УДК 004.67

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

Мониторинг информационно-коммуникационной компьютерной сети с применением модуля дополнительной диагностики

Рассматривается проблема оперативного реагирования на возникающие аварийные события на стыке проактивного и реактивного мониторинга работы информационно-коммуникационной компьютерной сети. Часто по результатам проактивного мониторинга нет возможности спрогнозировать, а по результатам реактивного мониторинга – корректно среагировать на появившееся событие без дополнительной диагностической информации. Для решения данной проблемы предлагается подход к организации мониторинга информационно-коммуникационной компьютерной сети с применением модуля дополнительной диагностики аномалий и предварительной их кластеризацией. Модуль дополнительной диагностики основан на искусственной нейронной сети, которая идентифицирует инструменты, необходимые для устранения аномалий. По результатам дополнительной диагностики системного инженера уведомляют о проделанной работе и о текущем функционировании информационно-коммуникационной компьютерной сети.

Система мониторинга сети, проактивный и реактивный мониторинг, нейронная сеть, модуль диагностики, кластеризация аномалий, компьютерная сеть

С каждым годом использование информационно-коммуникационных компьютерных сетей (КС) в различных направлениях промышленности становится необходимым аспектом поддержания работы и развития предприятий промышленности. На сегодняшний день информационно-коммуникационная компьютерная сеть – один из основных инструментов по обмену информацией, важной для предприятий. Одновременно с увеличением востребованности в скорости обмена информацией по КС растут как количество приложений, работающих через эту КС, так и количество подключаемых новых сетевых устройств. В связи с этим также растут и проблемы, связанные с обеспечением корректной работы информационно-коммуникационных компьютерных сетей.

Несмотря на то, что для обеспечения надежности и функционирования информационно-коммуникационных КС задействуются команды специалистов, отслеживание критически важных объектов такой сети является одной из первичных задач. Это значит, что необходимо осуществлять мониторинг критически важных объектов компьютерной сети предприятия и оперативно реагировать на возникающие события.

Надо заметить, что существуют разные аппаратно-программные средства мониторинга компьютерной сети. К ним относятся различные инструменты мониторинга, использующие протокол ICMP [1], средства по обеспечению синхронизации и проведению опросов из центра мониторинга [2], инструменты для мониторинга потребления вычислительных ресурсов или для выявления аномалий [3], [4] в работе сетевых узлов с последующим выводом оповещений при возникновении незапланированных критических ситуаций.

Когда на предприятии возникает непредвиденная ситуация в работе КС, это часто обнаруживается, во-первых, слишком поздно, а во-вторых, как правило, сложно установить точную причину сбоев без дополнительной диагностики. Однако без своевременного определения причины возникновения сбоев невозможно применение соответствующего механизма для устранения проблем в работе КС и восстановления ее работы в штатном режиме с последующим предотвращением подобных проблемных ситуаций.

В данной статье предлагается подход к мониторингу информационно-коммуникационной се-

ти, позволяющий в режиме реального времени отслеживать состояние компьютерной сети, с применением методов искусственного интеллекта, кластеризировать аномалии и в зависимости от кластеризации применять либо дополнительные средства диагностики, либо средства устранения проблем в сети.

Обзор существующих решений. Из-за огромного количества приложений, использующих компьютерные сети, некоторые из которых имеют решающее значение для пользователей и предприятий, управление сетью имеет важное значение. Поэтому поддержание целостности и доступности компьютерных сетей становится приоритетной задачей для обеспечения функционирования предприятия.

Несмотря на длительную историю развития компьютерных сетей, исследования различных аспектов создания и улучшения их функционирования по-прежнему обладают высокой степенью актуальности сегодня. Это относится к задачам планирования, защиты, мониторинга, оптимизации компьютерных сетей и часто связано с определением и реализацией автоматически настраиваемых механизмов предоставления услуг, обеспечением безопасности, повышением качества услуг, учетом проходящей через сеть информации и т. п.

Особенно много исследований проводится в области мониторинга и управления сетевым трафиком. Так, в [5] авторы рассмотрели последние достижения и выделили основные тенденции развития подходов к классификации трафика, а также их компромиссы в области применимости, надежности и конфиденциальности. Авторы делают акцент на некоторые нерешенные проблемы в классификации интернет-трафика и предлагают несколько стратегий для их решения. В [6] авторы предлагают алгоритм обнаружения сетевого аномального трафика в среде облачных вычислений с помощью применения гибридной информационной энтропии, нормализации значений сетевых функций и использования SVM для обнаружения аномального поведения сети.

Еще одно направление исследований, которое сегодня на пике популярности и еще будет долго оставаться на этом пике, – безопасность сети. Повсеместное использование проводных и беспроводных сетей связи, интенсивное развитие интернета вещей предъявляют повышенное требование к безопасности важной и секретной информации с учетом того, что число желающих получить к ней доступ и развитие методов атак также растут быстро. Сетевые атаки – одна из главных угроз для Интернета вообще и предприятий в частности.

Гибкость сетевого взаимодействия в рамках сетевых протоколов – основа функционирования КС, но такая же гибкость допускает возможность неправомерного использования сети. В частности, вредоносное поведение в КС может маскироваться под рабочую нагрузку по трафику, становясь сложно уловимым для систем, предназначенных для обнаружения неправомерного использования сетевых ресурсов. Выявлению таких аномальных вредоносных элементов в сетях различных типов посвящена [7]. Две модели обнаружения «атак нулевого дня», основанные на глубоком обучении с использованием шумоподавляющего автокодера, предложены в [8].

В последнее время интенсивно развивается мобильная технология пятого поколения (5G), которая включает в себя расширенные функции связи и создает новые проблемы для систем кибербезопасности. Поэтому в литературе стали появляться результаты исследований по выявлению аномалий в таких сетях. Например, такие результаты, основанные на применении нейронных сетей, приводятся в [9].

Огромное число исследований в последние десятилетия посвящается нейронным сетям в части развития их фундаментальных основ и расширения сферы их применения. В [10] автор дает обзор классификаторов нейронных сетей с прямой связью в применении к статическим моделям с непрерывными входными данными. В [11] авторы делают обзор методологий глубокого обучения, включая глубокую сеть доверия на основе ограниченных машин Больцмана, глубокую нейронную и рекуррентную нейронную сети, а также методы машинного обучения, относящиеся к обнаружению сетевых аномалий.

В [12] авторы предлагают нейронную сеть C-LSTM для эффективного моделирования пространственной и временной информации, содержащейся в данных о трафике. Эта сеть состоит из трех основных слоев: уровень CNN (сверточная нейронная сеть) используется для уменьшения изменения частоты в пространственной информации; слой LSTM подходит для моделирования информации о времени; слой DNN (глубокая

нейронная сеть) используется для отображения данных в другое пространство. Фактически это комбинация из трех нейронных сетей, что сильно усложняет процесс выявления аномалий и требует значительных вычислительных ресурсов.

Еще один нейросетевой подход, многослойный персептрон (MLP), применяемый для обнаружения сетевых атак, представлен в [13]. Отличие данного подхода от большинства других описываемых в литературе заключается в том, что тип атаки также обнаруживается нейронной сетью, а не классифицируется по принадлежности одному из двух классов – нормальному или атакующему.

Надо отметить, что по сравнению с аномалией вредоносного действия в сети работ, посвященных другим аномалиям, немного и совсем немногие публикации касаются выявления аномалий в целом.

Обычные автоматизированные методы в значительной степени основаны на статистическом моделировании, а некоторые используют машинное обучение. Так, в [14] описана схема обнаружения гибридных аномалий, называемая авторами согласованной классификационной моделью для обнаружения сетевых аномалий (Ensemble-based Classification Model for Network Anomaly Detection – EnClass). Эта модель имеет три модуля: кластеризация для определения оптимального подмножества свойств сети, которые необходимо использовать для классификации сетевого трафика; уточнение набора функций и удаление ненужных атрибутов; построение дерева решений для классификации сетевого трафика. При подготовке реального набора данных авторы используют модель обнаружения знаний KDD [15].

В [16] представлен подход, основанный на иммунной системе, который позволяет применять обычные алгоритмы классификации для обнаружения аномалий. Этот подход представляется очень полезным, когда доступны только положительные образцы для обучения системы обнаружения аномалий. Предложенный подход использует положительные выборки для генерации отрицательных выборок, которые используются в качестве обучающих данных для алгоритма классификации.

Чтобы обеспечить нормальную работу большой компьютерной системы, часто практикуют постоянный сбор системных журналов и анализ сетевой активности для обнаружения аномалий. В [17] авторы демонстрируют интерактивную визуализацию как альтернативный и эффективный метод анализа файлов журнала для понимания сложного поведения компьютерных сетевых систем.

В [18] представлен подход к обнаружению сетевых аномалий для систем с ограниченными ресурсами, основанный на поведенческом анализе компьютерных систем и/или сетей. В статье рассматриваются два типа поведения модели: нормальное поведение (ожидаемая и желаемая активность) и аномальное поведение (все виды деятельности, которые не попадают в категорию нормального поведения). Во время процесса диагностики каждый конкретный случай оценивается как нормальное или аномальное поведение. Для определения степени аномальности вводятся весовые значения, применяются метолы математической статистики и скользящего окна. Сложность данного подхода остается в однозначной классификации события как аномального.

Из вышесказанного следует, что в настоящее время существует большое количество методов и подходов к выявлению сетевых угроз, мониторингу сетевого трафика, выявлению отдельных видов аномалий в работе компьютерной сети (как правило, связанных с информационной безопасностью). Это логично, так как из-за возникновения аномалий в сетевом трафике нарушается корректное функционирование информационно-коммуникационной компьютерной сети. Эффективность любой модели обнаружения аномалий в основном зависит от выбора соответствующих функций и алгоритмов обучения, которые используются для классификации аномалий. Однако из-за разнообразия аномалий многие решения, описанные в литературе, не подходят для других случаев и требуют адаптации или комбинирования с дополнительными методами. В нашей статье мы отходим от проблемы классификации аномалий и показываем, что инструмент для устранения аномалии может быть выбран без четкой их классификации. Наш метод подходит для устранения многих аномалий в сети. Он позволяет провести кластеризацию аномалий для определения класса тех аномалий, для которых не подходят заготовленные системным инженером сценарии, и тех, о которых не достаточно простого информирования системного инженера. Это –

группа аномалий, которые не относятся к числу часто встречающихся, но могут возникать в любой компьютерной сети. Их сложно классифицировать, но как показал метод, описанный в данной статье, с помощью нейронных сетей для их устранения можно подобрать подходящий инструмент из числа имеющихся в распоряжении системного инженера.

Постановка задачи. Под аномалиями в нашем исследовании понимается превышение установленных пороговых значений наблюдаемых параметров сетевых узлов при функционировании компьютерной сети. В результате таких отклонений КС может целиком или частично перестать корректно работать. Для выявления аномалий в работе информационно-коммуникационной компьютерной сети необходимо осуществлять ее мониторинг. Мониторинг информационно-коммуникационной КС разделяется на проактивный и реактивный [19], [20].

На сегодняшний день существует множество подходов для проведения *проактивного мониторинга* информационно-коммуникационных КС с применением методов искусственной нейронной сети. Эти подходы различаются набором входных данных, методами анализа (временные ряды [21], пассивный сбор симптомов и активные проверки [21], мониторинг на основе результирующего сигнала нейронной сети [22], применение гибридных нейросетей [23]) и реализации, а также способами представления результатов. Однако если такой мониторинг только начал работу, то данные за продолжительный период времени еще не собраны, а это значит, что корректно прогнозировать события, которые могут произойти, не представляется возможным [24]. Также надо заметить, что при появлении критического события по результатам работы проактивного мониторинга информационно-коммуникационной КС может быть только уведомление системному инженеру об уже произошедшем событии, и прогнозировать дальнейшее развитие ситуации становится проблематично. В таких ситуациях применяется реактивный мониторинг компьютерной сети.

При *реактивном мониторинге* информационно-коммуникационной компьютерной сети реакция на возникшую критическую ситуацию происходит уже после ее возникновения. В результате этого запускаются механизмы по информированию, определению и, по возможности, устранению возникшей критической ситуации. Например, автоматический сбор дополнительной информации и отправка уведомления системному инженеру, а также выполнение заранее написанного сценария для устранения возникшей ситуации на сетевом узле.

Однако бывают случаи, когда необходимо «вручную» проводить дополнительную диагностику для выявления причин возникающих проблем – например, когда наблюдаемый сетевой узел перестал отвечать системе мониторинга компьютерной сети, но при этом данные, проходящие через него, могут успешно передаваться на соседние сетевые узлы. Проведение дополнительной диагностики может занять много времени. Для уменьшения времени проведения дополнительного анализа и увеличения скорости реагирования на появляющиеся события в работе КС возможно применение искусственных нейронных сетей для проведения дополнительного анализа возникшей ситуации и запуска соответствующего ответного «действия», когда по результатам проактивного мониторинга нет возможности спрогнозировать, а по результатам реактивного – корректно среагировать на появившееся событие без дополнительной диагностической информации.

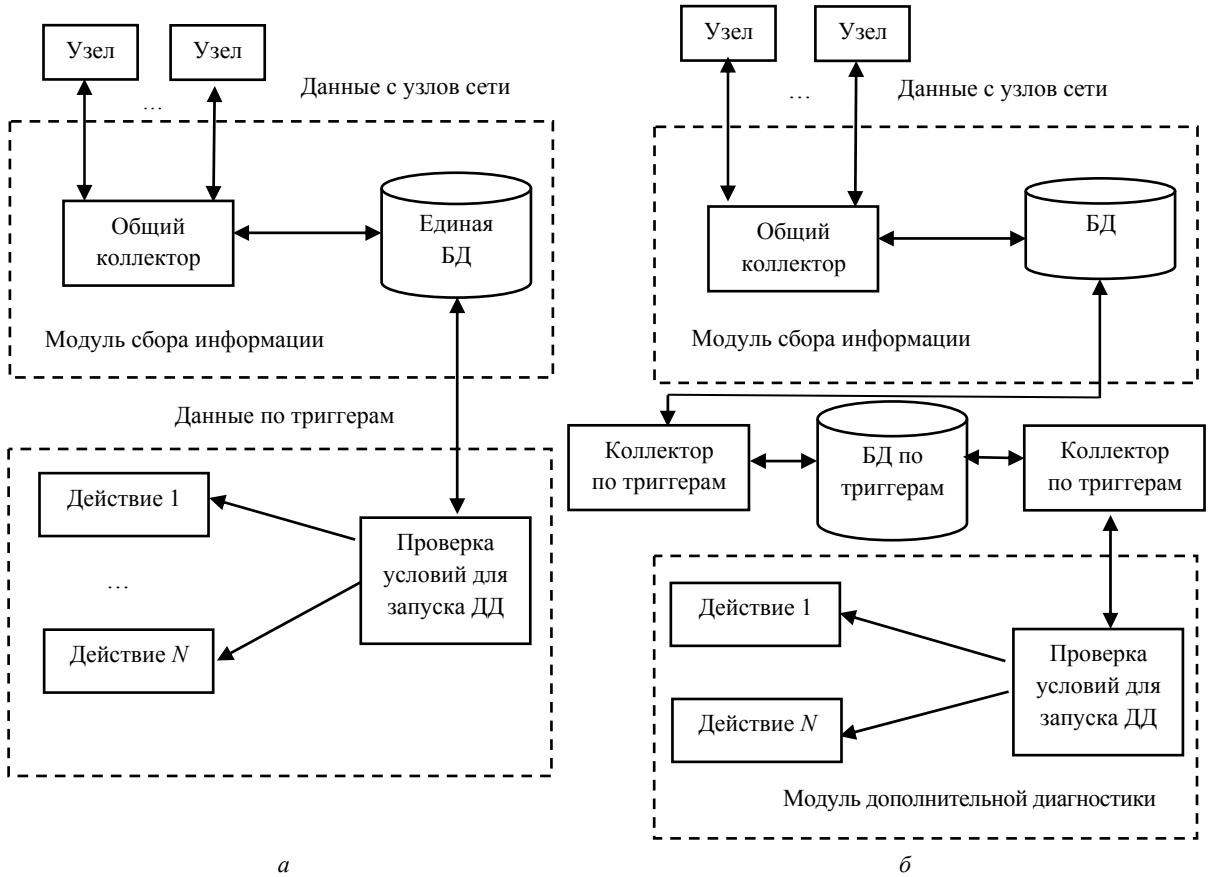
Целью проводимых исследований была оценка возможности применения нейронных сетей для выполнения дополнительной диагностики компьютерной сети на примере двухслойного персептрона. Для этого были проведены исследования подходов к формированию и хранению входных данных для метода дополнительной диагностики КС, кластеризации ее аномалий на основе сформированных входных данных, разработке метода дополнительной диагностики аномалий при мониторинге КС.

Система мониторинга компьютерной сети с модулем дополнительной диагностики аномалий. Конфигурируемая в рамках данного исследования система мониторинга информационно-коммуникационной компьютерной сети должна собирать, обрабатывать, хранить собранные данные с наблюдаемых сетевых узлов и в случае возникновения аномалий запускать дополнительную диагностику с непосредственным применением сценариев на основе нейронной сети к опознанным аномалиям или с предварительной идентификацией инструментария для неизвестных аномалий.

К признакам наблюдаемых узлов могут относиться самые разные параметры, например имена узлов и групп узлов, сетевая идентификация узлов (ip-адреса, доменные имена), значения аппаратных параметров (насколько загружен ЦП, ОЗУ, ПЗУ и др.), временные параметры (частота опроса сетевых узлов, периоды хранения истории), состояния установленных триггеров, а также параметры системы мониторинга, необходимые для представления соответствующей информации системному инженеру. Все значения этих параметров хранятся в базе данных (БД) системы мониторинга. Для проведения дополнительной диагностики используется только их часть. Поэтому отдельно стоит вопрос об использовании отдельной базы данных для хранения параметров, необходимых для диагностики, или об их извлечении из единой БД системы мониторинга в ходе диагностики.

Модуль дополнительной диагностики (ДД) может быть задействован только после обучения нейронной сети. На вход модуля ДД поступают значения триггеров, соответствующие параметрам, чьи значения превысили установленные пороговые значения, тем самым сигнализируя о возможном наличии аномалии. Значения этих триггеров могут храниться как в самой базе данных системы мониторинга вместе с другими данными по мониторингу КС, так и в отдельной БД. Преимущества и недостатки использования системы мониторинга (СМ) информационно-коммуникационной КС с единой БД и отдельной БД для триггеров представлены в табл. 1 и 2, а схемы с отдельной БД и без нее – на рис. 1, *а* и *б* соответственно.

Основное преимущество использования единой базы данных СМ для хранения всех данных по мониторингу КС, включая и данные для модуля ДД (табл. 2), – это отсутствие накладных расходов на проведение дополнительных вычислительных операций по перезаписи данных в отдельную БД и экономия памяти за счет отсутствия дубликатов данных. Однако в этом случае будет потеряно время на выбор и обработку данных, необходимых для модуля ДД, и возможны потери данных, необходимых для нейронной сети, в случае сбоя в единой базе данных СМ. Этих недостатков лишена система с отдельной базой



а *б*

Рис. 1

Таблица 1

Преимущества	Недостатки
Скорость обработки данных. Нет необходимости осуществлять выбор необходимых данных из всех данных, собираемых СМ КС в единой БД. **Независимость и сохранность данных.** Входные данные хранятся в отдельной БД. В случае сбоя единой БД системы мониторинга отдельная БД может быть сохранена	**Длительность обработки данных.** Увеличение вычислительных операций за счет перезаписи входных данных для модуля ДД в отдельную БД. **Связь СМ с БД.** Необходимость определять способы взаимодействия системы мониторинга с отдельной БД (например, при помощи API или создания отдельных инструментов на Python, Java, PHP или др.). **Расход памяти.** Так как происходит перезапись входных данных для модуля ДД, то размер памяти для хранения информации увеличивается

Таблица 2

Преимущества	Недостатки
Длительность обработки данных. Нет дополнительных вычислительных операций на перезапись данных в отдельную БД. **Меньший расход памяти**, так как нет перезаписи входных данных для модуля ДД в отдельную БД	**Риски потери информации для ДД.** Нет дополнительной независимости и сохранности входных данных для модуля ДД, так как нет перезаписи входных данных для модуля ДД в отдельную БД. **Связь СМ с БД.** Необходимо определить способы взаимодействия с единой БД (например, при помощи API или создания отдельных инструментов на Python, Java, PHP или др.). **Увеличение времени на выборку входных данных для модуля ДД,** так как выборка входных данных для модуля ДД осуществляется из всех собираемых данных СМ

данных для модуля ДД. Однако у нее также есть свои недостатки, перечисленные в табл. 1. Поэтому при выборе подхода к построению системы мониторинга КС с дополнительным модулем диагностики необходимо учитывать самые разные аспекты – объем доступных ресурсов, оперативность в обработке данных, риски потери информации и т. п.

В случае появления аномалии в работе информационно-коммуникационной КС срабатывают триггеры, значения которых обрабатываются модулем дополнительной диагностики.

Результатом проведения ДД может быть одно из следующих действий:

– информирование системного инженера о проблемных участках сети;

– проведение ДД для идентификации инструментария устранения аномалии и запуск выбранного инструментария с информированием системного инженера о результатах его выполнения или рекомендация для системного инженера к запуску выбранного инструментария;

– выполнение сценариев для аномалий, не требующих идентификации, и информирование системного инженера о результатах выполнения сценариев.

При проведении дополнительной диагностики входные данные должны поступать на вход обученной нейронной сети, которая должна идентифицировать соответствующий инструмент для устранения появившейся аномалии.

Вследствие этого одной из задач данного исследования стал выбор архитектуры нейронной сети, формирование входных данных для обучения и работы нейронной сети.

Формирование входных данных для нейронной сети. Искусственная нейронная сеть в модуле ДД решает задачу классификации запуска дополнительных средств диагностики.

Пусть:

• A – множество всех наблюдаемых параметров системы мониторинга компьютерной сети:

$$A = \{a_1, ..., a_i\}, \quad (1)$$

где i – максимальное количество наблюдаемых параметров множества A;

• B – множество наблюдаемых параметров одного сетевого узла:

$$B = \{b_1, ..., b_j\}, \quad (2)$$

где j – максимальное количество наблюдаемых параметров множества B.

Так как собираемые значения параметров каждого сетевого узла – только часть всех наблюдаемых параметров системы мониторинга, то

$$A = \{B_1, ..., B_k\},$$
$$A = \{\{b_{11}, ..., b_{j1}\}, ..., \{b_{1k}, ..., b_{jk}\}\},\ b_{jk} = a_i, \quad (3)$$

где k – максимальное количество наблюдаемых сетевых узлов.

Пусть C – множество выбранных для наблюдения анализируемых сетевых узлов:

$$C = \{B_1, ..., B_p\}, \quad (4)$$

где p – максимальное количество выбранных для наблюдения анализируемых сетевых узлов.

Для анализируемых узлов могут оцениваться не все параметры, а только некоторая их совокупность. Пусть d_p – интересующий наблюдаемый параметр анализируемого узла, тогда D – множество выбранных наблюдаемых параметров анализируемых сетевых узлов:

$$d_p \in B_p;$$
$$D = \{d_1, ..., d_p\}. \quad (5)$$

Для каждого параметра d_p системный инженер устанавливает пороговое значение, характерное для штатной роботы его информационно-коммуникационной компьютерной сети. Показателем выхода значения наблюдаемого параметра за пороговое значение является дополнительный параметр – триггер. Триггеры могут принимать значение 0 или 1, где 0 означает, что значение наблюдаемого параметра не вышло за установленное пороговое значение, а 1 – что значение

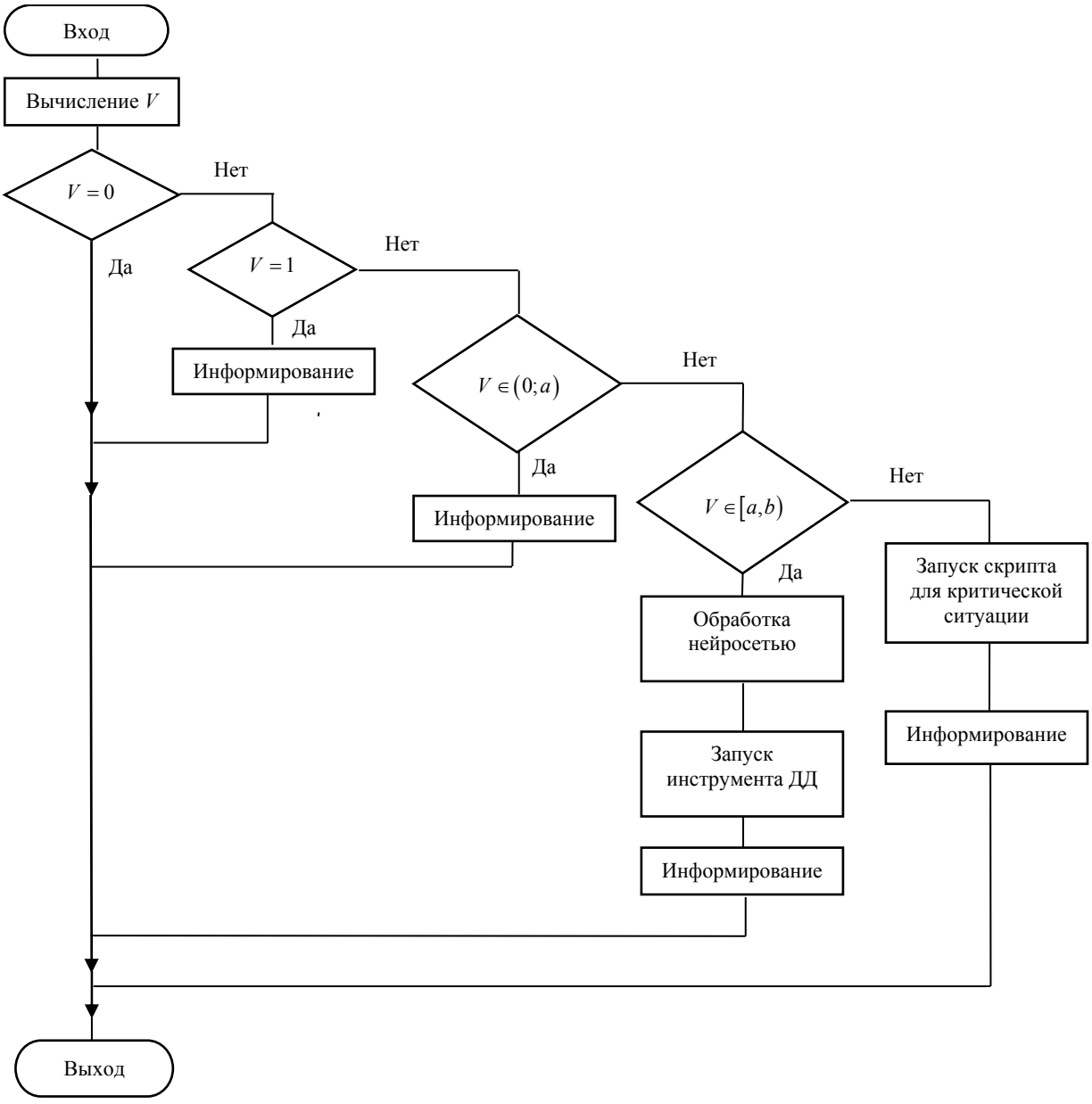


Рис. 2

наблюдаемого параметра вышло за установленное пороговое значение. Если поставить каждому значению d_p в соответствие триггер, то всему множеству D будет соответствовать множество триггеров

$$X = \{x_1, ..., x_n\},\ n = p, \qquad (6)$$

где n – максимальное количество установленных триггеров на выбранные наблюдаемые параметры сетевых узлов.

Это множество X и подается на вход модуля ДД. Схема работы модуля ДД изображена на рис. 2.

После того как сформированы входные данные для модуля дополнительной диагностики, необходимо определить, в каких случаях стоит подавать эти данные на вход искусственной нейронной сети, а в каких – нет. Для этого необходимо множеству X поставить в соответствие некоторое число (вес), которое позволяло бы его отнести к одному из трех видов аномалий, соответствующих действиям в разделе о тестировании модуля ДД. Будем полагать, что диапазон допустимых значений весов равен [0, 1].

В качестве веса V множества X можно взять среднее значение составляющих его триггеров:

$$V = \sum_{i=1}^{n} x_u \Big/ n, \qquad (7)$$

где V – среднее значение триггеров множества X; x_u – значение триггера; n – количество триггеров.

Диапазоны для информирования, дополнительной диагностики и информирования, запуска заранее написанного сценария и информирования определяются системным инженером исходя из требований к функционированию его информационно-коммуникационной компьютерной сети.

Метод дополнительной диагностики аномалий при мониторинге КС. Входные данные: множество триггеров, сформированное по формулам (1)–(6).

Выходные данные: значения [0, 1], в соответствии с которыми запускается ответное действие на возникшую ситуацию в работе компьютерной сети.

Шаг 1. Кластеризация аномалий по (7).

Шаг 2. Если $V = 0$ (вся группа сетевых узлов работает в штатном режиме), то шаг 12. Иначе шаг 3.

Шаг 3. Если $V = 1$ (вся группа сетевых узлов недоступна), то шаг 7. Иначе шаг 4.

Шаг 4. Если $V \in (0; a)$ (информирование о проблемных участках сети), то шаг 7. Иначе шаг 5.

Шаг 5. Если $V \in [a, b)$ (запуск модуля дополнительной диагностики), то шаг 8. Иначе шаг 6.

Шаг 6. Если $V \in [b, 1)$ (запуск заранее написанного сценария для критических случаев), то шаг 11. Иначе шаг 12.

Шаг 7. Информирование системного инженера о текущем состоянии работы компьютерной сети. Переход к шагу 12.

Шаг 8. Подача входных данных на входы искусственной нейронной сети. Переход к шагу 9.

Шаг 9. Обработка искусственной нейронной сетью входных данных. Переход к шагу 10.

Шаг 10. Запуск соответствующего инструмента дополнительной диагностики – по результатам работы искусственной нейронной сети. Переход к шагу 7.

Шаг 11. Запуск заранее написанного сценария для критической ситуации. Переход к шагу 7.

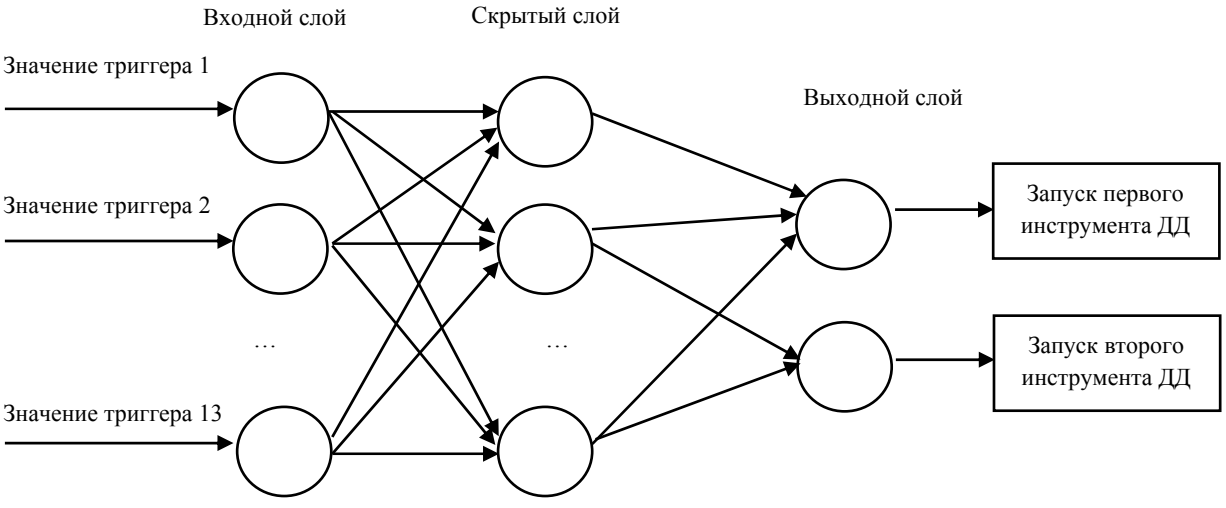


Рис. 3

Шаг 12. Завершение работы модуля дополнительной диагностики по поступившим входным данным. Ожидание новых входных данных.

Применение нейронной сети для выбора инструмента устранения аномалий. Искусственная нейронная сеть в модуле ДД решает задачу классификации инструментов, которые необходимо запускать для дополнительной диагностики. На рис. 3 показана структура нейронной сети, применяемой в рамках данного исследования.

Обучение искусственной нейронной сети происходит с помощью «учителя» с использованием метода обратного распространения ошибки. Используемая нейронная сеть представляет собой двухслойный персептрон. В качестве функции активации используется «сигмоид»:

$$\sigma(x) = \frac{1}{1+e^{-x}}.$$

Данная функция позволяет более «гладко» корректировать выходной сигнал, нормируя его в диапазоне от 0 до 1.

Тестирование работы модуля ДД. На данный момент существует много систем мониторинга компьютерной сети. В рамках данного исследования была применена система мониторинга Zabbix [25]. Она позволяет собирать метрики при помощи зеркалирования трафика, работы через SNMPv3 (Simple Network Management Protocol), RMON (Remote Network MONitoring), проверок через ICMP (Internet Control Message Protocol), IPMI (Intelligent Platform Management Interface), проверки, а также содержит возможность использования отдельного специального Zabbix-агента на сетевых узлах. Модуль ДД написан на языке программирования Python 3 [26]. Работа с наблюдаемыми параметрами осуществлялась посредством API Zabbix.

Из двух возможных СМ, представленных на рис. 1, для тестирования был выбран вариант системы мониторинга информационно-коммуникационной КС с единой базой данных СМ.

Первичное тестирование системы мониторинга информационно-коммуникационной компьютерной сети с применением модуля ДД проводилось на основе 13 тестовых сетевых узлов. Доступность сетевых узлов проверялась при помощи протокола ICMP. Для классификации действий установлен следующий тестовый диапазон:

– 0 – никаких действий не осуществлять;

– (0; 0.4) – информирование системного инженера о проблемных сетевых участках;

– [0.4; 0.8) – запуск модуля дополнительной диагностики и информирование системного инженера о результатах работы;

– [0.8; 1) – применение заранее написанного сценария и информирование системного инженера о результатах работы;

– 1 – информирование системного инженера о критической ситуации.

В табл. 3 отражены результаты тестирования кластеризации аномалий и сопоставление с соответствующими действиями в ответ на эти появляющиеся в работе информационно-коммуникационной КС аномалии.

Результатом работы модуля ДД, основанного на нейронной сети (рис. 3), был запуск следующих инструментов дополнительной диагностики:

– утилит ping и traceroute для проверки передачи данных по сетевым маршрутам до сетевых узлов;

– заранее написанного скрипта по сбору дополнительных метрик.

По завершении проведения дополнительной диагностики проводилось информирование системного инженера о результатах проделанной работы.

Результат обучения искусственной нейронной сети в модуле ДД на 700 циклах обучения сформирован при помощи библиотеки matplotlib [27] на Python 3 и представлен на рис. 4.

По графику результатов обучения нейронной сети видно, как изменялась точность правильного ответа и ее приближение к значению абсолютной точности, равному 1. Для циклов с 1-го по 34-й обучение идет быстро, дальше начинается замедление и только с 670-го цикла значение точности правильного ответа становится более 0.96, что приемлемо в данном тестировании.

Таблица 3

Недоступно хостов	Значение V	Диапазон	Действие
0	0	0	Никаких действий не производить
13	1	1	Информирование о критической ситуации
3	0.23077	(0; 0.4)	Информирование о проблемном участке сети
6	0.46153	[0.4; 0.8)	Запуск дополнительной диагностики и информирование
11	0.84615	[0.8; 1)	Запуск заранее написанного сценария

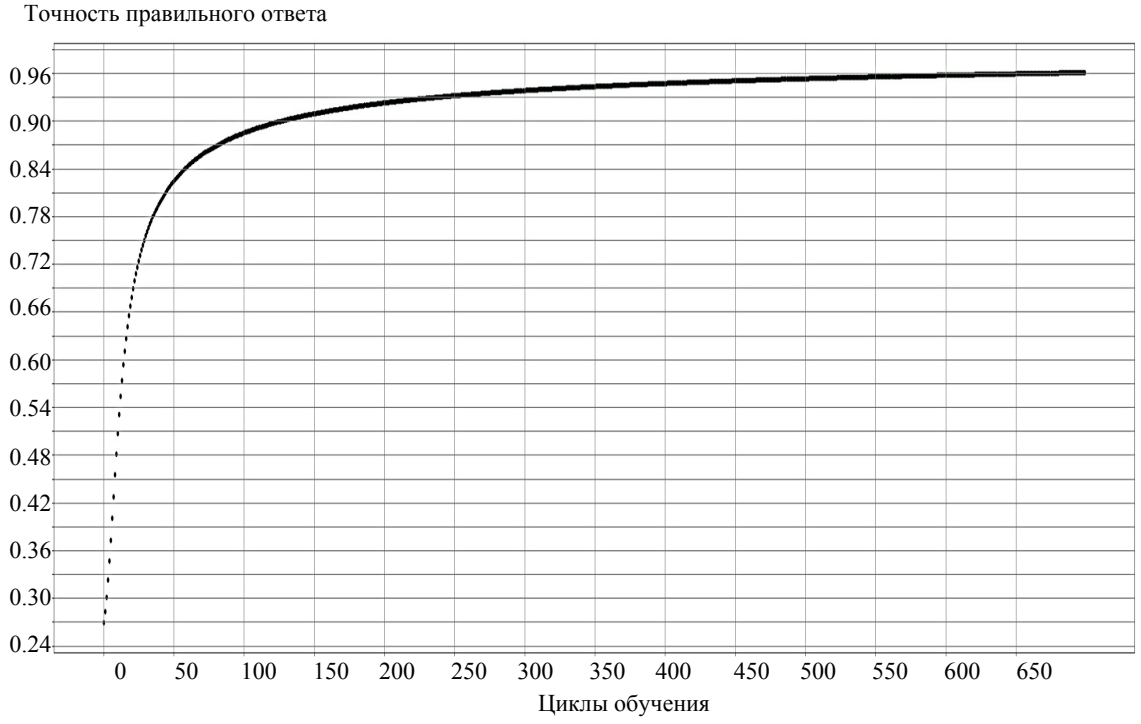


Рис. 4

Результаты. Тестирование предложенного метода дополнительной диагностики аномалий при мониторинге компьютерной сети показало положительные результаты. Применение модуля дополнительной диагностики на основе двухслойного персептрона показывает, что при помощи такого модуля можно проводить дополнительный анализ и осуществлять определенное реагирование на возникающие события во время работы информационно-коммуникационной компьютерной сети без вспомогательной классификации аномалий.

Применение подхода к работе системы мониторинга КС с единой БД системы мониторинга дает возможность работать с данными без выполнения дополнительных операций по перезаписи данных в отдельную БД, что позволяет сократить объем памяти, выделяемый для хранения собранной системой мониторинга информации. Однако при применении такого подхода увеличивается время на выборку входных данных для модуля дополнительной диагностики и не осуществляется дополнительное хранение этих входных данных, поэтому для их сохранности необходимо проводить автоматическое систематическое резервное копирование единой базы данных.

В рамках исследования оценивалась только возможность применения нейронных сетей для выбора инструментов устранения аномалий модуля ДД, но не проводился анализ наилучших архитектуры и типа нейронной сети. Архитектура и способы обучения искусственной нейронной сети могут быть разными и вполне могут различаться в зависимости от специфики области деятельности предприятия и количества инструментов, имеющихся у системного инженера для устранения аномалий. В данном направлении исследование продолжается.

СПИСОК ЛИТЕРАТУРЫ

1. Обеспечение потребных нагрузок сетевых интерфейсов утилитой ping программного обеспечения протокола ICMP / М. К. Бойченко, И. П. Иванов, А. Ю. Кондратьев, В. А. Лохтуров // Вестн. МГТУ им. Н. Э. Баумана. Сер. Приборостроение. 2016. № 4. С. 74–84.

2. Шардаков К. С. Сравнительный анализ популярных систем мониторинга сетевого оборудования, распространяемых по лицензии GPL // Интеллектуальные технологии на транспорте. 2018. № 1 (13). С. 44–47.

3. Канаев А. К., Камынина М. А., Опарин Е. В. Способы обнаружения отклонений в функционировании элементов сети передачи данных в интересах системы управления // Бюл. результатов науч. исследований. 2012. Вып. 4 (3). С. 137–148.

4. Бажаев Н. А., Лебедев И. С., Кривцова И. Е. Анализ статистических данных мониторинга сетевой инфраструктуры для выявления аномального поведения локального сегмента системы // Науч.-техн.

вестн. информационных технологий, механики и оптики. 2017. Т. 17, № 1. С. 92–99.

5. Dainotti A., Pescape A., Claffy K. C. Issues and future directions in traffic classification // IEEE Network. 2012. Vol. 26, № 1. P. 35–40.

6. Chen Yang. Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment // Cluster Computing. 2019. Vol. 22. P. 8309–8317.

7. Compression analytics for classification and anomaly detection within network communication / C. Ting, R. Field, A. Fisher, T. Bauer // IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, № 5. P. 1366–1376.

8. Aygun R. C., Yavuz A. G. Network anomaly detection with stochastically improved autoencoder based models // IEEE 4th Intern. Conf. on Cyber Security and Cloud Computing (CSCloud). New York, NY, 2017. P. 193–198.

9. A Self-adaptive deep learning-based system for anomaly detection in 5G networks / L. F. Maimó, A. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, G. M. Pérez // IEEE Access. 2018. Vol. 6. P. 7700–7712.

10. Lippmann R. P. Pattern classification using neural networks // IEEE Communications Magazine. 1989. Vol. 27, № 11. P. 47–50.

11. A survey of deep learning-based network anomaly detection / D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, K. J. Kim // Cluster Computing. Vol. 22. P. 949–961.

12. Kim T. Y., Cho S. B. Web traffic anomaly detection using C-LSTM neural networks // Expert Systems with Applications. 2018. Vol. 106. P. 66–76.

13. Moradi M., Zulkernine M. A Neural network based system for intrusion detection and classification of attacks // Proc. of 2004 IEEE Intern. Conf. on Advances in Intelligent Systems, 2004. URL: http://research.cs.queensu.ca/home/moradi/148-04-MM-MZ.pdf (дата обращения 10.02.2020).

14. EnClass: Ensemble-based classification model for network anomaly detection in massive datasets / S. Garg, A. Singh, S. Batra, N. Kumar, M. S. Obaidat // 2017 IEEE Global Communications Conf. Singapore, 2017. P. 1–7.

15. Degtyarev A., Shichkina Y., Koblov A. Technology of cleaning and transforming data using the Knowledge Discovery in Databases (KDD) technology for fast application of Data Mining methods // CEUR Workshop Proc. 2016. № 1787. P. 428–434.

16. Gonzalez F., Dasgupta D., Kozma R. Combining negative selection and classification techniques for anomaly detection // Proc. of the 2002 Congress on Evolutionary Computation. Honolulu, HI, USA, 2002. Vol. 1. P. 705–710.

17. Visual data analysis for detecting flaws and intruders in computer network systems / Teoh Soon Tee, T. J. Jankun-Kelly, Ma Kwan-Liu, S. Wu Felix // IDAV Publications. URL: https://escholarship.org/uc/item/0v06v231 (дата обращения 10.02.2020).

18. Behavioural Approach to Network Anomaly Detection for Resource-Constrained System – Presentation of the Novel Solution – Preliminary Study / M. Pelc, D. Galus, M. Zolubak, S. Ozana, W. Chlewicki, K. Cichon, M. Podpora, A. Kawala Sterniuk // IFAC-PapersOnLine. 2019. Vol. 52, № 27. P. 121–126.

19. Дубровин М. Г., Глухих И. Н. Модели и методы проактивного мониторинга ИТ-систем // Моделирование, оптимизация и информационные технологии. 2018. Т. 6, № 1 (20). С. 314–324.

20. Методы тестирования и диагностирования компьютерных сетей / А. Л. Моисеев, Р. Р. Моисеева, В. В. Шаров, Ю. Н. Зацаринная // Вестн. Казан. технол. ун-та. 2014. Т. 17, № 1. С. 315–316.

21. Дубровин М. Г., Глухих И. Н. Методы проактивного мониторинга информационных систем // Системный администратор. 2018. Вып. 2. URL: http://samag.ru/archive/article/3599 (дата обращения 19.02.2020).

22. Петраков В. А., Богачев Д. Н. Применение нейронных сетей в мониторинге вычислительных центров // Изв. Юж. фед. ун-та. Техн. науки. 2009. № 2. С. 82–87.

23. Саенко И. Б., Скорик Ф. А., Котенко И. В. Мониторинг и прогнозирование состояния компьютерных сетей на основе применения гибридных нейронных сетей // Изв. вузов. Приборостроение. 2016. Т. 59. № 10. С. 795–800.

24. Прогнозирование отказов оборудования в условиях малого количества поломок / Н. И. Шаханов, И. А. Варфоломеев, Е. В. Ершов, О. В. Юдина // Вестн. Череповецкого гос. ун-та. 2016. № 6. С. 36–41.

25. Что такое Zabbix. URL: https://www.zabbix.com/ru/features (дата обращения 19.02.2020).

26. Python 3. URL: https://www.python.org/ (дата обращения 19.02.2020).

27. Matplotlib, URL: https://matplotlib.org/ (дата обращения 19.02.2020).

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

MONITORING OF AN INFORMATION AND COMMUNICATION COMPUTER NETWORK USING A NEURAL NETWORK MODULE

The problem of rapid response to emerging emergency events at the intersection of proactive and reactive monitoring of the information and communication computer network is considered. Often, the results of proactive monitoring do not allow you to predict, and the results of reactive monitoring do not allow you to correctly react to an event that appears without additional diagnostic information. To solve this problem, we propose an approach to organizing monitoring of an information and communication computer network using the module for additional diagnostics of anomalies and preliminary clustering of these anomalies. The advanced diagnostics module is based on an artificial neural network that identifies the tools needed to eliminate anomalies. Also, according to the results of additional diagnostics, the system engineer is notified about the work done and about the current functioning of the information and communication computer network.

Network monitoring system, computer network, proactive and reactive monitoring, artificial neural network

УДК 612.087.1

Т. В. Гордеева, М. Е. Шурыгина, А. О. Козловский
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Применение цифровой лицевой антропометрии в практических задачах

Лицевая антропометрия нашла широкое применение во многих областях науки и медицины. Статья включает краткую историю антропометрии, начиная от зарождения как науки и заканчивая актуальными алгоритмами. Исследуется использование антропометрических точек в практических задачах – таких, как замена изображений лиц, морфинг изображений лиц, реконструкция лиц из 2D в 3D, распознавание лиц, оценка привлекательности лиц, определение эмоций, а также детектор сонливости. Рассматриваются основные алгоритмы и этапы морфинга, сваппинга и реконструкции изображений лиц из 2D в 3D. Описываются методы реализации алгоритмов с помощью сторонних библиотек OpenCV и Dlib как с использованием пакета и языка программирования MATLAB, так и на языке C++. Приводятся результаты практических исследований алгоритмов морфинга, сваппинга и реконструкции изображений лиц из 2D в 3D на нескольких примерах, а также приводятся некоторые выводы, основанные на этих результатах.

Детекция лиц, лицевая антропометрия, триангуляция Делоне, метод обратных расстояний, сваппинг лиц, морфинг лиц, реконструкция лиц из 2D в 3D, распознавание лиц, привлекательность и красота лица, определение эмоций, детектор сонливости

Появление антропометрии как науки относится к XIII в., когда Марко Поло описал особенности строения и размеры различных частей тела представителей племен, встретившихся ему во время путешествия вокруг света. Однако наиболее активное развитие антропометрии происходило уже в XIX в., когда ее начали использовать в криминалистике. В биометрии, криминалистике, антропологии, лицевой пластической медицине и т. д. особенно важную роль получила лицевая антропометрия, позволяющая наиболее полно характеризовать индивидуальные черты лица человека.

С развитием компьютерных технологий наиболее активно используется цифровая лицевая антропометрия, которая включает [1]: автоматическое определение координат ключевых антропометрических точек (АПТ) на изображениях лиц (ИЛ), томографических сканах головы или черепа; оценку всех базовых (габаритных) размеров лица и его частей по расположению координат АПТ; оценку координат АПТ и границ примитивов лица; вычисление соотношений между выбранными координатами АПТ; составление сводных таблиц по этим соотношениям; проведение