УДК 621.391

К.А. ПОЛЬЩИКОВ, Р.М. КАБАКЧЕЙ

Полтавский военный институт связи, Украина

МЕТОДИКА ОБОСНОВАНИЯ ТРЕБОВАНИЙ К ЭКСПЕРТНОЙ СИСТЕМЕ СРЕДСТВ ДИАГНОСТИКИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

Рассматривается математическая модель процесса диагностики и восстановления корпоративной информационной сети, излагается сущность методики обоснования количественных требований к экспертной системе, применяемой в сетевых диагностирующих средствах.

экспертная система, вероятностно-временной граф, дефект, диагностика

Актуальность научно-технической задачи

Корпоративные информационные сети (КИС) сейчас стремительно развиваются. Поэтому поддержание корректного функционирования сетевой инфраструктуры является очень важной задачей и подразумевает постоянный мониторинг и контроль поведения сети. Постоянное усложнение аппаратных и программных компонентов КИС, применение новых сетевых и пользовательских приложений неизменно влечет к появлению в сетях большого количества различных дефектов. При этом часто возникают дефекты, с которыми сетевые администраторы ранее не сталкивались при диагностике сети. Поэтому чтобы значительно сократить убытки компаний от простоев и отказов КИС, требуется постоянная модернизация сетевых диагностирующих средств, направленная на повышение эффективности их работы по локализации дефектов в сети.

Постановка задачи. Дефекты КИС можно условно разделить на две категории: «скрытые» и «явные» [1]. К категории «явных» относятся дефекты, которые сопровождаются какими-либо ошибками на канальном уровне сети и которые можно легко выявить путем анализа статистической информации о сетевом трафике.

Дефекты, относящиеся к категории «скрытых», не сопровождаются какими-либо ошибками на канальном уровне сети. Их можно локализовать только с помощью более детального анализа захваченных сетевых пакетов и декодирования содержащихся в них данных (декодирование сетевых протоколов). Явные дефекты в большинстве случаев легко обнаруживаются и быстро локализуются и поэтому не являются большой проблемой в процессе диагностики КИС. Следует также отметить, что именно скрытые дефекты являются основной проблемой для нормального функционирования сети.

Допустим, что переход сети из исправного состояния в неисправное вызван появлением в ней скрытых и явных дефектов 1-й группы, а появление скрытых и явных дефектов 2-й группы является причиной перехода сети из исправного (работоспособного) состояния в неработоспособное.

Ряд организаций интенсивно занимаются проблемами диагностирования сетей на предмет наличия в них различного рода дефектов и уже достигли в этом значительных успехов. Другие компании занимаются разработкой диагностического оборудования (кабельные тестеры, сканеры, системы управления, анализаторы и др.). Наиболее перспективными с точки зрения локализации различного рода дефектов являются системы управления сетью и анализаторы протоколов. Некоторые из этих средств диагностики оснащаются интеллектуальными экспертными системами (ЭС) [2], которые локализуют дефекты в

сети, выдают рекомендации о том, как их устранить, а также могут пояснять пользователю, что означают те или иные результаты измерений. Благодаря этому значительно повышается эффективность диагностики и управления корпоративными информационными сетями. Экспертные системы постоянно совершенствуются. Сегодня актуальны исследования, направленные на создание гибридных интеллектуальных систем [3].

ЭС должна удовлетворять определенным требованиям, при выполнении которых диагностика сети будет эффективной. Эти требования могут быть как качественными, так и количественными. Качественные требования определяются кругом задач, решаемых ЭС. К таким требованиям можно отнести полноту, необходимую глубину и точность анализа, многофакторность учета поведения сети. Неотъемлемым свойством ЭС является возможность ее модификации с целью пополнения базы знаний, совершенствования пользовательского интерфейса и т.п.

К количественным требованиям, предъявляемым к ЭС, можно отнести время и вероятность правильного решения задачи по локализации дефектов КИС. Известны работы, например [4], в которых решается задача обоснования требований к ЭС диагностики сетей передачи информации, но при этом не учитывается наличие в сети дефектов различных групп. Поэтому возникает актуальная задача разработки новой методики обоснования требований к ЭС, применяемых в средствах диагностики КИС. Данная методика должна учитывать специфические особенности КИС, состоящие в том, что в той или иной сети чаще появляются те или иные дефекты.

Предлагаемое решение задачи

Для решения поставленной задачи разработана математическая модель процесса диагностики и восстановления сети. При создании модели использован аппарат вероятностно-временных графов, позволяющий адекватно отражать исследуемый процесс с необходимой детализацией и наглядностью [5].

Граф, моделирующий исследуемый процесс, изображен на рис. 1.

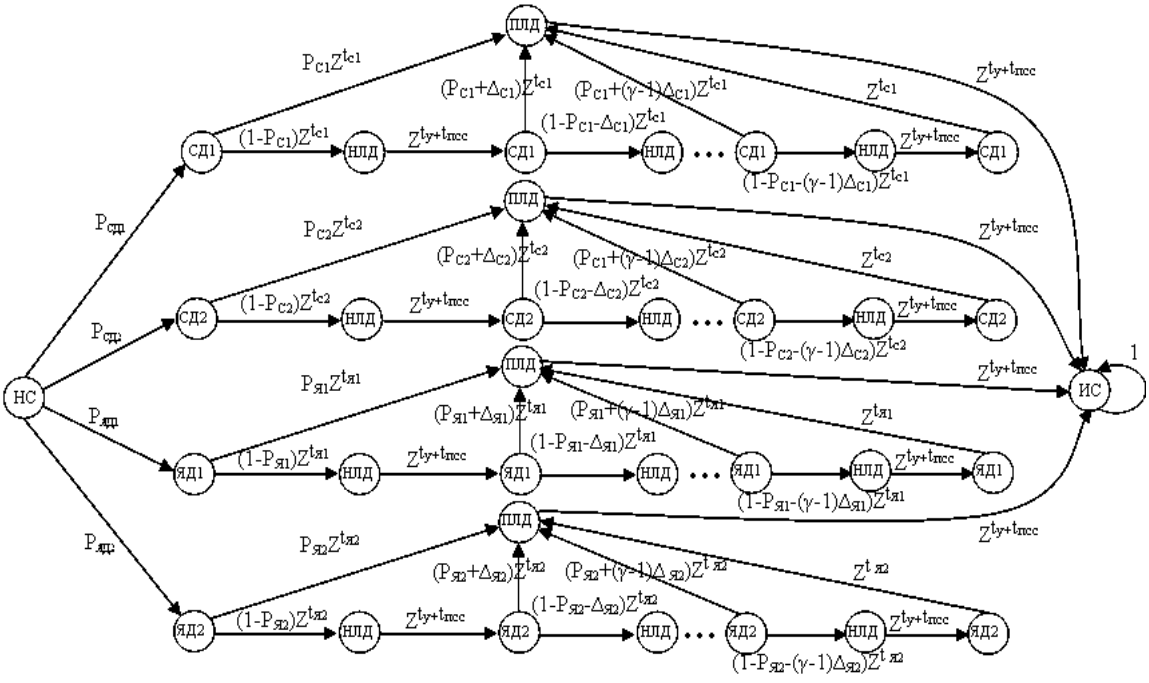

Рис. 1. Граф, моделирующий процесс диагностики и восстановления КИС

Пусть в исходном состоянии сеть является неисправной или неработоспособной, т.е. в ней имеется какой-то дефект. Этому состоянию моделируемого процесса соответствует начальная вершина графа «НС». С вероятностью $P_{СД1}$ в сети возникнет скрытый дефект 1-й группы, с вероятностью $P_{СД2}$ – скрытый дефект 2-й группы, явный дефект 1-й группы будет иметь место с вероятностью $P_{ЯД1}$, а явный дефект 2-й группы – с вероятностью $P_{ЯД2}$. С вероятностью $P_{С1}$ за время $t_{С1}$ скрытый дефект 1-й группы будет правильно локализован. При этом процесс из состояния «СД1» перейдет в состояние «ПЛД». Данный дефект будет локализован не правильно с вероятностью $(1-P_{С1})$ за то же время $t_{С1}$. При этом моделируемый процесс из состояния «СД1» перейдет в состояние «НЛД».

Если дефект локализован правильно, то через время, которое будет затрачено на устранение дефекта t_y и проверку состояния сети $t_{ПСС}$, сеть снова станет исправной. На графе это моделируется дугой, соединяющей вершину «ПЛД» с вершиной «ИС». В случае неправильной локализации скрытого дефекта 1-й группы восстановить исправность сети не удастся. Поэтому по истечению времени $(t_y + t_{ПСС})$ в сети все равно будет иметь место указанный дефект. При этом моделируемый процесс из состояния «НЛД» перейдет в состояние «СД1».

Если первая попытка локализации скрытого дефекта 1-й группы была неудачной, то поиск причины неисправности производится повторно. Ясно, что вероятность правильной локализации дефекта при повторном диагностировании сети увеличится. Величина этого увеличения, если от попытки к попытке вероятность правильной локализации указанного дефекта возрастает по линейному закону, может быть найдена из соотношения:

$$\Delta_{С1} = \frac{1 - P_{С1}}{\gamma - 1}, \qquad (1)$$

где γ – количество предпринятых попыток для правильной локализации дефекта.

Таким образом, со второй попытки скрытый дефект 1-й группы будет правильно локализован с вероятностью $(P_{С1} + \Delta_{С1})$, с третьей попытки – с вероятностью $(P_{С1} + 2\Delta_{С1})$ и т.д. Естественно, вероятность правильной локализации данного дефекта с последней попытки равна 1. Скрытый дефект 1-й группы может быть локализован неправильно со второй попытки с вероятностью $(1 - P_{С1} - \Delta_{С1})$, с третьей попытки – с вероятностью $(1 - P_{С1} - 2\Delta_{С1})$ и т.д. В конце концов, скрытый дефект 1-й группы будет локализован и устранен, т.е. исследуемый процесс перейдет в конечное состояние «ИС».

Аналогично данный процесс протекает, если в сети будет иметь место другой дефект. Это отражено на рассматриваемом графе. При этом введены следующие обозначения: $P_{С2}$, $P_{Я1}$ и $P_{Я2}$ – вероятности правильной локализации скрытого дефекта 2-й группы, явного дефекта 1-й и явного дефекта 2-й группы соответственно; $t_{С2}$, $t_{Я1}$ и $t_{Я2}$ – время локализации скрытого дефекта 2-й группы, явного дефекта 1-й и явного дефекта 2-й группы соответственно; $\Delta_{С2}$, $\Delta_{Я1}$ и $\Delta_{Я2}$ – увеличение вероятности правильной локализации скрытого дефекта 2-й группы, явного дефекта 1-й и явного дефекта 2-й группы соответственно.

Очевидно, что при разных значениях γ граф будет иметь разную структуру. Рассмотрим пример, при котором $\gamma = 3$. В этом случае граф, моделирующий исследуемый процесс, будет иметь следующий вид (рис. 2).

Путем проведения эквивалентных преобразований граф (рис. 2) можно представить в

следующем виде (рис. 3). Дальнейшие преобразования позволяют упростить вероятностно-временной граф до вида, изображенного на рис. 4.

Затем путем окончательных преобразований получим простейший граф (рис. 5).

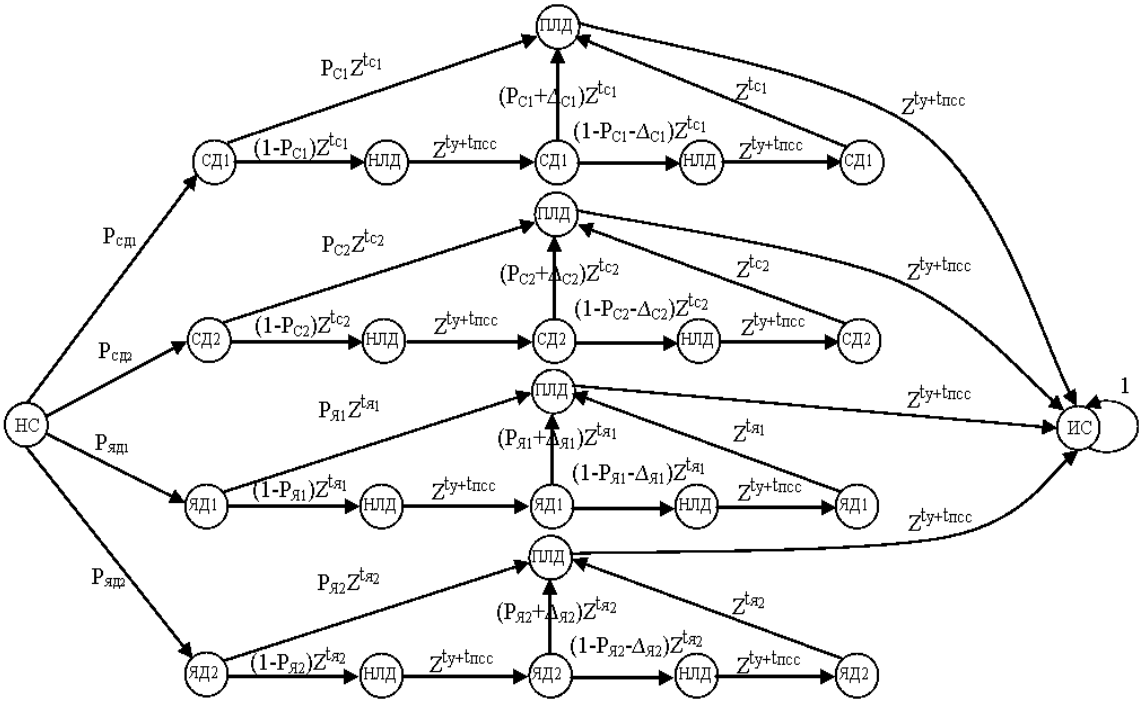

Рис. 2. Граф, моделирующий процесс диагностики и восстановления КИС, построенный для случая, если $\gamma = 3$

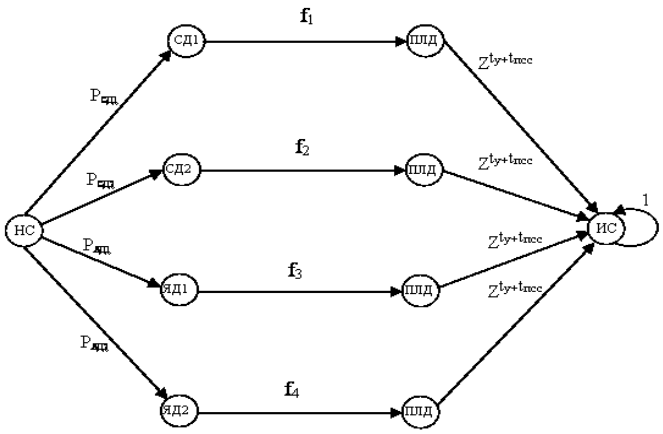

Рис. 3. Граф в преобразованном виде

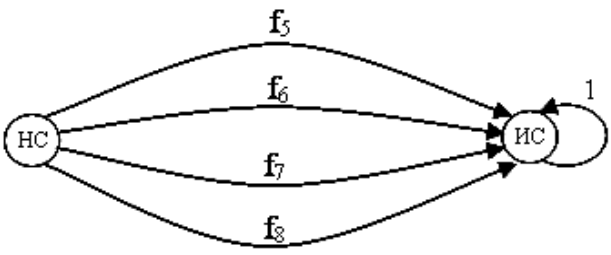

Рис. 4. Граф в преобразованном виде

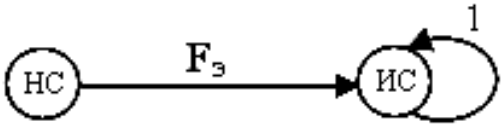

Рис. 5. Простейший вид графа

Функции дуг графов (рис. 3, 4) можно вычислить, используя следующие выражения:

$$f_1(z) = [(1 - P_{C1} - \Delta_{C1}) z^{2t_{C1} + t_y + t_{ПСС}} + (P_{C1} + \Delta_{C1}) z^{t_{C1}}][P_{C1} z^{t_{C1}} + (1 - P_{C1}) \times z^{t_{C1} + t_y + t_{ПСС}}]; \quad (2)$$

$$f_2(z) = [(1 - P_{C2} - \Delta_{C2}) z^{2t_{C2} + t_y + t_{ПСС}} + (P_{C2} + \Delta_{C2}) z^{t_{C2}}][P_{C2} z^{t_{C2}} + (1 - P_{C2}) \times z^{t_{C2} + t_y + t_{ПСС}}]; \quad (3)$$

$$f_3(z) = [(1 - P_{Я1} - \Delta_{Я1}) z^{2t_{Я1} + t_y + t_{ПСС}} + (P_{Я1} + \Delta_{Я1}) z^{t_{Я1}}][P_{Я1} z^{t_{Я1}} + (1 - P_{Я1}) \times z^{t_{Я1} + t_y + t_{ПСС}}]; \quad (4)$$

$$f_4(z) = [(1 - P_{Я2} - \Delta_{Я2}) z^{2t_{Я2} + t_y + t_{ПСС}} + (P_{Я2} + \Delta_{Я2}) z^{t_{Я2}}][P_{Я2} z^{t_{Я2}} + (1 - P_{Я2}) \times z^{t_{Я2} + t_y + t_{ПСС}}]; \quad (5)$$

$$f_5(z) = P_{СД1} \cdot f_1(z) \cdot z^{t_y + t_{ПСС}}; \quad (6)$$

$$f_6(z) = P_{СД2} \cdot f_2(z) \cdot z^{t_y + t_{ПСС}}; \quad (7)$$

$$f_7(z) = P_{ЯД1} \cdot f_3(z) \cdot z^{t_y + t_{ПСС}}; \quad (8)$$

$$f_8(z) = P_{ЯД2} \cdot f_4(z) \cdot z^{t_y + t_{ПСС}}. \quad (9)$$

Производящую функцию $F_Э(z)$ (рис. 5) можно найти по формуле:

$$F_Э(z) = f_5(z) + f_6(z) + f_7(z) + f_8(z). \quad (10)$$

Среднее время, которое уйдет на диагностику и восстановление сети, находится из выражения:

$$T_{ср}(z) = \left. \frac{dF_Э(z)}{dz} \right|_{z=1}. \quad (11)$$

Полученные результаты и их анализ

Для любой корпоративной информационной сети есть возможность задать максимальное значение времени $T_{\max}$, которое можно потратить на диагностику и восстановление сети. Превышение этого значения недопустимо из-за огромных убытков компании или других негативных последствий. Задавшись этим значением, можно предъявить количественные требования к экспертной системе средств диагностики корпоративной информационной сети.

На рис. 6 изображен график зависимости $T_{ср} = f(P_{C1})$.

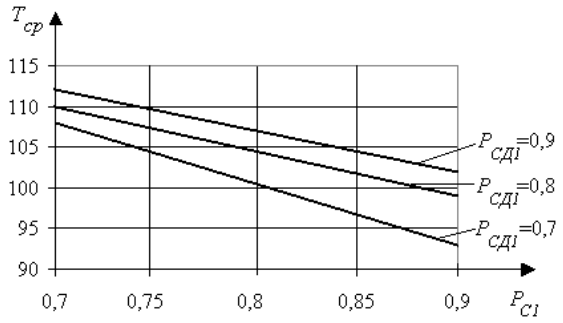

Рис. 6. График зависимости $T_{ср} = f(P_{C1})$

Допустим, для сети задано $T_{\max} = 105$ относительных единиц. Тогда анализ графической зависимости (рис. 7) показывает, что если скрытые дефекты 1-й группы в сети возникают с вероятностью $P_{СД1} = 0{,}7$, то экспертная система должна обеспечить правильность локализации данных дефектов с вероятностью не ниже $P_{C1} = 0{,}74$.

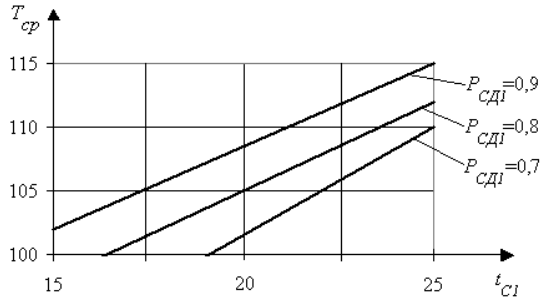

Рис. 7. График зависимости $T_{ср} = f(t_{C1})$

Если вероятность появления данных дефектов в сети равна $P_{СД1} = 0{,}8$, то вероятность их правильной локализации экспертной системой должна быть не ниже $P_{C1} = 0{,}79$. Если же скрытые дефекты 1-й группы в сети возникают с вероятностью $P_{СД1} = 0{,}9$, то экспертная система

должна обеспечить правильность их локализации с вероятностью не ниже $P_{C1} = 0{,}84$.

На рис. 7 изображен график зависимости $T_{ср} = f(t_{C1})$. Его анализ показывает, что при $P_{СД1} = 0{,}7$ время локализации скрытых дефектов 1-й группы не должно превышать $t_{C1} = 24$ относительные единицы.

При $P_{СД1} = 0{,}8$ экспертная система должна обеспечить принятие правильного решения по локализации указанных дефектов за время, не превышающее $t_{C1} = 20$ относительных единиц. Если же скрытые дефекты 1-й группы в сети возникают с вероятностью $P_{СД1} = 0{,}9$, то для принятия решения по их локализации не должно быть отведено времени больше, чем $t_{C1} = 17{,}5$ относительных единиц.

Выводы

Таким образом, методика обоснования требований к экспертной системе, применяемой в средствах диагностики КИС, состоит в последовательном выполнении следующих действий:

1. Для имеющейся КИС определяются значения величин $P_{СД1}$, $P_{СД2}$, $P_{ЯД1}$, $P_{ЯД2}$, t_y, $t_{ПСС}$, а также задается значение $T_{\max}$. При этом во многих случаях целесообразно применять методы математической статистики.

2. С использованием выражений (1) – (11) для различных значений вероятности правильной локализации тех или иных дефектов, времени их локализации, а также количества сделанных при этом попыток принять правильное решение рассчитываются значения среднего времени $T_{ср}$, которое будет потрачено на диагностику и восстановление сети.

3. Проводится анализ полученных результатов, и делаются выводы о том, в каком диапазоне значений должны находиться величины P_{C1}, P_{C2}, $P_{Я1}$, $P_{Я2}$, t_{C1}, t_{C2}, $t_{Я1}$, $t_{Я2}$ и γ, чтобы выполнялось условие $T_{ср} < T_{\max}$.

Литература

1. Юдицкий С.С., Швецов В.И. Увидеть слона целиком. Часть 1 // Сети и системы связи. – 2000. – № 10 (60).

2. Диагностика сетей. – [Электрон. ресурс]. – Режим доступа: http://www.lanit-partner.ru/Company /net_diag.html.

3. Люгер Дж. Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание: Пер с англ. – М.: Издательский дом «Вильямс», 2003. – 864 с.

4. Усачев А.М., Резцов В.Н. Разработка требований к экспертной системе поддержки принятия решения при управлении сетью обмена данными // Искусственный интеллект. – Донецк: Национальная академия наук Украины. Институт проблем искусственного интеллекта. – 2001. – С. 27-34.

5. Невмержицкий И.М., Шаповалов С.В., Польщиков К.А. Методика оценки эффективности протокола транспортного уровня TCP/IP // Радиотехника. – Х.: ХНУРЭ. – 2001. – Вып. 121. – С. 203-205.

Поступила в редакцию 20.02.2006

Рецензент: д-р техн. наук, проф. Н.В. Галай, Полтавский национальный технический университет, Полтава.