Полученные с помощью (5–8) безусловные вероятности нахождения системы угроз на любом (*k*-м) шаге состояния способствуют построению в ИТКС ВН достаточно адекватной и высокоэффективной системы защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Документы ФСТЭК РФ. «Информационная безопасность и защита информации». Сборник терминов и определений.
2. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001.
3. *Норткатт С., Новак Д.* Обнаружение вторжений в сеть. –М.: Изд-во «ЛОРИ», 2001.
4. *Скудис Э.* Противостояние хакерам. Полное руководство по компьютерным атакам и эффективной защите: Пер. с англ. – М.: ДМК Пресс, 2003. – 502 с.
5. *Венцель Е.С., Овчаров Л.А.* Теория случайных процессов и ее инженерные приложения. – М.: Наука. 1991.

УДК 621.33

А.Б. Клевцова, Г.С. Клевцов

МОДЕЛИ ПАРАМЕТРИЧЕСКОЙ ЭКСПРЕСС-ОЦЕНКИ СОСТОЯНИЯ ТЕХНИЧЕСКОГО ОБЪЕКТА

Оценка состояния сложного технического объекта является одной из важных задач мониторинга. Эта задача базируется на изучении поведения технического объекта, математические модели которого в общем случае описываются интегро-дифференциальными уравнениями [1]. Для предварительной оценки состояния предпочтительнее использование упрощенных моделей технического объекта, построенных на основе приближенных функциональных зависимостей между переменными объекта. Часто экспресс-оценка является достаточной для прогнозирования и предотвращения нештатных и аварийных ситуаций. Дополнительным преимуществом такого подхода служит возможность осуществления оценки на нижних уровнях распределенной микрокомпьютерной системы мониторинга, где выполнение сложных вычислений в реальном масштабе времени затруднительно или нереализуемо.

В настоящей статье рассматриваются особенности различных моделей параметрической экспресс-оценки состояния технического объекта.

Модель рейтинговой оценки строится на основе структурной декомпозиции объекта на составляющие компоненты [2]. Набор компонентов определяется в результате декомпозиции объекта на значимые функционально законченные единицы. Для каждого компонента назначается ряд критериев, позволяющих полностью охарактеризовать данный компонент. Общая совокупность критериев всех компонентов используется для построения единого критерия для рейтинговой оценки объекта управления.

Для нахождения рейтинговой оценки объекта можно воспользоваться следующей формулой:

$$R = \sum_{i=1}^{N} (Vp_i * \sum_{j=1}^{P} (K_j * Vk_j)),$$

где R – рейтинг; $i=1,2,...,N$ – вектор компонентов; Vp_i – весовой коэффициент i-го компонента; $j=1,2,...,P$ – вектор критериев в компоненте; K_j – числовое значение j-го критерия; Vk_j – весовой коэффициент j-го критерия.

Необходимость ввода весовых коэффициентов компонента и весовых коэффициентов критериев вызвана тем, что как критерии в одном компоненте, так и

компоненты между собой различаются по приоритету и по придаваемой им значимости пользователем при оценке рейтинга.

Модель рейтинговой оценки проста, однако реализация может вызвать затруднения в связи с необходимостью определения исходных весовых коэффициентов с помощью экспертов.

При использовании модели, в основе которой лежат процедуры формировании логических выражений, определяющих критерии оценки состояния, объект, как правило, представляется в виде древовидной структуры [3]. Если условно назвать уровни иерархии структуры: объект, субобъект, компонент, то состояние объекта определяется состоянием субобъектов, которые оцениваются состоянием их компонентов, состояние которых в свою очередь определяется переменными состояния, описывающими эти компоненты.

Для формирования алгоритма интегральной оценки состояния объекта введем следующие обозначения: P_{ijk} – *k*-переменная состояния *j*-компонента *i*-субобъекта; *Qij* – *j*-компонент i-субобъекта; *KR* – коэффициент критичности переменной состояния; $KR_{P_{ijk}}$ – коэффициент критичности *k*-переменной состояния *j*-компонента *i*-субобъекта; $S_{P_{ijk}}$ – качественная оценка *k*-переменной состояния *j*-компонента *i*-субобъекта; $S_{Q_{ij}}$ – качественная оценка состояния *j*-компонента *i*-субобъекта.

Коэффициент критичности переменной состояния может принимать следующие значения: 11 – критичная переменная состояния – наиболее важная переменная, по состоянию которой однозначно определяется состояние компонента; 01 – некритичная переменная состояния – переменная, состояние которой в совокупности с другими переменными определяет состояние компонента; 00 – информационная переменная состояния – переменная, влияющая на состояние объекта косвенным образом. Любое значение такой переменной не может привести к аварийной ситуации.

Степень критичности той или иной переменной состояния определяет важность и серьезность действий по ее нормализации в случае выхода значения за пределы нормы.

Введем три градации для оценки переменной состояния, компонентов, субобъектов, объектов: 00 – нормальное; 01 – опасное; 11 – аварийное.

Тогда правила определения состояния компонентов объекта, считая, что переменные состояния на данный момент уже оценены, могут выглядеть следующим образом:

– значение “аварийное” критичной переменной состояния определяет состояние компонента как “аварийное” независимо от значений некритичных и информационных переменных состояния:

$$((KR_{P_{ijk}}=11)\&(S_{P_{ijk}}=11))\rightarrow S_{Q_{ij}}=11;$$

– если значение критичной переменной состояния “нормальное”, то состояние компонента определяется совокупностью значений состояний некритичных и информационных переменных состояния:

а) значение “аварийное” одной некритичной переменной состояния определяет состояние компонента как “опасное”, независимо от состояний информационных переменных состояния:

$$((KR_{P_{ijk}}=11)\&(S_{P_{ijk}}=00)\&(\forall\ KR_{P_{ijm}}=01)\&(S_{P_{ijm}}=11))\rightarrow S_{Q_{ij}}=01,$$

где m – любое из набора кроме k;

б) одновременная фиксация значений “аварийное” для двух и более некритичных переменных состояния может определять состояние компонента как “аварийное”, независимо от состояний информационных переменных состояния:

$$((KR_{P_{ijk}}=11)\&(S_{P_{ijk}}=00)\ \&\forall\ (((KR_{P_{ijm}}=01)\ \&\ (KR_{P_{ijn}}=01))\ \&$$
$$((S_{P_{ijm}}=11)\ \&\ (S_{P_{ijn}}=11)))\rightarrow S_{Q_{ij}}=11;$$

в) фиксация значения “опасное” для одной и более некритичных переменных состояния определяет состояние компонента как “опасное”, независимо от состояний информативных переменных состояния:

$$((KR_{P_{ijk}}=11)\&(S_{P_{ijk}}=00)\ \&(KR_{P_{ijm}}=01)\ \&(S_{P_{ijm}}=01))\rightarrow S_{Q_{ij}}=01;$$

– если значение критичной переменной состояния “опасное”, то состояние компонента доопределяется состоянием некритичных переменных состояния:

а) если значение некритичных переменных состояния “нормальное” или “опасное” (любого количества), то состояние компонента определяется как опасное:

$$((KR_{P_{ijk}}=11)\&(S_{P_{ijk}}=01)\ \&(\forall\ (KR_{P_{ijk}}=01)\ \&\ (S_{P_{ijk}}=00)\vee\ (S_{P_{ijk}}=01)))\rightarrow$$
$$S_{Q_{ij}}=01;$$

б) если значение одной или нескольких некритичных переменных “аварийное”, то состояние компонента может определяться как “аварийное”:

$$((KR_{P_{ijk}}=11)\&(S_{P_{ijk}}=01)\ \&(\forall\ (KR_{P_{ijk}}=01)\ \&\ (S_{P_{ijk}}=11)\rightarrow S_{Q_{ij}}=11;$$

– если значения критичных и некритичных переменных состояния “нормальное”, то состояние компонента определяется информационными переменными состояния:

$$((KR_{P_{ijk}}=11)\&\ (KR_{P_{ijk}}=01)\ \&\ (S_{P_{ijk}}=00)\ \&(\forall\ ((KR_{P_{ijk}}=00)$$
$$\&\ (S_{P_{ijk}}=11)\vee\ (S_{P_{ijk}}=10))\rightarrow S_{Q_{ij}}=01.$$

Все остальные сочетания значений всех переменных состояния определяют состояние компонента как “нормальное”. Оценив компоненты объекта можно, используя этот же метод перейти к следующему уровню – к оценке субобъектов, а затем к оценке и самого объекта.

При использовании модели, учитывающей критичность параметров объекта, каждому параметру объекта, с учетом иерархической структуры технического объекта и объекта, как составной его части, на этапе настройки системы экспертом присваиваются свойства критичности, значимости и реализации, определяются их значения [4].

Качественная оценка состояния объекта осуществляется в следующем порядке:

1 стадия: оценка состояния параметров объекта с учетом дискриминирующего признака, которым является одно из свойств;

2 стадия: качественная оценка состояния объекта на текущий момент времени без учета дискриминирующего признака;

3 стадия: уточнение оценки состояния объекта.

Полученные оценки состояния объектов являются исходной информацией для оценки состояния системы и любых ее частей.

Представленный формализованный алгоритм позволяет осуществить реалистичную, понятную и эффективную интегральную параметрическую качественную оценку как текущего, так и прогнозного состояния технического объекта.

Построение графоаналитической модели технического объекта для решения задачи упрощенной оценки его состояния позволяет формировать и использовать функциональные и качественные зависимости между переменными на основе обработки экспертных знаний и опытных данных [5].

В основе модели лежит параметрическое представление технического объекта [6]. Имеется технический объект G, характеризуемый переменными $pi \in \{p_i\}_{i=1}^{m}$, где m – количество переменных объекта. Для каждой переменной pi определена область значений: а) область нормальных значений $q_i^н$. Если $pi \in q_i^н$, то переменная pi находится в норме; б) область предупреждения q_i^n. Если pi $\in$ q_i^n, то переменная pi находится в допустимых пределах, однако для предотвращения негативных последствий ее изменения необходимо выполнить исследование состояния объекта и провести анализ возможных изменений его состояния; в) область опасных значений q_i^o. Если $p_i \in q_i^o$, то переменная p_i находится в опасной зоне. В этом случае объект в зависимости от номенклатуры таких p_i и их значений может находиться в опасной зоне; г) область аварийных значений q_i^a. Если существует l, такое, что $p_i \in q_i^a$, то состояние объекта G, в зависимости от номенклатуры и значений остальных переменных p_i может характеризоваться как аварийное или функционально-ограниченное.

Таким образом, вводится следующая градация состояния объекта: нормальное, опасное, функционально-ограниченное и аварийное.

Тогда последовательность проведения текущей и прогнозной оценки состояния технического объекта выглядит следующим образом:

1) на основе определения взаимосвязей переменных объекта формируется его графоаналитическая модель [6]. Функциональные связи формируются на основе упрощения более сложных зависимостей, анализа данных о значениях переменных состояния, например, методом статистического анализа или обработки экспертных знаний;

2) текущая оценка состояния объекта осуществляется на основе анализа значений его переменных;

3) прогнозная оценка состояния объекта проводится путем моделирования в рамках графоаналитической модели объекта [5]. Вводится изменение одной из переменных объекта и фиксируется его возможное состояние.

Оценка состояния объекта может осуществляться с помощью системы правил (четких или нечетких) или с помощью вычисления функционала, зависящего от переменных объекта.

Представленные модели в случае реализации позволяют с помощью простых вычислений проводить упрощенную оценку состояния технического объекта. Ее выполнение возможно на нижних уровнях распределенной микрокомпьютерной системы мониторинга, что важно для оперативного мониторинга объекта в реальном масштабе времени.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Васильев В.В.* Современные проблемы компьютерного мониторинга в энергетике // Известия ТРТУ. – Таганрог: Изд-во ТРТУ, 2001.– № 3. – С.99–120.
2. *Клевцов С.И., Клевцова А.Б.* Модель качественной экспресс-оценки управляемого объекта // Материалы Всероссийской НТК“Компьютерные технологии в инженерной и