УДК 519.711.3:004.021
DOI: 10.25206/1813-8225-2018-162-256-259

Н. Р. СТОРОЖЕНКО
А. И. ГОЛЕВА

Омский государственный
технический университет,
г. Омск

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И АЛГОРИТМ МОНИТОРИНГА ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В целях проведения диагностики и прогнозирования возможных отклонений в работе узлов информационной системы в статье приводится математическое и алгоритмическое описание мониторинга сетевых параметров. Разработанные схема и алгоритм обнаружения неисправностей и прогнозирования отказов сети дают наглядное представление о процессе мониторинга и обнаружения аномалий и необходимы для исполнения программного комплекса системы мониторинга с функциями контроля и диагностики оборудования, а также возможностью прогнозирования и наблюдения за состоянием сети в условиях изменения параметров сетевых устройств.

Ключевые слова: алгоритм мониторинга, корпоративная сеть передачи данных, математическая модель, мониторинг неисправностей, обнаружение аномалий, прогнозирование отказа.

Введение. В настоящее время современные возможности в области информационных технологий внедряются и используются во всех отраслях жизнедеятельности. Повсеместное применение современных средств вычислительной техники делает актуальными задачи обеспечения надежности, защищенности и доступности сетевых ресурсов в современных информационных системах [1]. Такие задачи в условиях интенсивного развития и широкого применения средств информатизации и автоматизации процессов хранения, обработки и передачи информации являются приоритетными и особенно остро нуждаются в решении.

В целях решения данных задач в работах [2–7] авторы исследуют базовые принципы и модели диагностики функционирования сетевых узлов и обнаружения аномалий в работе оборудования. При этом не уделяется должное внимание вопросу прогнозирования возможных отказов в работе устройств информационной системы.

На данный момент на рынке IT-продукции предлагается немало решений для обеспечения контроля и диагностики сетей передачи данных, но, несмотря на их широкое использование, по данным статистики компании Positive Technologies, происходит усложнение организации сетей, увеличение числа применяемых сервисов, это сопровождается ростом числа отказов коммуникационного оборудования. В силу этого применение известных методов и средств оказывается недостаточным, а в ряде случаев неэффективным. Исходя из этого в данной сфере актуальной является задача создания эффективной системы мониторинга с функциями контроля, диагностики, а также прогнозирования отказов.

Обоснование необходимости мониторинга. В связи с активным, нарастающим характером развития информационных технологий происходит рост сложности и масштаба корпоративных информационных систем и сетей, это, в свою очередь, особенно затрудняет и усложняет проведение контроля и прогнозирования возможных отклонений (аномалий) в работе критически важных узлов, включающих устройства связи и сервера корпораций:

— коммутаторы и маршрутизаторы, обеспечивающие передачу сообщений по выделенным каналам, а также хранение таблиц коммутации сети;

— контроллер домена, который обеспечивает централизованное управление рабочими станциями и серверами в сети;

— файловый сервер для хранения и предоставления доступа к общим сетевым папкам и данным;

— почтовый сервер, выполняющий функции отправки, получения и хранения сообщений корпоративной переписки;

— сервер приложений, обеспечивающий хранение информации и управление жизненным циклом производимых изделий;

— сервер для хранения документов финансовой отчетности;

— сервер безопасности для реализации защиты от утечки конфиденциальной информации, разграничения прав доступа к внешним и внутренним ресурсам корпоративной сети, а также для централизованного управления системой антивирусной защиты.

Для таких узлов необходимо обеспечить повышенные требования надежности и защищенности, а также отказоустойчивости для всех легитимных пользователей на всем временном интервале. В силу этого крайне важно непрерывно проводить мониторинг такого оборудования, а также контроль и диагностику обнаружения отказов в целях своевременного выявления аномалий в работе сетевых устройств [8].

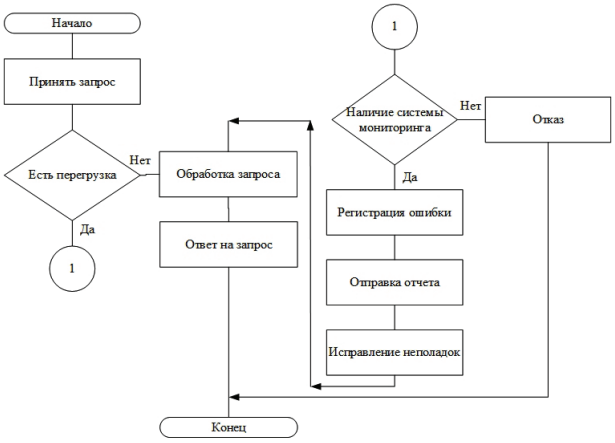

Рис. 1. Схема алгоритма работы сетевых ресурсов

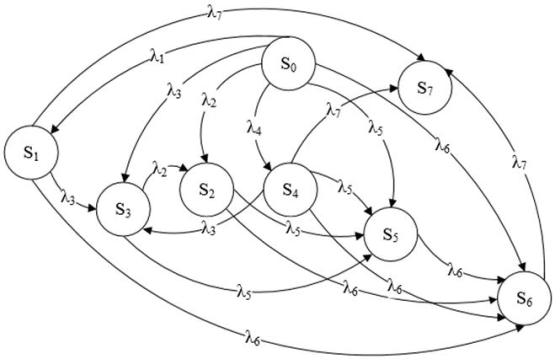

Рис. 2. Граф обнаружения неисправных параметров в процессе мониторинга

Также необходимость применения системы мониторинга в корпоративных системах обработки и передачи данных обусловлена схемой работы сетевых ресурсов (рис. 1), при хранении, обработке и передаче которых требуется обеспечить надежность, безопасность и отказоустойчивость.

Данная схема показывает преимущества применения систем контроля и мониторинга, а также наглядно демонстрирует, что в условиях повышенной нагрузки на сетевые ресурсы при отсутствии системы мониторинга происходят отказы оборудования, в то время как функции системы мониторинга позволяют в режиме реального времени зафиксировать и исправить возникающие неполадки.

Так контроль и мониторинг сетевых неисправностей, обеспечивая автоматизированную проверку оборудования и осуществляя сбор статистики о его работоспособности, позволяет минимизировать отказы оборудования и оптимизировать работу сетевых ресурсов системы [8, 9].

Математическое описание мониторинга сети. Для определения вероятности обнаружения сетевых аномалий, неисправностей и отказов в работе [10] подробно описывается задача моделирования и математического описания процесса мониторинга параметров работоспособности критически важного оборудования в сети. Граф обнаружения неисправных параметров в процессе мониторинга представлен на рис. 2, где S_0, S_1, ..., S_7 — состояния, характеризующиеся отсутствием или наличием неисправностей в работе сетевого оборудования, причем S_0 — состояние, при котором все устройства исправны, а S_7 — отказ всех параметров сети.

В качестве интенсивности переходов (λ_i) в данном случае принимается — интенсивность опроса системой мониторинга i-го параметра в сети.

$$\lambda_i = f(\lambda'_0, priority\,(i)), \qquad (1)$$

где λ'_0 — базовая интенсивность опроса, которая, к примеру, может быть определена как величина, равная 1/30 минут; *priority* (i) — приоритет опроса i-го параметра.

Так как мониторинг, предусматривающий постоянный контроль, представляет собой систему упорядоченного опроса, порядок опроса определяется назначенным приоритетом [4, 10]. Так, интенсивность опроса сетевого параметра тем выше, чем выше его приоритет, назначенный администратором сети.

Математическое описание состояний в ходе мониторинга (рис. 2) представляется в виде системы уравнений (2) [10–12]:

$$\begin{cases} \frac{dp_0}{dt} = -p_0 \cdot (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6), \\ \frac{dp_1}{dt} = p_0 \cdot \lambda_1 - p_1 \cdot (\lambda_3 + \lambda_6 + \lambda_7), \\ \frac{dp_2}{dt} = p_0 \cdot \lambda_2 + p_3 \cdot \lambda_2 - p_2 \cdot (\lambda_5 + \lambda_6), \\ \frac{dp_3}{dt} = p_0 \cdot \lambda_3 + p_1 \cdot \lambda_3 + p_4 \cdot \lambda_3 - p_3 \cdot (\lambda_2 + \lambda_5), \\ \frac{dp_4}{dt} = p_0 \cdot \lambda_4 - p_4 \cdot (\lambda_3 + \lambda_5 + \lambda_6 + \lambda_7), \\ \frac{dp_5}{dt} = p_0 \cdot \lambda_5 + p_2 \cdot \lambda_5 + p_3 \cdot \lambda_5 + p_4 \cdot \lambda_5 - p_5 \cdot \lambda_6, \\ \frac{dp_6}{dt} = p_0 \cdot \lambda_6 + p_1 \cdot \lambda_6 + \\ + p_2 \cdot \lambda_6 + p_4 \cdot \lambda_6 + p_5 \cdot \lambda_6 - p_6 \cdot \lambda_7, \\ \frac{dp_7}{dt} = p_1 \cdot \lambda_7 + p_4 \cdot \lambda_7 + p_6 \cdot \lambda_7. \end{cases} \qquad (2)$$

Решением данной системы уравнений являются значения вероятностей обнаружения сетевых неисправностей, что позволяет оценивать эффективность функций обнаружения системы мониторинга.

Так, решение задачи (2) позволяет отследить динамику диагностирования системой мониторинга неисправных параметров, а также аномалий в работе критически важных узлов корпоративной сети.

Для математического описания функций прогнозирования системы мониторинга при помощи условных вероятностей необходимо учесть, что на состояние полного отказа системы S_n в процессе мониторинга основное влияние оказывают результаты $n-1$ предыдущих испытаний:

$$p(S_1 ... S_n) = p(S_1) \cdot \prod_{j=2}^{n} p(S_j \mid S_1 S_2 .... S_{j-1}). \qquad (3)$$

Данная формула позволяет в процессе мониторинга осуществить прогнозирование полного отказа сети на основе информации о предыдущих состояниях неисправности.

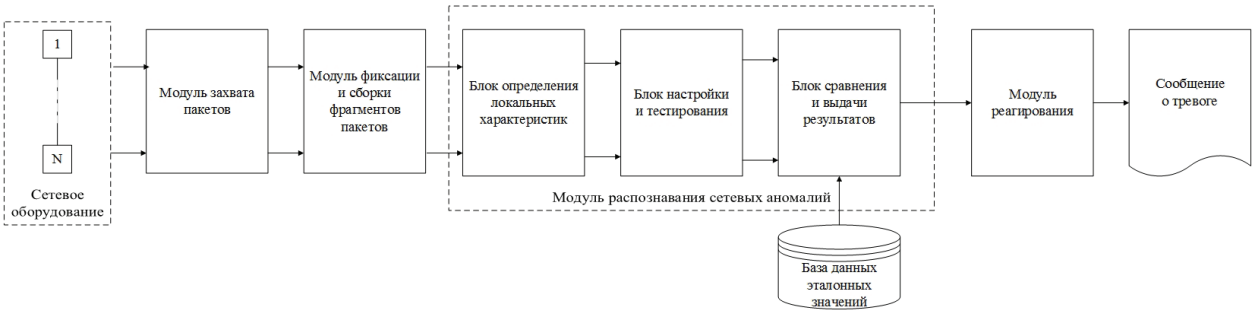

Рис. 3. Схема работы системы мониторинга

Алгоритм мониторинга сетевых неисправностей. В целях реализации данной модели, а также для создания эффективной системы мониторинга, обеспечивающей своевременный поиск и устранение аномалий, в данной работе ставится задача разработки алгоритма сетевого мониторинга для последующей реализации его в виде программного комплекса активной системы мониторинга параметров сети.

Для решения поставленных задач необходимо выделить блоки и модули, реализующие отдельные функции системы мониторинга.

Так, схема работы системы мониторинга в сети с N устройствами представлена на рис. 3.

На вход системы мониторинга в модуль захвата пакетов поступают данные с сетевого оборудования, в частности, информация о работоспособности устройств, а также пакеты, проходящие через них. Далее модуль фиксации отбирает пакеты по заголовкам для дальнейшей передачи их в модуль распознавания аномалий, в блоке определения локальных характеристик происходит сбор информации по контролируемым в ходе мониторинга параметрам сети, в следующем блоке происходит проверка работоспособности, анализ собранных значений и поиск причин отказа, затем происходит сравнение полученных величин с эталонными (взятыми в базе данных эталонных значений) и принятие решения о нормальном функционировании или обнаружения причин замедленной или ненадежной работы сетевого оборудования. Модуль реагирования отвечает за своевременное устранение неисправностей и оповещение администратора об аномальном поведении сетевых устройств.

Таким образом, можно представить процесс мониторинга параметров корпоративной сети в виде схемы алгоритма рис. 4.

На первом шаге алгоритма происходит выбор критически важных узлов и параметров, для которых нужно обеспечить контроль и диагностику надежности и безопасности.

На втором шаге задается набор эталонных значений, которые характеризуются нормальным уровнем функционирования параметров устройств, и формируется база данных для того, чтобы при отклонении от этих значений производилось информирование администратора сети. Далее нужно определить интенсивность опроса сетевых устройств.

На следующем шаге происходит опрос оборудования, анализ полученных пакетов. Затем на этапе сбора параметров определяются характеристики опрашиваемых узлов сети, происходит их накопление и передача в анализатор, где полученные значения сравниваются с эталонными.

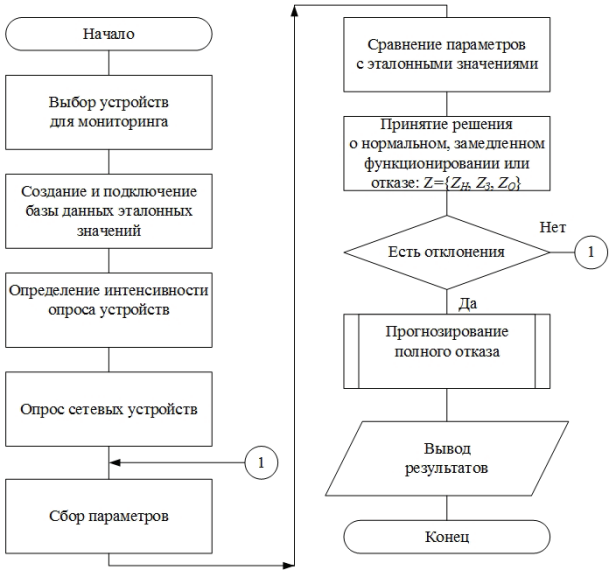

Рис. 4. Схема алгоритма мониторинга

Таким образом, принимается решение о нормальном или замедленном функционировании устройства либо о его отказе. В случае обнаружения аномального поведения в работоспособности оборудования происходит прогнозирование полного отказа сети.

Заключение. Полученное в статье математическое и алгоритмическое описание мониторинга технического состояния информационной системы может быть применено для поиска и прогнозирования неисправностей узлов в корпоративных сетях с множественным доступом и критичными к качеству, надежности и отказоустойчивости сервисами, такими как электронная почта, IP-телефония, видеоконференции. Программная реализация предлагаемой системы позволит создать систему мониторинга, выполняющую, в отличие от существующих, не только диагностику оборудования и наблюдение за состоянием сети в условиях изменения параметров сетевых устройств и своевременное обнаружение аномалий, но и прогнозирование отказов на основании данных о предыдущих неисправностях.

Библиографический список

1. Цвитун А. А., Корнейчук В. И., Долголенко А. Н. Надежность компьютерных сетей. К.: Корнійчук, 2010. 116 с. ISBN 966-7599-67-6.

2. Бычков Е. Д., Батраков С. А. Оценка достоверности функционирования сетевого элемента телекоммуни-

кационной сети // Известия Транссиба. 2013. № 3 (15). С. 114–120.

3. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей / пер. с англ. О. Труфанова. М.: Лори, 2013. 350 с. ISBN 5-85582-350-9.

4. Yolanda S., Georgina G., Mariela C. Evaluation of monitoring tools for cloud computing environments // 2012 XXXVIII Conferencia Latinoamericana En Informatica (CLEI), Oct. 1–5, 2012. Medellin, 2012. DOI: 10.1109/CLEI.2012.6427251.

5. Lee S., Levanti K., Kim H. S. Network monitoring: Present and future // Computer Networks. 2014. Vol. 65. P. 84–98. DOI: 10.1016/j.comnet.2014.03.007.

6. Kufel L. Security Event Monitoring in a Distributed Systems Environment // IEEE Security and Privacy. 2013. Vol. 11, no. 1. P. 36–43. DOI: 10.1515/fcds-2016-0014.

7. Kufel L. Tools for Distributed Systems Monitoring // Foundations of Computing and Decision Sciences. 2016. Vol. 41, Issue 4. P. 237–260. DOI: 10.1515/fcds-2016-0014.

8. Ачилов Р. Построение защищенных корпоративных сетей. М.: Наука и техника, 2013. 250 с. ISBN 978-5-94074-884-7.

9. Стороженко Н. Р., Голева А. И. Анализ и оценка отказоустойчивости сетевых ресурсов // Виртуальное моделирование, прототипирование и промышленный дизайн: материалы IV Междунар. науч.-практ. конф., 15–17 ноября 2017 г. / ТГТУ. Тамбов, 2017. Т. 3, вып. 4. С. 240–244. ISBN 978-5-8265-1839-7.

10. Стороженко Н. Р., Голева А. И. Построение математической модели процесса мониторинга параметров информационной системы // Омский научный вестник. 2018. № 3 (159). С. 133–136. DOI: 10.25206/1813-8225-2018-159-133-136.

11. Боровиков А. А. Вероятностные процессы в теории массового обслуживания. М.: Физматлит, 1972. 368 с.

12. Вентцель Е. С. Исследование операций: задачи, принципы, методология. 6-е изд., стер. М.: Кнорус, 2018. 192 с. ISBN 978-5-4365-1925-8.

СТОРОЖЕНКО Никита Русланович, аспирант кафедры «Информатика и вычислительная техника»; инженер-программист АО «Омский научно-исследовательский институт приборостроения» (АО «ОНИИП»).
Адрес для переписки: snikr@bk.ru
ГОЛЕВА Алина Игоревна, аспирантка кафедры «Информатика и вычислительная техника»; инженер-программист АО «ОНИИП».
Адрес для переписки: frybkf07.93@mail.ru

Для цитирования

Стороженко Н. Р., Голева А. И. Математическая модель и алгоритм мониторинга параметров информационной системы // Омский научный вестник. 2018. № 6 (162). С. 256–259. DOI: 10.25206/1813-8225-2018-162-256-259.

Статья поступила в редакцию 29.10.2018 г.

УДК 004.02
DOI: 10.25206/1813-8225-2018-162-259-264

А. Л. ТКАЧЕНКО
О. Г. ШЕВЕЛЕВА

Омский государственный технический университет, г. Омск

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ ОТДЕЛА ПРОГРАММНЫХ РАЗРАБОТОК ИТ-КОМПАНИИ

В статье рассматривается проблема повышения эффективности деятельности ИТ-компании. В рамках процессного подхода с помощью метода реинжиниринга был построен и проанализирован бизнес-процесс ИТ-компании по выполнению технических заданий. Рассмотрена оптимизация методом математического моделирования распределения рабочих процессов как один из методов повышения эффективности деятельности ИТ-компании.

Ключевые слова: бизнес-процесс, эффективность бизнес-процесса, реинжиниринг, оптимизация рабочих процессов, целевое программирование.

Многие крупные и мелкие предприятия для повышения конкурентоспособности вынуждены прибегать к реструктуризации своей деятельности. Для этого производится анализ деятельности предприятия в рамках какого-либо метода ее совершенствования.

Существует большое количество методов совершенствования деятельности предприятия, наибольшее распространение получили идеализация, статистическое управление, бенчмаркинг, реинжиниринг, оптимизация рабочих процессов.

Идеализация как метод улучшения деятельности предприятия опирается на данные опроса работников предприятия. В начале применения такого метода существует две модели деятельности предприятия: идеальная — та, к которой предприятие стремится, и фактическая, описывающая реальную работу предприятия. В большинстве случаев руководство собирает данные опроса начальников структурных подразделений и на их основе принимает те или иные решения по модернизации деятельности предприятия с целью приближения фактической модели деятельности предприятия к идеальной [1].

При статистическом управлении всю совокупную деятельность предприятия разбивают на составляющие, которые характеризуют некоторыми