

I. V. Grekov, V. B. Mantusov
Russian Customs Academy

P. N. Afonin
Saint Petersburg Electrotechnical University

IMPROVING THE PROCESS OF DIGITALIZATION OF CUSTOMS SERVICES DURING THE «INTELLECTUAL» CUSTOMS CONTROL OF INTERNATIONAL POSTAL ITEMS IN THE CUSTOMS AUTHORITIES OF THE RUSSIAN FEDERATION

The article discusses approaches to the process of improving new digital technologies in the field of customs services and customs control of international mail. The statistics of the growth rates of international mailings (with a forecast value) are given. Based on the new digital technologies already used in the world, the author proposes a model of digitalization of customs services and customs control using the capabilities of artificial intelligence. The use of performance indicators and automation values necessary for calculating data on the results of using the digitalization model is proposed. The use of this model in practice will have an impact on the identification and suppression of cases of importation into the customs territory of goods with violations of customs legislation (prohibited and dangerous goods, commercial shipments of goods under the guise of goods for personal use).

Artificial intelligence, international mail, customs control, performance and automation indicators, customs services, non-trade turnover, goods for personal use, e-commerce, automatic categorization of the consignment, analysis of X-ray images

УДК 004.67

М. И. Авилов, Ю. А. Шичкина
Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Дополнительная диагностика аномалий при мониторинге динамической компьютерной сети с применением рабочих сценариев

Рассматривается проблема своевременного реагирования на возникающие аномалии в работе компьютерной сети с учетом изменения количества наблюдаемых сетевых узлов. В случаях изменения их количества необходима корректировка границ диапазонов кластеризации аномалий компьютерной сети. Предлагаемый в статье метод корректировки границ диапазонов кластеризации аномалий с учетом общего числа наблюдаемых узлов и установленных триггеров позволяет проводить гибкую дополнительную диагностику аномалий в динамической компьютерной сети. После определения или предсказания класса аномалии следующим шагом предполагается выбор инструментария по предотвращению наступления аномалии или ликвидации ее последствий. С этой целью в данной статье предлагается метод выбора вспомогательных инструментов дополнительной диагностики работы компьютерной сети с применением рабочих сценариев. О результатах проведения дополнительной диагностики информируют системного инженера. Оба метода позволяют автоматизировать процесс выявления аномалий в компьютерной сети и повысить надежность и качество ее работы.

Система мониторинга сети, динамическая компьютерная сеть, мониторинг компьютерной сети, модуль диагностики, кластеризация аномалий

На сегодняшний день большое количество устройств используются в компьютерных сетях (КС), о чем говорит проблема адресного про-

странства IPv4 [1]. Несмотря на то, что IPv4 решает проблему нехватки адресов, рост числа сетевых устройств в различных сферах деятельно-

сти продолжается. Количество устройств в компьютерных сетях различных учреждений редко бывает постоянным, если это не закрытая сеть для решения специальных задач. Отслеживание состояния устройств в динамических, т. е. изменяемых по количеству узлов, сетях, а также своевременное реагирование на ситуации может стать нетривиальной задачей.

Команды специалистов по мониторингу сетевой инфраструктуры применяют различные инструменты для отслеживания состояния соединений и устройств сети, однако когда необходима дополнительная диагностика для корректного выявления и устранения проблемных участков, такие действия часто осуществляются в ручном режиме. Если при этом еще и изменяется количество наблюдаемых узлов, то время выявления причин и устранения возникшей ситуации может значительно увеличиться относительно ситуации, когда количество наблюдаемых узлов известно.

Существуют различные системы мониторинга компьютерных сетей (в [2] приведен сравнительный анализ часто применяемых систем мониторинга КС). Однако универсальное решение, подходящее для всех существующих задач при мониторинге КС, не найдено, поэтому происходит построение комплексных систем мониторинга, которые осуществляют как активный, так и на определенных участках пассивный мониторинг компьютерной сети. В зависимости от ситуации системный инженер может вручную комбинировать

такие подходы. В случае небольшой загруженности компьютерной сети применяется активный подход, а в случае полной загруженности – ручной перевод КС на пассивный мониторинг. Построение систем комбинированного мониторинга сети трудоемко, потому что требуется определять в автоматическом режиме, когда осуществлять активный, а когда пассивный мониторинг КС, считывать загруженность трафиком не только каналов, но и вычислительных ресурсов сетевых узлов, а также другие специфические аспекты эксплуатации компьютерной сети организации. В таблице приведен сравнительный анализ активного, пассивного и комбинированного подходов к мониторингу компьютерной сети.

По результатам сравнения различных подходов к мониторингу КС можно отметить, что при любой системе сбор, обработка данных и реакция на неклассифицированные заранее аномалии в работе сети необходимы для оперативного их выявления и устранения. Методы выявления и проведения дополнительной диагностики для решения таких задач реагирования на аномалии могут дополнять как активный, так и пассивный или комбинированный мониторинг работы компьютерной сети.

В данной статье предлагается метод кластеризации аномалий при мониторинге динамической КС, а также метод выбора вспомогательных инструментов дополнительной диагностики аномалий компьютерной сети с применением рабочих сценариев

Параметры сравнения	Активный	Пассивный	Комбинированный
Нагрузка на канал	При активном измерении создается дополнительный трафик	Дополнительный трафик не добавляется	Трафик добавляется только при активном измерении и когда нагрузка в сети ниже установленного порогового значения
Отображение информации в режиме реального времени	Поддерживается. Относительно небольшая задержка в обработке информации	Не поддерживается. Сначала информация собирается в течение некоторого времени, после обрабатывается и предоставляется в нужном виде	Поддерживается, но оптимально задействовать только при сетевой нагрузке ниже установленного порогового значения
Сбор информации	Сбор информации осуществляется путем опроса нескольких сетевых устройств.	Сбор информации осуществляется на отдельном каждом сетевом узле	Использует лучшие стороны активного и пассивного мониторинга. Зависит от нагрузки на сетевые ресурсы
Актуальность информации	Так как информация предоставляется в режиме реального времени, то информация актуальна	При больших объемах данных требуются большие временные затраты на обработку этих данных, а значит часть информации может быть не актуальной	Зависит от расстановки приоритетов. Критическая информация может собираться в режиме реального времени, не критическая собираться отдельно

риев. Статья является продолжением исследования, описанного в [3], по мониторингу статической компьютерной сети с применением модуля дополнительной диагностики.

Обзор существующих решений. С учетом того, что в настоящее время активно развиваются сетевые технологии и появляется все больше различных распределенных систем, используемых в организациях, растет и количество аномалий в работе компьютерных сетей, лежащих в основе этих систем. В [4] авторы описывают результаты анализа способов появления сетевых аномалий, как наблюдаемых, так и не имеющих видимых признаков. Также авторы делают выводы, что наиболее опасным источником сетевых аномалий служат действия злоумышленников.

Существуют работы по выявлению классификаций аномалий на основе отклонений в использовании сетевых ресурсов. Авторы [5] предлагают собственный программный инструмент, позволяющий автоматически выявлять аномалии и анализировать журналы сетевых служб. Авторы отмечают, что применение такого инструмента позволяет конфигурировать первую линию защиты сети, что повышает эффективность предотвращения вторжений, потому что выявляются инциденты, пропущенные стандартными средствами мониторинга и защиты сети.

Авторами [6] предлагается обобщенный подход к классификации сетевых аномалий. Отмечается, что для выявления аномалии может быть достаточно основных параметров трафика (телеметрии) без детального анализа сетевых пакетов. Также в [6] приводится описание аномалий по причине и характеру изменения сетевого трафика.

Для выявления аномалий могут использоваться методы нейронных сетей. В [7] приводится обоснование возможностей выявления аномалий в работе компьютерной сети с применением многослойного персептрона.

В [8] представлен анализ следующих алгоритмов обнаружения сетевых аномалий: гибридный алгоритм обнаружения сетевых аномалий на основе голосования, алгоритм на основе дискретного вейвлет-преобразования, алгоритм Бродского–Даровского, алгоритм на основе критерия согласия Колмогорова–Смирнова, алгоритм на основе суммы квадратов вейвлет-коэффициентов. Также авторы предлагают гибридный алгоритм обнаруже-

ния сетевых аномалий и процедуру обнаружения сетевых аномалий, основанную на этом алгоритме.

В [9] представлено решение раннего обнаружения появления рисков снижения качества функционирования компьютерной сети. Результаты работы позволяют проводить диагностику работы компьютерной сети и уменьшать время устранения проблем. На основе исторических данных нейросеть обучается выявлению симптомов ухудшения работы компьютерной сети, благодаря чему можно осуществлять прогнозирование. Сопоставляются текущее состояние функционирования КС с проблемами «в прошлом».

Авторы [10] предлагают модель прогнозирования отказов оборудования на основе Random Forest. Аномалии и отказы выявляются посредством определения разности показаний фактического и прогнозного значений сигналов. При прогнозировании используется алгоритм машинного обучения Random Forest. Сама модель включает несколько подмоделей, которые прогнозируют отказ оборудования.

Многие алгоритмы и методы строятся с учетом заранее определенной классификации аномалий, будь то аномалии программные или аппаратные, аномалии в трафике или в доступности сетевых узлов. Классификации могут быть как созданы самими системными инженерами, так и взяты их готовые варианты, которые предлагаются в различных публикациях по классификации аномалий работы компьютерной сети. Однако все равно могут возникать ситуации, когда аномалию сложно классифицировать. В таких случаях необходимо проводить дополнительную диагностику для определения причин ее возникновения и корректного реагирования на нее. Для того чтобы знать, когда необходимо запускать дополнительную диагностику, требуется кластеризация аномалий.

Из вышеизложенного следует, что в данное время существует много методов, алгоритмов, подходов к выявлению аномалий в функционировании компьютерной сети. Однако когда аномалия не подпадает под классификацию, а количество наблюдаемых узлов изменяется, необходимо проводить коррекцию с учетом этого изменения. Это требует корректировки границ диапазонов кластеризации для дополнительной диагностики в случаях выявления аномалий в работе сети. В данной

статье предлагается метод кластеризации аномалий при мониторинге динамической компьютерной сети, учитывающий изменение границ диапазонов кластеризации, в случаях изменения количества наблюдаемых узлов. Кроме этого предлагается выбирать вспомогательные инструменты на основе сформированных рабочих сценариев, а при отсутствии таковых формировать сценарии эмпирически, отслеживая состояние сетевого узла, на котором возникла проблемная ситуация.

Постановка задачи. Проведение дополнительной диагностики аномалий при мониторинге динамической компьютерной сети должно заключаться в том, что при появлении аномалии в работе КС проводится кластеризация аномалии и при необходимости осуществляется дополнительная диагностика с запуском вспомогательного инструмента, выбранного в соответствии с рабочим сценарием воздействия на аномалию. Формирование рабочего сценария происходит через эмпирическое обучение применению вспомогательного инструментария. Такая дополнительная диагностика аномалии в работе компьютерной сети необходима для своевременного выявления причин и реагирования на возникшую аномалию, чтобы устранить причины возникновения аномалии и/или минимизировать их деструктивные последствия в работе динамической компьютерной сети.

Целью проводимых исследований являлась оценка возможностей выявления и своевременно реагирования на аномалии при мониторинге работы динамической компьютерной сети с учетом изменений количества наблюдаемых узлов. Для этого были разработаны методы кластеризации аномалий при мониторинге динамической компьютерной сети и метод выбора вспомогательных инструментов дополнительной диагностики аномалий компьютерной сети с применением рабочих сценариев.

Метод кластеризации аномалий при мониторинге динамической компьютерной сети. В случае если осуществляется кластеризация аномалии при мониторинге динамической компьютерной сети, то первоначально границы кластеризации устанавливаются так же, как в случае со статической компьютерной сетью, но в дальнейшем они изменяются согласно изменению количества узлов сети, относящихся к диапазонам кластеризации. Т. е. при добавлении или удалении наблюдаемых узлов сети границы кластеризации корректируются с учетом этого изменения.

Первоначальные границы диапазонов определяются так же как в [3]. Пусть a и b – границы диапазонов для выбора соответствующего инструментария дополнительной диагностики, например: $[0, a)$ – информирование о проблемных участках сети; $[a, b)$ – запуск диагностики с дополнительными инструментами мониторинга компьютерной сети; $[b, 1]$ – запуск заранее написанного сценария для критических случаев и информирование о ситуации. Количество узлов для диапазонов кластеризации известно, так как узлы промаркированы, но не идентифицированы для кластеризации. Дальше сетевые узлы могут добавляться или удаляться из компьютерной сети в ручном или автоматическом режиме. Однако при их удалении или добавлении изменяется количество маркированных узлов, и это влияет на диапазоны кластеризации. Границы кластеризации в таком случае рассчитываются слева направо, от 0 до 1, следующим образом:

Если узлы относятся к диапазону $[0, a)$, то диапазоны кластеризации будут следующими:

$$[0; N_1 \pm \Delta N), [N_1 \pm \Delta N; N_2 \pm \Delta N), [N_2 \pm \Delta N; 1], \quad (1)$$

где $0, N_1, N_2, 1$ – границы диапазонов кластеризации аномалий до изменения числа узлов сети; ΔN – изменение границ кластеризации аномалий, т. е.

$$N_y \pm \Delta N = \frac{h_y \pm \Delta h}{m \pm \Delta m}, \quad (2)$$

где N_y – значение правой границы диапазона кластеризации; h_y – максимальное количество сработанных триггеров, привязанных к наблюдаемым параметрам и подходящих для формирования диапазона кластеризации; Δh – число, на которое изменилось максимальное значение триггеров, подходящих для формирования диапазона кластеризации при удалении или добавлении узлов в сети; m – максимальное количество установленных триггеров (привязанных к наблюдаемым параметрам); Δm – значение, на которое изменилось максимальное количество установленных триггеров.

Если подставить (2) в (1), то получим

$$\left[0; \frac{h_1 \pm \Delta h}{m \pm \Delta m}\right), \left[\frac{h_1 \pm \Delta h}{m \pm \Delta m}; \frac{h_2 \pm \Delta h}{m \pm \Delta m}\right), \left[\frac{h_2 \pm \Delta h}{m \pm \Delta m}; 1\right], \quad (3)$$

где h_1 и h_2 – максимальное количество сработанных триггеров, привязанных к наблюдаемым параметрам и подходящих для формирования первого и второго диапазонов кластеризации.

Если узлы относятся к диапазону $[a, b)$, то изменение границ происходит по формуле

$$[0; N_1), [N_1; N_2 \pm \Delta N), [N_2 \pm \Delta N; 1]. \quad (4)$$

Подставив (2) в (4), получим

$$\left[0; \frac{h_1}{m \pm \Delta m}\right), \left[\frac{h_1}{m \pm \Delta m}; \frac{h_2 \pm \Delta h}{m \pm \Delta m}\right), \left[\frac{h_2 \pm \Delta h}{m \pm \Delta m}; 1\right]. \quad (5)$$

Если узлы относятся к диапазону $[b, 1]$, то изменение границ происходит по формуле

$$[0; N_1), [N_1; N_2), [N_2; 1]. \quad (6)$$

Подставив (2) в (6), получим

$$\left[0; \frac{h_1}{m \pm \Delta m}\right), \left[\frac{h_1}{m \pm \Delta m}; \frac{h_2}{m \pm \Delta m}\right), \left[\frac{h_2}{m \pm \Delta m}; 1\right]. \quad (7)$$

В случае, если узлы удаляются и распределение по диапазонам становится невозможным, то границы между диапазонами начинают объединяться слева направо:

$$\begin{aligned} &[0; a), [a; b), [b; 1] \\ &[0; b), [b; 1] \\ &[0; 1]. \end{aligned}$$

С учетом описанного общего проведения дополнительной диагностики аномалий при мониторинге компьютерной сети и предложенного формирования границ кластеризации по формулам (1)–(7) был разработан метод кластеризации аномалий при мониторинге работы динамической компьютерной сети.

Пусть V – среднее значение сработавших триггеров наблюдаемых узлов.

Входные данные для кластеризации: множество триггеров, сформированное по (1)–(7).

Выходные данные по кластеризации: значение в диапазоне $[0, 1]$, в соответствии с которым запускается ответное действие на возникшую ситуацию в работе компьютерной сети.

Шаг 1. Исходя из требований к работе компьютерной сети, определяется правая граница a для диапазона $[0; a)$ по (1). Переход к шагу 2.

Шаг 2. Исходя из требований к работе компьютерной сети, определяется правая граница b для диапазонов $[a; b)$ и $[b; 1]$ по (4), (6). Переход к шагу 3.

Шаг 3. На основе рассчитанных границ a и b по (1)–(7) формируем диапазоны кластеризации. Переход к шагу 4.

Шаг 4. Проверяется изменение количества наблюдаемых узлов. Если изменений нет, то переход к шагу 8. Иначе – шаг 5.

Шаг 5. Если произошло изменение количества наблюдаемых узлов для диапазона $[0; a)$, то происходит корректировка границ диапазонов по (3). Иначе – шаг 6.

Шаг 6. Если произошло изменение количества наблюдаемых узлов для диапазона $[a; b)$, то происходит корректировка границ диапазонов по (5). Иначе – шаг 7.

Шаг 7. Если произошло изменение количества наблюдаемых узлов для диапазона $[b; 1]$, то происходит корректировка границ диапазонов по (7). Иначе – шаг 4.

Шаг 8. Расчет веса V для кластеризации по формуле

$$V = \frac{\sum_{i=1}^n x_i}{n},$$

где V – среднее значение сработавших триггеров множества X ; x_i – значение триггера; n – максимальное количество триггеров. Переход к шагу 9.

Шаг 9. Если $V = 0$ (вся группа сетевых узлов работает в штатном режиме), то шаг 18. Иначе – шаг 10.

Шаг 10. Если $V = 1$ (вся группа сетевых узлов недоступна), то запуск специального сценария и переход к шагу 14. Иначе – шаг 11.

Шаг 11. Если $V \in [0; a)$ (информирование о проблемных участках сети), то шаг 14. Иначе – шаг 12.

Шаг 12. Если $V \in [a; b)$ (запуск модуля дополнительной диагностики), то шаг 15. Иначе – шаг 14.

Шаг 14. Если $V \in [b; 1]$ (запуск заранее написанного сценария для критических случаев), то шаг 17. Иначе – шаг 18.

Шаг 14. Информирование системного инженера о текущем состоянии работы компьютерной сети. Переход к шагу 18.

Шаг 15. Обработка данных для запуска вспомогательного инструмента. Переход к шагу 16.

Шаг 16. Проведение дополнительной диагностики при помощи вспомогательных инструментов. Переход к шагу 14.

Шаг 17. Запуск заранее написанного сценария для критической ситуации. Переход к шагу 14.

Шаг 18. Завершение работы модуля дополнительной диагностики по поступившим входным данным. Ожидание новых входных данных.

Конец метода.

Метод выбора вспомогательных инструментов дополнительной диагностики аномалий компьютерной сети с применением рабочих сценариев. В случае, когда в динамической компьютерной сети часто меняется количество наблюдаемых сетевых узлов, нейросеть необходимо переучивать с учетом измененного их количества. Поэтому для проведения дополнительной диагностики в динамической сети предлагается эмпирическое применение вспомогательных инструментов и фиксация рабочих сценариев ответных действий, а не нейросеть, как в [3]. Под рабочим сценарием понимаются условия, при кото-

рых запускается тот или иной вспомогательный инструмент проведения дополнительной диагностики аномалий. Такие рабочие сценарии записываются в базе данных (БД) сценариев (фиксация). Однако такой рабочий сценарий может быть записан только в случае нормализации значения наблюдаемого параметра сетевого узла. На рис. 1 представлена схема проведения дополнительной диагностики при мониторинге работы динамической компьютерной сети.

Этапы дополнительной диагностики с рабочими сценариями:

1. Идет систематический опрос значений критически значимых параметров узлов.
2. Если на узле срабатывает триггер, привязанный к критически значимому наблюдаемому параметру, то происходит опрос признаков для

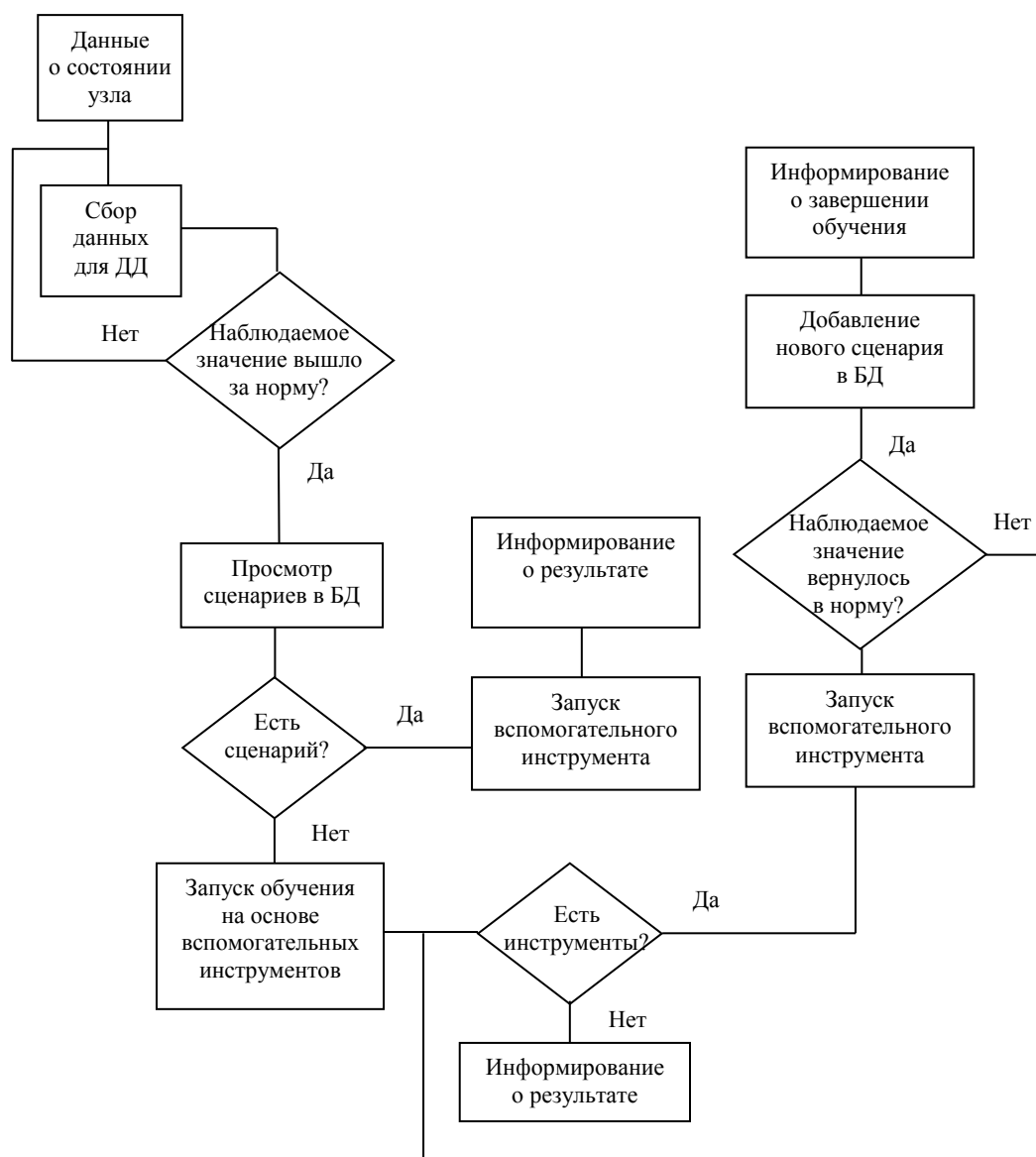


Рис. 1

формирования условий по запуску вспомогательного инструмента.

3. После получения данных происходит прогон по БД сценариев.

4. Если сценарий обнаружен, то запускается вспомогательный инструмент.

5. Если нет, то запускается эмпирическое обучение путем формирования рабочего сценария.

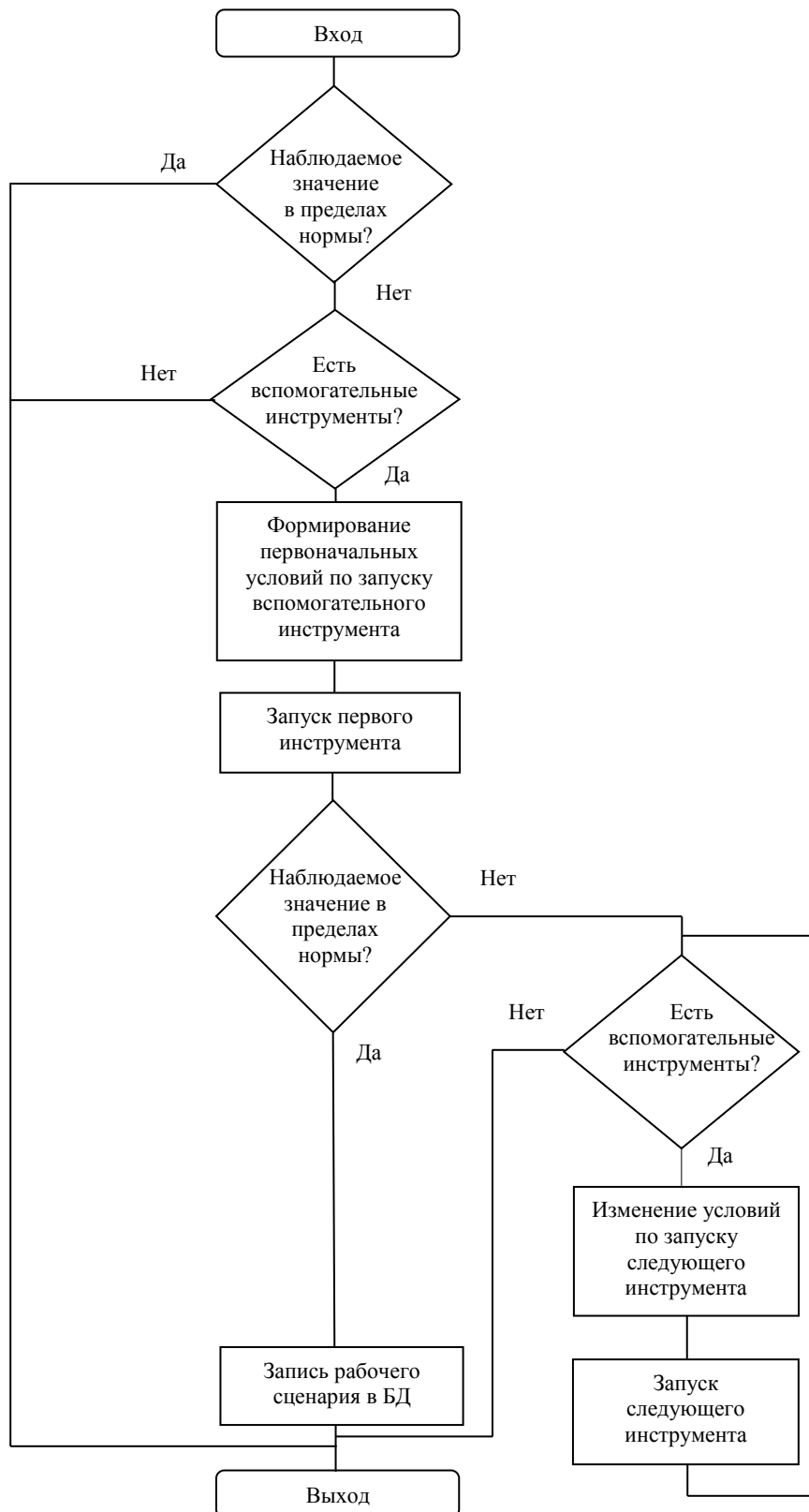


Рис. 2

6. Если инструмент помог (значение триггера, привязанного к наблюдаемому параметру, вернулось в изначальное состояние), то рабочий сценарий добавляется в БД сценариев.

7. Если инструмент не помог, то применяется следующий инструмент.

8. Если инструменты закончились, то происходит информирование инженера о ситуации. Ожидаются новые входные данные.

Выбор инструментов и эмпирическое обучение. Системный инженер определяет список вспомогательных инструментов для дополнительной диагностики из имеющегося у него инструментария. Получаем:

$$G = \sum_{y=1}^k g_y; \quad T = \sum_{w=1}^u t_w,$$

где G – суммарное количество инструментов для проведения дополнительной диагностики; g_y – выбранный инструмент; k – максимальное количество выбранных инструментов; T – суммарное количество признаков сети для запуска вспомогательного инструмента диагностики аномалии; t_w – признак для запуска вспомогательного инструмента диагностики аномалии; u – максимальное количество признаков; y, w – номера текущего и вспомогательного инструментов.

Получаем матрицу выбора инструментов для проведения дополнительной диагностики

$$M = GT.$$

Однако далее расстановка признаков сети относительно вспомогательных инструментов не происходит. Для дополнительной диагностики собираются и фиксируются данные по признакам, после чего применяются вспомогательные инструменты диагностики. Если какой-то инструмент срабатывает, то фиксируется рабочий сценарий.

Рабочий сценарий включает в себя информацию о признаках сети, положительно сработавшем инструменте и идентификатор наблюдаемого узла.

На рис. 2 схематично показано, как происходит выявление рабочего сценария.

Посредством проверок результатов применения инструментов формируется рабочий сценарий для выявленной аномалии в работе

компьютерной сети. Результатом положительной проверки служит возвращение значения наблюдаемого параметра на сетевом узле в пределы, установленные как «норма». Если этот инструмент не помог, применяется следующий. Перебор инструментов происходит до тех пор, пока они не закончатся или не будет достигнут положительный результат.

Результаты. Предложен метод кластеризации аномалий при мониторинге работы динамической компьютерной сети. Такая кластеризация осуществляется через распределение диапазонов реагирования на аномалии и расчет весового значения для попадания в соответствующий диапазон. Границы диапазонов кластеризации устанавливает системный инженер, исходя из требований к работе компьютерной сети. При кластеризации аномалий динамической компьютерной сети предложена регулировка границ диапазонов кластеризации на основе изменения количества наблюдаемых значимых сетевых узлов. Также предложен метод выбора вспомогательных инструментов дополнительной диагностики аномалий компьютерной сети с применением рабочих сценариев. Метод с применением рабочих сценариев основан на эмпирическом обучении выбору вспомогательных инструментов и формировании рабочего сценария в случае успешного применения вспомогательного инструмента. По результатам проведения дополнительной диагностики информируется системный инженер.

В рамках исследования оценивалась возможность выявления и своевременного реагирования на аномалии при мониторинге работы компьютерной сети с учетом изменения количества наблюдаемых узлов, но не проводился анализ наилучшей архитектуры хранения сценариев с целью ее распространения как базы знаний для других систем, связанных с поддержкой работы сетевой компьютерной инфраструктуры. В данном направлении исследования продолжаются.

Исследование выполнено при финансовой поддержке РФФИ и СИТМА (Министерство науки, технологии и окружающей среды Республики Куба) в рамках научного проекта №18-57-34001.

СПИСОК ЛИТЕРАТУРЫ

1. White B., Robertson A. Available pool of unallocated IPv4 Internet addresses now completely emptied. 2011. URL: <https://itp.cdn.icann.org/en/files/announcements/release-03feb11-en.pdf> (дата обращения 13.10.2021).
2. Костенко Е. Ю., Дуйсенгалиев Р. Р., Барабанова Е. А. Система мониторинга для контроля трафика технологических сетей передачи данных // Вестн. Астрахан. гос. техн. ун-та. Сер. управление, вычисл. техн. информ. 2015. № 4. С. 101–109.
3. Авилов М. И., Шичкина Ю. А., Куприянов М. С. Мониторинг информационно-коммуникационной компьютерной сети с применением модуля дополнительной диагностики // Изв. СПбГЭТУ «ЛЭТИ». 2020. Вып. 5. С. 34–45.
4. Причины и источники сетевых аномалий / В. С. Оладько, С. Ю. Микова, М. А. Нестеренко, Е. А. Садовник // Молодой ученый. 2015. № 22 (102). С. 158–161.
5. Кулясов Н. В., Исаев С. В. Исследование сетевых аномалий корпоративной сети Красноярского научного центра // Сибирский журн. науки и технологий. 2018. Т. 19, № 3. С. 412–422.
6. Микова С. Ю., Оладько В. С., Нестеренко М. А. Подход к классификации аномалий сетевого трафика // Междунар. науч. журн. «Инновационная наука». 2011. № 11. С. 78–80.
7. Кусякина Н. М. Применение методов нейронных сетей для построения систем выявления аномалий сетевого трафика // Colloquium-j. 2019. № 2 (26). С. 36–38.
8. Микова С. Ю., Оладько В. С., Мелких А. А. Гибридный алгоритм обнаружения сетевых аномалий на основе системы голосования // Вестн. УГАТУ. июнь 2018. Т. 20, № 1 (71). С. 168–174.
9. Шелухин О. И., Осин А. В., Костин Д. В. Мониторинг и диагностика аномальных состояний компьютерной сети на основе изучения «исторических данных» // Т-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 23–30.
10. Шаханов Н. И., Варфоломеев И. А., Ершов Е. В., Юдина О. В. Прогнозирование отказов оборудования в условиях малого количества поломок // Вестн. Череповецкого гос. ун-та. 2016. № 6. С. 36–41.

M. I. Avilov, Yu. A. Shichkina
Saint Petersburg Electrotechnical University

ADDITIONAL DIAGNOSTICS OF ANOMALIES WHEN MONITORING A DYNAMIC COMPUTER NETWORK USING WORKING SCENARIOS

The problem of timely response to emerging anomalies in the computer network is considered, taking into account changes in the number of observed network nodes. In cases of changes in the number of observed nodes it is necessary to adjust the boundaries of the anomaly clustering ranges of the computer network. The method proposed in the paper to adjust the boundaries of anomaly clustering ranges taking into account the total number of observed nodes and the set triggers allows a flexible additional diagnosis of anomalies in a dynamic computer network. Once the anomaly class has been identified or predicted, the next step is to select tools to prevent the anomaly from occurring or to eliminate its consequences. To this end, this paper proposes a method for selecting auxiliary tools for additional diagnostics of computer network operation using work scenarios. Based on the results of additional diagnostics, the system engineer is informed. Both methods allow you to automate the process of detecting anomalies in the computer network and improve the reliability and quality of its work.

Network monitoring system, dynamic computer network, computer network monitoring, diagnostics module, anomaly clustering
