B обычно подчиняются показательным законам распределения [6] с соответствующими функциями плотности

$$f(t_n) = \lambda_1^{n\Gamma} \exp(-\lambda_1^{n\Gamma} t_H);$$
$$f(t_H) = \mu \exp(-\mu t_n),$$

где $\lambda_1^{n\Gamma}$ – интенсивность операций подготовки СИБ; $\mu = (T_B \_)^{-1} = (\lambda_{51} + \lambda_{56})$ – параметр потока операций восстановления системы. При этом для рассматриваемой модели среднее время пребывания СИБ в состоянии восстановления определяется как математическое ожидание случайной величины:

$$T_B = \int_0^{\infty} t_B dF_5(t_B) = \int_0^{\infty} t_B d\left[1 - \nu_{51} e^{-\lambda_{51} t_B} - \nu_{56} e^{-\lambda_{56} t_B}\right], \qquad (1)$$

где $F_5(t_B)$ – функция распределения времени пребывания СИБ в состоянии восстановления; ν_{51}, ν_{56} – весовые коэффициенты восстановления системы при переводе ее в состояния $S_1(S_1^{\Gamma}, S_1^{n}, S_1^{B})$ или S_6.

При отказе подсистемы СИБ восстановление работоспособности системы осуществляется автоматическим подключением резервного комплекта за время

распределенное, например, по нормальному закону [5]. Аналогичным законом распределения описывается длительность обслуживания СИБ с ожиданием, что характерно при замене элементов подсистем, выработавших свой ресурс.

Предполагается, что длительность восстановления СИБ T_{51} при переходе ее в состояние S_1 без учета времени ожидания, осуществляемого одним специалистом обслуживающего персонала, распределяется по логарифмически нормальному закону вида:

$$T_{51} = \exp\left\{\frac{1}{M}\left[a_{ЛН} + a_{ЛН}\left(\sum_{i=1}^{12}\varphi_i - 6\right)\right]\right\}, \qquad (2)$$

где M – математическое ожидание, для десятичного и натурального логарифмов соответственно M=0,434 и M=1,0; $a_{ЛН}$ – параметры логарифмически нормального закона:

$$a_{ЛН} = \ln m_{51} - 0{,}5\sigma^2_{ЛН}; \sigma^2_{ЛН} = \ln\left[\sigma^2_{51}e^{-2\ln m_{51}} + 1\right], \qquad (3)$$

φ – случайное число, равномерно распределенное в интервале (0,1); m_{51}, σ_{51} – соответственно математическое ожидание и среднеквадратическое отклонение времени восстановления системы.

Остальные параметры процесса функционирования рассматриваемой модели имеют следующие особенности [2, 3, 6]:

– начало рабочего режима функционирования должно происходить в определенный момент времени, который задается, так как в противном случае СИБ переводится в состояние ожидания, отказа или восстановления;

– операции управления оперативной готовностью и своевременным использованием системы по назначению могут быть описаны в общем случае простейшим потоком событий;

– моменты появления неисправностей и отказов, в том числе и профилактируемых S_2, подчиняются распределению Пуассона;

λ_{12} – интенсивность переходов системы из ТС одного класса в ТС другого класса; λ^P_{12} – интенсивность постепенных отказов, связанных с переходом при определении величин контролируемых параметров к эксплуатационным упреждающим допускам; λ_{23} – интенсивность постепенных отказов, приводящих СИБ в состояние неисправности, классифицируемой НТД; λ_{21} – такого типа неисправности являются неустранимыми при проведении профилактических работ; λ^P_{13} – интенсивность постепенных отказов тех параметров, упреждающие допуски, на которые не назначаются; λ^P_{14}, $\lambda^Г_{14}$ – интенсивности внезапных отказов, классифицируемых НТД; λ_{34} – интенсивность постепенных неклассифицируемых отказов системы, приводящих к отказам, классифицируемых НТД; λ^P_{16} – частота проведения трудоемких видов ТО системы; λ_{21} – интенсивность проведения настроечных и регулировочных операций, обеспечивающих вывод контролируемых параметров из зоны эксплуатационных упреждающих допусков; λ_{61} – интенсивность выполнения технологических операций регламентированного ТО [7].

Рассмотренная система функционирования элементов полумарковской модели СИБ S_1–S_6 разработана для одного комплекта системы в стационарном режиме. Однако на практике имеют место особенности резервирования основного комплекта СИБ (горячий или холодный резерв), контроля работоспособности и восстановления системы, которая является сложной системой, динамики функционирования. В этом случае возможно построение разнообразных марковских и полумарковских моделей надежности таких систем [1, 4, 5]. Выбор модели того или иного вида определяется законами распределения моментов вхождения системы в определенные технические состояния и случайных величин длительностей пребывания системы в этих состояниях. На выбор модели надежности накладываются определенные ограничения [6] и постановка задачи исследования.

Проанализируем надежность и работоспособность СИБ как системы, состоящей из двух идентичных комплектов (рис. 2), один из которых является рабочим, а другой – горячим резервом S_0.

Предусматривается регламентированное ТО обоих компонентов S_3 и обслуживание системы по уровню ее надежности при отказе одного из компонентов S_3. Возможны на практике другие технические состояния СИБ, которые характеризуются отказом одного из комплектов системы S_1, его восстановлением, когда другой комплект находится в рабочем режиме или состоянии ожидания восстановления S_5.

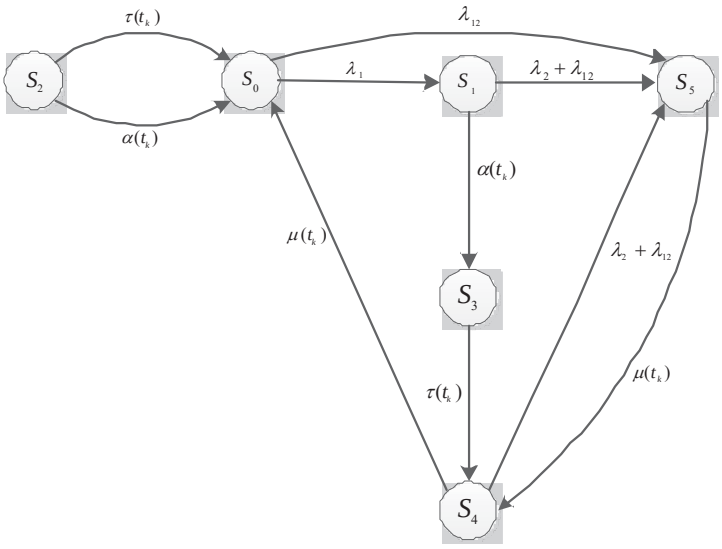

Рис. 2. Обобщенный граф технического состояния СИБ с горячим резервом

Рассмотрим возможность оптимизации периодичностей проведения регламентированного ТО и контроля системы t_k, а также ТО по уровню надежности S_3 в период эксплуатации t при условии получения высокой текущей работоспособности и готовности СИБ.

В качестве исходных данных предполагается экспоненциальный закон распределения времени наработки системы на отказ и восстановления при произвольном распределении других случайных величин.

Методика исследования динамики функционирования представленной модели предусматривает использование вероятностей $P_i(t,t_k)$ перехода системы через технические состояния S_i на интервале времени $t_k + \Delta t_k$ в дифференциальных уравнениях следующего вида:

$$\begin{aligned}
&\left[\frac{\partial}{\partial t}+\frac{\partial}{\partial t_k}+\lambda_1+\lambda_{12}+\alpha(t_k)\right]P_0(t,t_k)=0;\\
&\left[\frac{\partial}{\partial t}+\frac{\partial}{\partial t_k}+\lambda_2+\lambda_{12}+\alpha(t_k)\right]P_1(t,t_k)=\lambda_1 P_0(t,t_k);\\
&\left[\frac{\partial}{\partial t}+\frac{\partial}{\partial t_k}+\tau(t_k)\right]P_i(t,t_k)=0;\ i=2,3;\\
&\left[\frac{\partial}{\partial t}+\frac{\partial}{\partial t_k}+\lambda_2+\lambda_{12}+\mu(t_k)\right]P_4(t,t_k)=0;\\
&\left[\frac{\partial}{\partial t}+\frac{\partial}{\partial t_k}+\mu(t_k)\right]P_5(t,t_k)=(\lambda_2+\lambda_{12})P_4(t,t_k),
\end{aligned} \qquad (4)$$

где $\lambda_1, \lambda_2, \lambda_{12}$ – интенсивность отказов первого и второго компонентов СИБ и всей системы в целом; t_1 – случайный интервал времени, отсчитываемый в процессе функционирования системы от момента, когда оба компонента СИБ являются действующими, до момента проведения какого-либо ТО; $\tau(t_k)$, $\mu(t_k)$, $\alpha(t_k)$ – случайные величины интенсивностей обслуживания (продолжительности ТО), восстановления и периодичности ТО, характеризируемые соответственно функциями распределения $F_\tau(t_k), F_\mu(t_k), F_\alpha(t_k)$ и их плотностями

$$f_\tau(t_k), f_\mu(t_k), f_\alpha(t_k); \tau(t_k)=\frac{f_\tau(t_k)}{1-F_\tau(t_k)}; \mu(t_k)=\frac{f_\mu(t_k)}{1-F_\mu(t_k)}; \alpha(t_k)=\frac{f_\alpha(t_k)}{1-F_\alpha(t_k)}.$$

Начальные условия для решения системы уравнений (4) имеют вид:

$$\begin{aligned}
&P_0(0,0)=1;\ P_1(t,0)=0;\\
&P_0(t,0)=\int_0^t \tau(t_k)P_2(t,t_k)dt_k+\int_0^t \mu(t_k)P_4(t,t_k)dt_k;\\
&P_1(t,0)=\int_0^t \alpha(t_k)P_{i-2}(t,t_k)dt_k,\ i=2,3;\\
&P_4(t,0)=\int_0^t \tau(t_k)P_3(t,t_k)dt_k+\int_0^t \mu(t_k)P_5(t,t_k)dt_k;\\
&P_5(t,0)=\lambda_{12}\int_0^t P(t,t_k)+(\lambda_2+\lambda_{12})\int_0^t P_1(t,t_k)dt_k.
\end{aligned} \qquad (5)$$

Очевидно, что система будет работоспособной в состоянии S_0, S_1 и S_4. Следовательно, выражение для определения вероятности текущей работоспособности СИБ может быть записано в следующем виде;

$$P_{раб}(t) = \int_0^t \left[P_0(t,t_k) + P_1(t,t_k) + P_4(t,t_k)\right]dt_k \qquad (6)$$

Используя преобразование Лапласа для систем уравнений (4) и (5), последовательно проведя операции дифференцирования оригинала при условии $\lambda_1 \neq \lambda_2$, получим:

$$\begin{aligned} &P_{раб}(P) = P_0^*(p,0)\{(1-b)(p+\lambda_1')^{-1}\left[1-f_\alpha^*(p+\lambda_1')\right] \\ &+b(p+\lambda_2')\left[1-f_\alpha^*(p+\lambda_2'\right]+\left[1-f_\mu^*(p+\lambda_2')\right]\times\left[f_\tau^*(p)f_{\alpha 1}^*(p)+f_\mu^*(p)f_{\alpha 2}^*(p)\right]\times, \\ &\times(p+\lambda_2')\left[1+f_2^*(p+\lambda_2')-f_\tau^*(p)\right]\}^{-1} \end{aligned} \qquad (7)$$

где:

$$f_{\alpha 1}^*(p) = b\left[f_\alpha^*(p+\lambda_2' - f_\alpha^*(p+\lambda_1')\right];$$

$$b = \frac{\lambda_1}{\lambda_1-\lambda_2}; \lambda_1' = \lambda_i + \lambda_{12}\,(i=1,2);$$

$$f_{\alpha 2}^*(p) = b\lambda_2'(p+\lambda_2')^{-1}\left[1-f_\alpha^*(p+\lambda_2'\right]+(1-b)\lambda_1'(p+\lambda_1')^{-1}\left[1-f_\alpha^*(p+\lambda_1')\right].$$

Проведя преобразования выражения (7), можно получить выражения для $P_{раб}(p)$ при устойчивом состоянии работоспособности СИБ $(t \to \infty)$ и оптимальном периоде обслуживания систему $[F_\alpha(t_k) = 0$ *для* $t_k < T$ *и* $F_\alpha(t_k) = 1$ *для* $t_k > T]$ при заданных изменениях таких характеристик исследуемой модели, как μ и τ.

Выводы

На основании проведения исследований можно сделать вывод, что рассмотренные характеристики трудоемких ТО полумарковской модели функционирования и обслуживания СИБ позволяют определить эксплуатационно-технические показатели исследуемой системы и, следовательно, проанализировать периодичность и продолжительность проведения различных технологичных операций управления и обслуживания.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основи недійсності інформаційних систем / С.М. Головань, О.В. Корнейко, О.С. Петров, В.О. Хорошко, Л.М. Щербак. – Луганськ : Ноулідж, 2012. – 335 с.

2. *Сірченко Г.А.* Алгоритм визначення показників для оцінки надійності систем спеціального призначення / Г.А. Сірченко, В.О. Хорошко, Ю.Є. Хохлачова // Інформаційна безпека. – 2013. – № 1(9). – С. 142–147.

3. *Бриль В.М.* Требования к автоматизированым средствам контроля технического состояния систем защиты информации / В.М. Бриль, Е.В. Иванченко, В.А. Хорошко // Інформаційна безпека. – 2013. – № 2(10). – С. 19–25.

4. *Розенберг В.Я.* Что такое теория массового обслуживания / В.Я. Розенберг, А.И. Прохоров. – М. : Сов. радио, 1962. – 254 с.

5. *Анисимов В.В.* Элементы массового обслуживания и ассимптотического анализа систем / В.В. Анисимов, О.К. Закусило, В.С. Донченко. – К. : Вища школа, 1987. – 248 с.

6. Модель и метод оценки эффективности организации процесса функционирования систем воздушного движения / Е.В. Иванченко, А.Н. Орехов, Е.П. Сластенко, В.А. Хорошко // Сучасний захист інформації. – 2013. Спецвипуск. – С. 73–81.

7. *Андреев В.И.* Количественная оценка защищенности технических объектов с учетом их функционирования / В.И. Андреев, В.С. Козлов, В.А. Хорошко // Захист інформації. – 2004. – № 2. – С. 47–51.

Отримано 15.12.2014

Рецензент Рибальський О.В., доктор технічних наук, професор.