ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿՐԹՈՒԹՅԱՆ ԵՎ ԳԻՏՈՒԹՅԱՆ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ՀԱՅԱՍՏԱՆԻ ԱԶԳԱՅԻՆ ՊՈԼԻՏԵԽՆԻԿԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Հովհաննիսյան Ծաղիկ Ստեփանի

ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ՕՊԵՐԱՏԻՎ ԿԱՌԱՎԱՐՄԱՆ ՄԻՋՈՑՆԵՐԻ ՄՇԱԿՈՒՄԸ

Ե12.03 - «Հեռահաղորդակցական ցանցեր, սարքավորումներ և համակարգեր» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ АРМЕНИЯ

НАЦИОНАЛЬНЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ АРМЕНИИ

ОганнисянЦагик Степановна

РАЗРАБОТКА СРЕДСТВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук по специальности
05.12.03– “Сети, устройства и системы телекоммуникации”

Ереван 2017

Ատենախոսության թեման հաստատվել է Հայաստանի ազգային պոլիտեխնիկական համալսարանում (ՀԱՊՀ)

Գիտական ղեկավար՝ տ.գ.դ., Գ.Տ. Կիրակոսյան

Պաշտոնական ընդդիմախոսներ՝ տ.գ.դ. Դ.Գ. Ասատրյան
տ.գ.թ. Խ.Գ. Շարոյան

Առաջատար կազմակերպություն՝ Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ

Ատենախոսության պաշտպանությունը տեղի կունենա2017թ. հուլիսի 11-ին ժամը 14.00-ին Հայաստանի ազգային պոլիտեխնիկական համալսարանում գործող ՀՀ ԲՈՀ-ի «Ռադիոտեխնիկայի և էլեկտրոնիկայի» 046 մասնագիտական խորհրդի նիստում: Հասցեն՝ 0009, Երևան, Տերյան փ. 105, 17 մասնաշենք):

Ատենախոսությանը կարելի է ծանոթանալ ՀԱՊՀ-ի գրադարանում:

Սեղմագիրն առաքված է 2017թ. հունիսի 7-ին:

046 Մասնագիտական խորհրդի
գիտական քարտուղար, տ.գ.թ. Մ.Յ. Այվազյան

Тема диссертацииутверждена в Национальном политехническом университете Армении (НПУА)

Научный руководитель: д.т.н.Г.Т. Киракосян

Официальные оппоненты: д.т.н. Д.Г. Асатрян
к.т.н. Х.Г. Шароян

Ведущая организация: Ереванский научно-исследовательский институт средств связи

Защита диссертации состоится 11 июля 2017г. в 14.00часов на заседании Специализированного совета 046 - “Радиотехника и электроника”, действующего при Национальном политехническом университете Армении (адрес: 0009, г. Ереван, ул. Теряна 105, корпус 17).

С диссертацией можно ознакомиться в библиотеке НПУА.

Автореферат разослан 7-го июня 2017г.

Ученый секретарь
Специализированного совета 046, к.т.н. М.Ц. Айвазян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Наряду с научно-техническим прогрессомпродолжают развиваться и усложняться корпоративные телекоммуникационные сети (КТС). Это обусловлено, прежде всего,применением в КТС новых телекоммуникационных технологий и устройств, повышением пропускной способности и уровня безопасности, увеличением количества пользователейи т.д.

В связи сувеличением информационных потоков, а также неэффективной организацией и реализацией управления в КТС часто нарушается нормальная работа разных организаций, и, как следствие, последние несут информационные и финансовые потери. Во избежание таких потерь необходимо разработать средства оперативного управления корпоративными телекоммуникационными сетями, позволяющими выявить аномалии и свести их к минимуму.

В настоящее время системы машинного обучения для выявления аномалий широко применяются в разных областях, следовательно,в рамках диссертационной работы особую актуальность представляет разработка самообучающей системы средств оперативного управления КТС. Внедрение данной системы в КТС позволит выявить не только те аномалии, которые появляются по известным причинам, но и те, которые ранее не были обнаружены.

Объект исследования. Объектом исследования являютсяразнотипные КТС, эффективная организацияи реализация их оперативного управления.

Цель и задачи работы. Целью диссертационной работы является повышение эффективности работы КТС, анализ мониторинга результатов и разработка средств оперативного управления КТС.

Для достижения указанной цели в работе были поставленыи решены следующие задачи:

1. Изучение, анализ и оценка современных методов организации КТС.
2. Сравнительный анализ и обоснованный выбор средств оперативногоуправления КТС.
3. Разработка системы оперативного управления безопасностью для контроля трафика в нижних слоях КТС посредством специализированных устройств и оборудования.
4. Разработка алгоритма и методики выявления аномалий, влияющих на работоспособность КТС.
5. Разработка автоматизированной системы средств оперативного управления КТС.

Методыисследования.В диссертации использованы теоретические и практические методыи средства построения разнотипных КТС, рассмотрены математические модели мониторинга и системы реализации КТС, а также методы

искусственного интеллекта.

Научная новизна. В процессе исследования получены следующие научные результаты:

1. Обоснована разработкамашинной самообучающей обучающей системы средств оперативного управления КТС, которая повышает надежность, работоспособность и эффективность эксплуатации этих сетей.
2. Разработан метод повышения эффективности решения задач в процессе оперативного управления КТС, при использовании которого для каждой задачи находится то единственное из существующих решений, которое уже с успехом было применено и испытано.
3. Разработан метод обнаружения аномалий посредством самообучающей системы для оперативного управления КТС.
4. Разработана автоматизированная открытая диалоговая система быстрого обнаружения и обработки аномалий в телекоммуникационных сетях для средств оперативного управления КТС, применение которой повышает надежность, работоспособность и эффективность эксплуатации сети, а также уменьшает ее загруженность.

Практическая значимость и внедрениерезультатов работы. Результаты диссертации использованы и внедрены в ООО "Онлайначурд" и ООО"ОМС" для повышения работоспособности и надежности, а также обеспечения эффективной эксплуатации КТС. Они применяются также при проведении лабораторных работ по предмету "Организация компьютерных сетей-2" на кафедре "Компьютерные системы и сети" Национального политехнического университета Армении (НПУА) в виде методических указаний для лабораторных работ "Организация сетей с оборудованиями D-Link".

На защиту выносятся следующие положения:

1. Обоснование выбора метода искусственного интеллекта для оперативного управления КТС.
2. Математическая модель, методи архитектура системы обнаружения аномалий посредством машинного обучения, действующего на работоспособность КТС.
3. Самообучающая и открытая диалоговая автоматизированная система обнаружения аномалий для оперативного управления КТС.

Достоверность научных положений подтверждена методологией исследования, применяемыми математическими моделями, результатами проведенных экспериментальных данных, соответствием разработанных методов и программного обеспечения, а также внедрением результатов работы.

Апробация работы. Основные научные и прикладные положения диссертации были доложены на научных конференциях НПУА (2012-2016гг.) и научных семинарах кафедры КСиС НПУА (2011-2016гг.).

Диссертационная работа реализована на кафедре КСиС НПУА в рамках проводимых научно-исследовательских и учебно-методических работ.

Публикации. Основные положения диссертации опубликованы в девяти научных статьях, список которых представлен в конце автореферата.

Структура и объем диссертации. Диссертация состоит из ведения, четырех глав, основных выводов, списка литературы из 110 наименований и трех приложений. Общий объем работы –131 страница, включая 41 рисунок и 7 таблиц. Диссертация написана на армянском языке.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформулированы цель и задачи исследования, представлены научная новизна, практическое значение и основные положения, выносимые на защиту.

В первой главе исследованы, анализированы и оценены текущее состояние и тенденции развития КТС. Изучены и сравнены действующие коммуникационные технологии для построения КТС: компьютерные, WiFi, WiMax,сети мобильных поколений GSM, NGN и облачные технологии (cloud technology). Рассмотрены средства оперативного управления трафиком телекоммуникационной сети. Проведены сравнительный анализ и оценка средств мониторинга, в результате которого было обоснованно было выбранопрограммное средство Zabbix, т.к. оно в открытом коде, работает со всеми операционными системами и является простым в эксплуатации.

Обоснована необходимость разработки разработанной автоматизированной открытой диалоговой системы для эффективного использования средств оперативного управления и построения КТС.

В конце главы представлены цель и сформулированы задачи исследования, а также даны выводы, полученные в результате выполнения работы.

Во второй главе исследованы вопросы организации безопасности, реализации и управления КТС. Для безопасности КТС предлагается разработанная система безопасного динамического оперативного управления KTCTNSCS (Telekommunication Network Security Control System). TNSCS использует программируемые коммутаторы, которые контролируют трафик в нижних слояхтелекоммуникационной сети. Система реализована архитектурой OpenFlow, в результате чего внешний контроллер может влиять на коммутатор направленного трафика.В частности, создается система управления динамическим доступом между контроллером и подсистемами интеграции мониторинга. Например, TNSCS может

автоматически переводить пользователей в карантин, если обнаружена опасность или имеются другие нарушения правил безопасности.

Для КТС были проведены вычисления загруженности сети по формуле

$$V = nv_i, \quad (1)$$

где n - число компьютеров в сети;v_i - загруженность одного компьютера в сети.

Загруженность одного компьютера в КТС вычисляется по формуле

$$V_i = D/t, \quad (2)$$

гдеD –количество передаваемых данных;t- время,в течение которого передаются данные.

Если D=3Мбит, t=60 с, то v=3/60=0,05Мбит/с. Учитывая, что в сети имеется 50 компьютеров, загруженность КТС составит V=50*0,05=2,5Мбит/с.

Пропускная способность для данной КТС - это наибольшая допустимая скорость передачи данных, которая определяется битовой скоростью и другими ограничивающими факторами (длительность между интервалами передаваемых блоков данных, объемом передаваемой по сети служебной информации и т.д.).

Во многих случаях пропускную способность можно считать равной битовой скорости. Согласно стандарту 100BASE-TX, пропускная способность составляет 100Мбит/с=12,5Мбит/с.

Одним из важнейших параметром сетиявляется коэффициент использования КТС(КИС), который равен отношению загруженности сети к его пропускной способности:

$$КИС = V/vmax, \quad (3)$$

где V –загруженность сети;vmax –пропускная способность.

Независимо от того, что скорость передачи данных для определенной технологии КТС всегда одинакова, производительностьтелекоммуникационной сети уменьшается параллельно с уменьшением объема передаваемых данных. Это связано в первую очередь с распределениемобъема передаваемых данных (трафика) между всемиузлами сети и с особенностями механизма работы доступа общей среды передаваемых данных.

Увеличение коэффициента использования КТС приводит к резкому уменьшению реальной скорости передачи данных. Потери времени, связанные с механизмом работы доступа распределенной среды, зависят от характера обращения к телекоммуникационнойсети и не могут быть точно вычислены.Следовательно, для обеспечения удовлетворительной производительности задается ограниченное значение использования КТС, при котором сеть быстро прореагирует на запросы пользователей.

На рис.1 представлены этапы процесса обнаружения и обработки аномалийв КТС. На этапе обработки данных необходимо выделить из потока информации все те данные, в результате анализа которых можно определить наличие аномалий.

Далее проводится обработка, на основе которой надо определить, действительно ли в КТС есть аномалия, или она работает в нормальном состоянии.

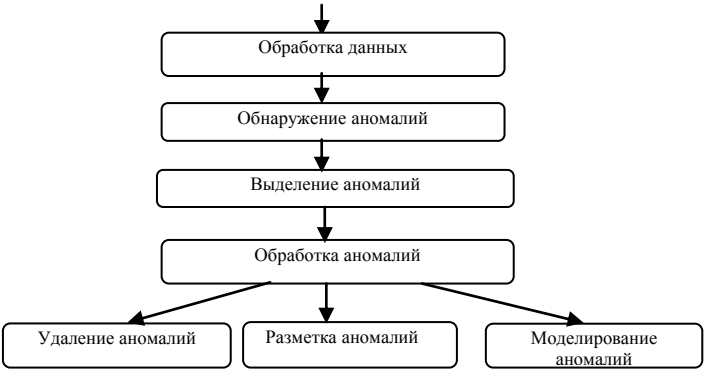

Рис.1. Пошаговая последовательность обнаружения и обработки аномалий в КТС

Если в КТС возникла аномалия, то необходимо выделить ее,а также те показатели, с помощью которых были обнаружены эти аномалии, и принять необходимые меры.

Процесс обнаружения аномалий состоит из двух этапов:

- на первом этапе классифицируются данные. В результате выделяется группа данных, которая имеет нормальное значение и которая не может быть причиной возникновения аномалии;
- на втором этапе проводится сравнение остальных данных с нормальным состоянием и выносится решение, не являются ли они измененными.

Для решения данной задачи существует множество методов машинного обучения. Результаты исследований показали, что наибольшую возможную точность можно получить, применяя методы машинного обучения нейронных сетей или опорные векторные методы (ОВМ), которыеприменимы не только для классификации трафика, но и наоснове их анализа впоследствии можно обнаружить возникающие в КТС аномалии.

ОВМотображает входные данные на многомерное пространство, используя соответствующую функцию, и строит функцию решений, по которой лучшим образом может данные одного класса отделить от данных другого класса. На рис. 2 приведено геометрическое представление ОВМ.

Предположим, задана группа данных $X_i \in R^n$, $i = 1,2,\dots,l$ без обучающей информации о классификации, где i - количество существующих точек в изучаемом наборе; R^n -входное пространство; n - размер входного пространства. $\Phi(x)$-отображающая функция, входное пространство xкоторой впоследствии

преобразуется в последующее пространство F. Функция определения $f(x)$имеет следующий вид:

$$f(x) = w^T \Phi(x) - \rho. \quad (4)$$

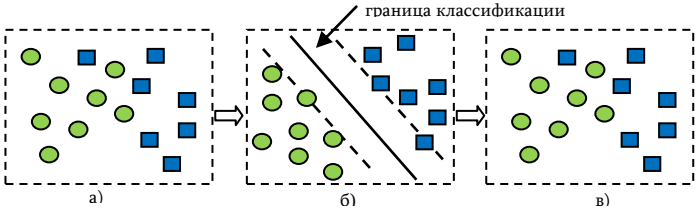

Рис.2. Нелинейное деление методомОВМ: а - входные данные, б - отображение на многомерное пространство, в - обратное отображение

Данная функция определения $f(x)$делит начальные данные на все возможные векторы $\Phi(x), i = 1,2,\dots,l$.

В (4) w - нормированная вертикаль гиперпространства;ρ- смещение гипер-пространства. Для определения w и ρ требуется решить следующую оптимизационную задачу:

- целевая функция:

$$min \frac{1}{2} w^T w + \frac{1}{vl} \sum_{i=1}^{l} \xi_i - \rho; \quad (5)$$

- ограничения:

$$w^T \Phi(x) \geq -\rho - \xi_i, \xi_i \geq 0, i = 1,2,\dots,l, \quad (6)$$

где ξ_i-переменная, вносящая точность в целевую функцию;$V \in (0,1)$-управляет компромиссом, доводя до максимума расстояние между гиперпространством и начальной точкой, а также количество точек в нем.Длярешения целевой функции для каждой x_i вводят множимое Лагранжа α_i.

Решение задачи приводится в виде

$$W = \sum_{i=1}^{l} \alpha_i \ \Phi(X_i), \quad (7)$$

где$0 \leq \alpha_i \leq \frac{1}{vl}$.

В качестве функции определения$f(x)$принимается следующая нелинейная функция:

$$f(x) = \sum_{i=1}^{l} \alpha_i K(x_i, x) - \rho, \quad (8)$$

где$K(x_i, x) = \Phi(x_i)^T \Phi(x)$, которая является ядром функции входного пространства.

Пусть задан временной ряд $W = W_1, W_2, \dots, W_T$, который состоит из равных Tчастей:$t = 1,2,\dots,T$.

Общую модель временного ряда можно представить в виде

$$w_t = g(t) + Y_t, \quad (9)$$

где $g(t)$ – детерминированная функция времени, а Y_t- представляет шум или ошибку.

Методом машинного обучения представим предсказание значения в данный момент времени следующим образом:

$$y = f(x) + n, \quad (10)$$

где $f(x)$- детерминированная функция;n- шум или ошибка.

В качестве входных данных имеем $\{(x_i y_i): i = 1, \dots, N\}$,где $x_i = (x_{i1}, \dots, x_{in})$, а$y_i$ генерируется на основе предыдущих данных.

Цель машинного обучения - найти такую$f'(x)$функцию, которая предскажет функцию $f(x)$.

При управлении ОВМ для значения, полученного в момент времениt, необходимо определить, находится ли оно в зоне аномалии.

Предположим, что значения, находящиеся в зоне аномалии, получаются из функции

$$y_{an} = f_{an}(t), \quad (11)$$

а значения вне зоны аномалии- из функции

$$y_n = f_n(t). \quad (12)$$

В этом случае в зависимости от того,к какойзоне наиболее близко будет находиться значение, полученное в момент t, этойзоне и будет оно соответствовать.Следовательно,требуется найти минимальное значение следующего выражения и по нему определить, какойзоне принадлежит входное значение:

$$Z=\min(y - y_{an}, y - y_n). \quad (13)$$

Внедрение машинной обучающей системы для обнаружения аномалий позволит выявить не только те аномалии, которые возникают по известным причинам, но и те, для возникновения которых до этого не было причин.

Втретьей главе представлены блок-схемы разработанного метода оперативного управления КТС, алгоритм обнаружения аномалий, а также архитектура системы обнаружения аномалий в КТС с помощью машинного обучения. Для обнаружения аномалий в КТС необходимо осуществлять постоянное наблюдение. На основе анализа результатов наблюдения можно обнаружить неполадки, загруженные узлы и т.д. Но прежде чем обнаружить аномалии,необходимо для КТС определить значения параметров наблюдения для нормального режима работы телекоммуникационной сети. Для повышения эффективности решения задач, возникаемых во время оперативного управления КТС, применяетсяразработанный метод, который приведен на рис. 3.

В данном случае инструментальными средствами проектирования специализированных сетей строится модель КТС, на которой проводится симуляция

разных ситуаций, и полученные результаты вводятся на вход системы машинного обучения. Это существенно повышает процесс обучения и позволяет системе быстрее обнаружить аномалии.

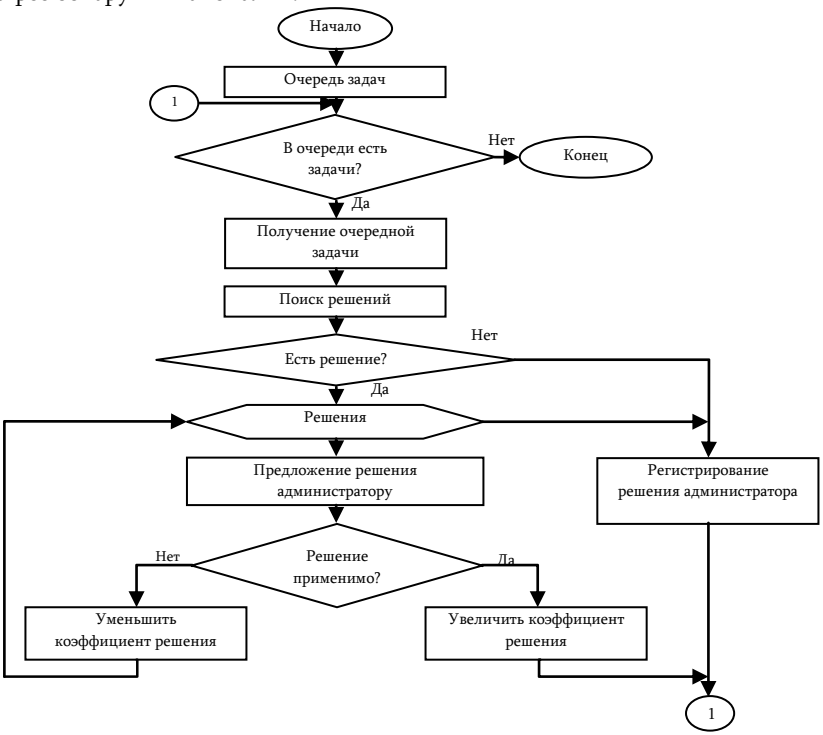

Рис. 3. Блок-схема методаоперативного управления КТС

Исходя из вышесказанного,предлагается следующая последовательность шагов, выполняемых для обнаружения аномалий (рис. 4).

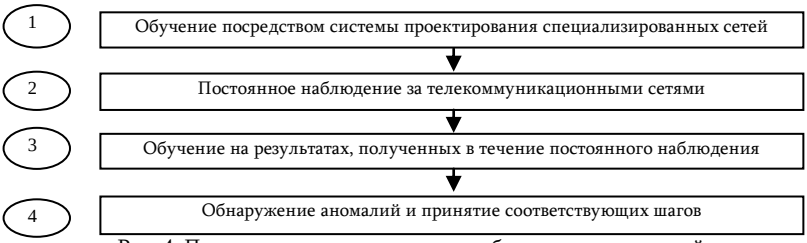

Рис. 4. Последовательность шагов для обнаружения аномалий

Обобщенная архитектура проектируемой системы обнаружения аномалий в КТС с помощью машинного обучения приведена на рис.5. Разработанная система состоит из следующих пяти подсистем: подсистема моделирования КТС, подсистема мониторинга КТС, подсистема машинного обучения, подсистема обнаружения аномалий и подсистема оперативного управления КТС.

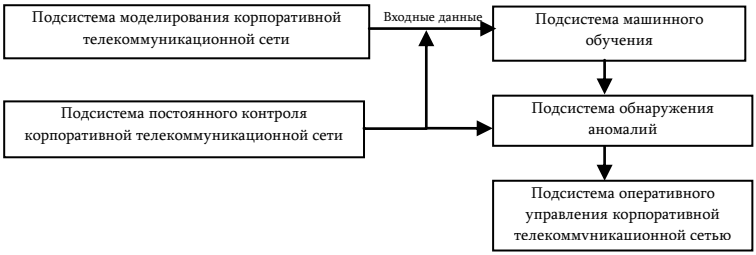

Рис. 5. Архитектура системы обнаружения аномалий в КТС с помощью машинного обучения

Подсистема моделирования позволяет с использованием специализированных инструментальных средств создать модель телекоммуникационной сети и реализовать симуляцию и сбор результатов разных ситуаций на этой модели. На основе анализа полученных данных получены результаты, соответствующие рассматриваемым параметрам моделируюшей ситуации. Подсистема мониторинга предусмотрена для получения рассматриваемых параметров сданных в эксплуатацию КТС.

Результаты, полученные при рассмотрении этих двух подсистем, передаются подсистеме обнаружения аномалий, которая, обрабатывая полученные результаты с помощью ОВМ, обнаруживает аномалии и сообщает об этом подсистеме оперативного управления. Посредством подсистемы оперативного управления выполняются шаги, соответствующие данной ситуации, и восстанавливается нормальная работа КТС.

Для обнаружения аномалий в КТС с помощью самообучающей системы, основанной на искусственном интеллекте, необходимо выполнить следующие шаги:

- выбор системы искусственного интеллекта;
- разработка автоматизированной системы обнаружения аномалий, выбранных самообучающей системой;
- оценка эффективности обнаружения аномалий разработанной системой.

Для реализации предложенных задач разработана открытая диалоговая система оперативного управления КТС – автоматизированная система CTNOCAS (**C**orporative**T**elecommunication **N**etworks **O**perative **C**ontrol **A**utomated **S**ystem), обобщенная структура которой приведена на рис. 6.

АвтоматизированнаясистемаCTNOCASоперативногоуправленияКТСсостоитизс ледующихподсистем: **CTNOCAS.Learn, CTNOCAS.Analize, CTNOCAS.Alert, CTNOCAS.Admin** (рис. 6).

Подсистема CTNOCAS.Learn ответственна за организацию процесса обучения на основе данных, полученных из разных входных источников. Процесс обучения в развернутом виде представлен на рис.7. В автоматизированной системеCTNOCAS обучение выполняется на основе сигналов, поступающих со стороны узла управления операциями. Данный узел находится в постоянной связи с инструментами моделирования и системами мониторинга, внедренными в эксплуатационную сеть.

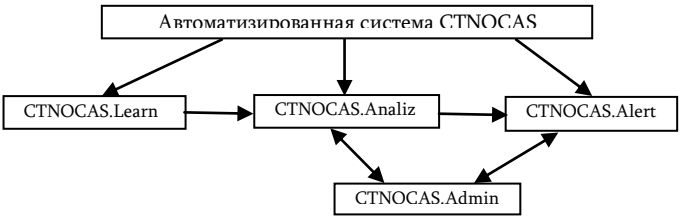

Рис. 6. Структура автоматизированной системы CTNOCAS

После получения новых данных узел управления операциями записывает их в базе данных.

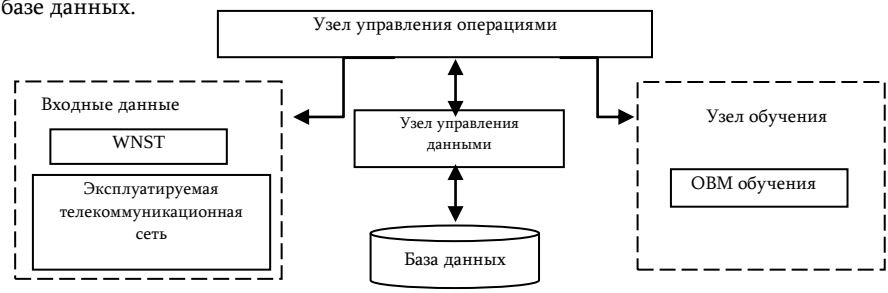

Рис. 7. Процесс обучения CTNOCAS.Learn

Запись и считывание данных в базе выполняются впомощью узла управления данными.Поскольку узел управления операциями не имеет непосредственного доступа к базам данных, то это придает автоматизированной системе CTNOCASопределенную гибкость. Благодаря тому, что работа с данными выполняется отдельным подузлом, становится возможным с легкостью менять базу данных или ее структуру, не влияя на работу основной системы.

При структурных или технологических изменениях в базе данных меняется только узел управления данными, интерфейс работы узла управления операциями изменению не подлежит.

Подсистема **CTNOCAS.Analize** отвечает за анализ данных, поступающих из обучающей системы, и при обнаружении аномалии подсистема CTNOCAS.Alert сообщает об этом администратору. Подсистема CTNOCAS.Alert может отправлять администратору сигналы посредством текстовых сообщений, электронной почты или телефонного звонка.

Подсистема **CTNOCAS.Admin** предназначена для администратора системы, обслуживающего КТС, для управления и обработки сигналов, поступающих от него. Именно с помощью этой подсистемы выполняется оперативное управление сетью. Структура подсистемы **CTNOCAS.Admin** приведена на рис.8.

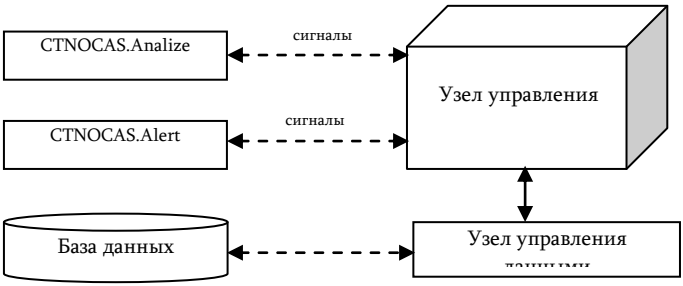

Рис. 8. Структура подсистемы CTNOCAS.Admin

Подсистема**CTNOCAS.Admin**находится в постоянной связи с подсистемами **CTNOCAS.Analize**и**CTNOCAS.Alert**, с которыми непрерывно обменивается управляющими сигналами. Узел управления данными ответственен за запись данных в базу и, при необходимости, за чтение и передачу данных узлу управления с помощью запросов. Как и в случае с **CTNOCAS.Learn,**отдельная подсистема управления данными позволяет хранить их в любой удобной среде и, при необходимости, с легкостью менять среду хранения.

В базе данных хранятся решения, используемые администратором для разных задач, и показана степень веса эффективности каждого из них, которые обновляются при появлении однотипных задач.

Работа администратора, реализующего оперативное управление КТС и подсистемы CTNOCAS.Admin, организована в виде веб-интерфейса, что позволяет применять систему с любого устройства, имеющего доступ в сеть, например, персональных компьютеров, ноутбуков, планшетов и смартфонов.

Автоматизированная система CTNOCAS,будучи открытой, с легкостью интегрируется в автоматизированную систему проектирования сетей WNST (**W**eb

based **N**etwork **S**imulation **T**ool).Структура обучения работы КТС в разных режимах посредством систем CTNOCAS и WNST приведена на рис. 9.

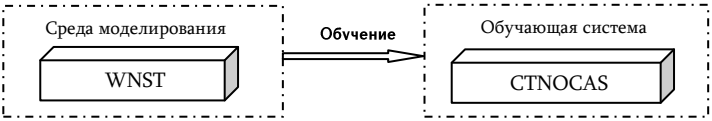

Рис. 9. Структура обучения работы КТС в разных режимах посредством CTNOCAS и WNST

WNST применяется в обучающей подсистеме CTNOCAS, что позволяет легко проектировать телекоммуникационную сеть и моделировать ее работу не только в условиях нормальной эксплуатации.Применение WNST в автоматизированной системе CTNOCAS позволяет также моделировать работу сети в таких ситуациях, как DdoS атаки, неисправности устройств телекоммуникационной сети, увеличение нагрузки и т.д.

В четвертой главе представлены результаты применения и внедрения разработанных методов. Разработанная открытая диалоговая автоматизированная система CTNOCAS позволяет не только увеличить количество симуляторов, эмуляторов и т.д., работающих с системой, но и заменить существующие симуляторына другие, совместимые с CTNOCAS.

Диалоговая автоматизированная система CTNOCAS имеет архитектуру клиент-сервер, где часть клиента реализуется в виде веб-системы.

При разработке CTNOCAS была применена технология .NET Core фирмы Microsoft.Для реализации веб-системы использована технология ASP.Net Core, а для хранения данных системы - технологияMSSQL Server. Системы применены как для операционной системы Microsoft Windows, так и для Red Hat Enterprise и Ubuntu семейства Linux.

Автоматизированная система CTNOCAS оперативного управления КТС внедрена в ООО “Онлайначурд” и в российском ООО“ОМС”.

CTNOCAS используется вООО “Онлайначурд” для обнаружения проблем в КТС и оперативного управления сетью. Учитывая тот факт, что организация занимается онлайн-аукционом, важно, чтобы КТС всегда была в рабочем состоянии, а при появлении неполадок они решались бы в минимальное время. С помощью диалоговой автоматизированной системы CTNOCAS создана модель КТС ООО “Онлайначурд”, на которой смоделированы всевозможные состояния разных типов неполадок. Для КТС ООО “Онлайначурд”определены значения нагрузок для нормальной и загруженной работы сети по времени суток. В рабочие дни наибольшая нагрузка сети бывает в вечернее время суток, что наглядно показанона рис. 10.

Рис.10.Значения нагрузок для нормальной и загруженной работы сети по времени суток для КТС ООО “Онлайначурд”

В нерабочее время сеть наиболее загружена в дневное и вечернее время, как показано на рис. 11.

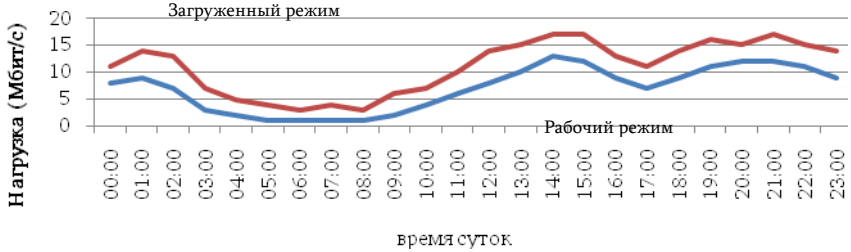

Рис.11. Значения нагрузок для нормальной и загруженной работы сети по времени суток в нерабочее время для КТС ООО “Онлайначурд”

Для КТС ООО “Онлайначурд” смоделированы многочисленные случаи ненормальной работы сети, в частности - увеличение загруженности сети, обусловленное большой активностью посетителей, что не присущедля данного времени суток. Нарис. 12 приведено изменение загруженности КТС данной организации в нерабочий день, что обусловлено изменением количества посетителей.

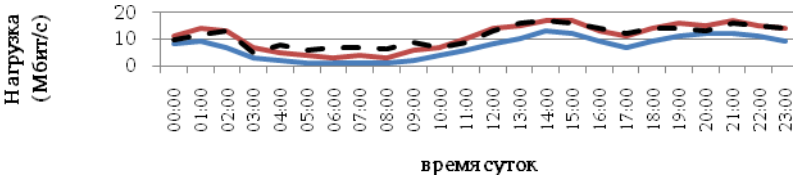

Рис.12. Изменение загруженности КТС ООО “Онлайначурд” в нерабочий день, обусловленное изменением количества посетителей

На рис.12 новая загруженность приведена пунктирной линией.
С помощью автоматизированной системы CTNOCASпутем оперативного управления телекоммуникационными сетями стало возможным обнаружение повышения загруженности сети для 97% случаев.

Предпринятые со стороны администратора соответствующие меры вносятся в систему, после чего при моделировании подобных случаев предлагаются решения.

ООО “ОМС” состоит из 35 отделений. Оно предлагает многочисленные услуги другим организациям, в частности, обслуживание инженерного оборудования, обслуживание инфраструктур сооружений, услуги по безопасности и т.д. Организацияимеет крупнуюКТС, с помощью которой проводится обслуживание ее отделений и предоставляются многочисленные услуги, по которым возможны управления удаленными объектами.

Автоматизированная система CTNOCAS оперативного управления КТС внедрена в ООО“ОМС” и применяется для ее оперативного управления. Представлена рабочая загруженность КТС, применяемая для организации дистанционного обслуживания системы безопасности одного из сооружений со стороны головного отделения.

В обслуживающей организации имеютсясистемы видеонаблюдения, многочисленные датчики, противопожарные системы. Графики загруженности для рабочих и нерабочих дней приведены на рис.13 и 14.

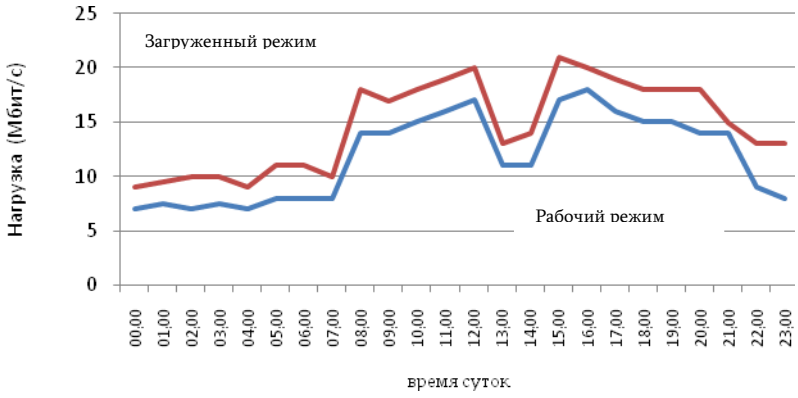

Рис.13. Загруженность КТС ООО “ОМС” по времени суток рабочего дня

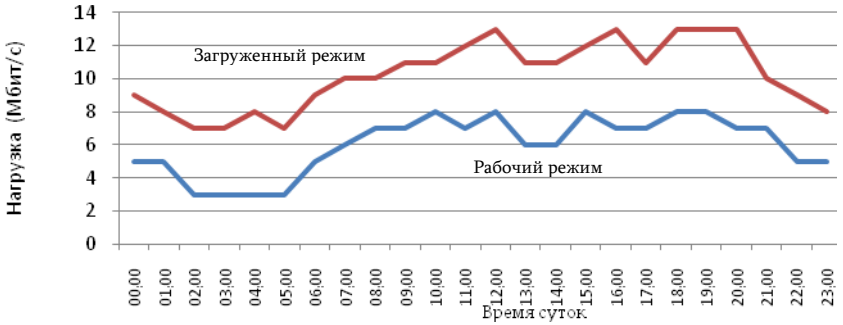

Рис.14. Загруженность КТС ООО "ОМС" по времени суток нерабочего дня

Для данной КТС смоделирована DdoSатака, целью которой являетсярасстройство системы безопасности обслуживания сети. ПосредствомDdoS атаки нагрузка сети резко увеличивается. Эти увеличения заблаговременно обнаруживаются с помощью автоматизированной системы CTNOCAS, и в результате предпринятых администратором мер восстанавливается нормальная работа сети. Подобные расстройства легко обнаруживаются, т.к. при них значительно увеличивается нагрузка сети.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Обоснована необходимость использования системы управления безопасностью сетей, предлагаемой для решения задач оперативного управления КТС, которая обеспечивает надежность работы сетей и проводит сканирование потоков[1,2,6].
2. Из методов искусственного интеллекта для обнаружения аномалий в КТС наиболее оптимальным является векторный метод, т.к. он дает более высокие результаты для обнаружения аномалий в сети [3, 4, 8].
3. Спроектирована система обнаружения аномалий в КТС с помощью машинного обучения[9].
4. Разработана автоматизированная диалоговая система CTNOCAS (**C**orporative **T**elecommunication **N**etworks **O**perative **C**ontrol **A**utomated **S**ystem) с открытой архитектурой, которая работает с автоматизированной системой WNST для проектирования сетей[5, 7].
5. Разработанная автоматизированная система CTNOCAS имеет открытую архитектуру,которая позволяет не только увеличить количество совместимыхсимуляторов, но и заменить существующие симуляторы на другие, совместимые с CTNOCAS[9].

Основные результаты диссертационной работы опубликованы в следующих научных статьях:

1. Սարգսյան Գ.Հ., Հովհաննիսյան Ծ.Ս. Ցանցի կառավարման ծրագրային միջոցների վերլուծություն և ցանցային տրաֆիկի բաշխումը Լինուքս օպերացիոն համակարգում // ՀՊՃՀ Լրաբեր. Գիտական հոդվածների ժողովածու.- Երևան: Ճարտարագետ, 2011. - էջ 241-248:
2. Պետրոսյան Ա.Հ., Հովհաննիսյան Ծ.Ս., Մանուկյան Հ.Մ. Միասնական տրանսպորտային վիրտուալ ցանցի ստեղծման հնարավորությունը և նպատակահարմարությունը // ՀՊՃՀ Լրաբեր. Գիտական հոդվածների ժողովածու.- Երևան: Ճարտարագետ, 2013.–Մաս1.-էջ 163-167:
3. Саргсян Г.О., Оганнисян Ц.С., Торосян Л.Ю. Анализ программ наблюдения трафика сети в режиме реальной работы // Materiały IX Międzynarodowej naukowi-praktycznej konferencji «Wschodnie partnerstwo - 2013».–Przemyśl: Nauka i studia, 2013.-Vol 35. Techniczne nauki.-C. 29-33.
4. Оганнисян Ц.С., Акопян А.А. Анализ программных методов управления трафика в корпоративной сети //Materiały IX Międzynarodowej naukowi-praktycznej konferencji «Wschodnie partnerstwo - 2013».-Przemyśl: Nauka i studia, 2013.- Vol 35. Techniczne nauki.-C.45-49.
5. HovhannisyanTs. The traffic management in different Linux distributive servers in corporative networks for effective routing //Proceedings ofEngineeringAcademy of Armenia. - 2013.- Vol.10, N4. – P.769-773.
6. Հովհաննիսյան Ծ.Ս. Հեռահաղորդակցական ցանցերում անվտանգության դինամիկ կազմակերպումը// ՀԱՊՀԲանբեր. Տեղեկատվական տեխնոլոգիաներ, էլեկտրոնիկա, ռադիոտեխնիկա.– 2015.- N1.- էջ 26-33:
7. Սարգսյան Գ.Հ., Հովհաննիսյան Ծ.Ս., Թորոսյան Լ.Յու. Հեռահաղորդակցության ցանցերում ապարատածրագրային սարքերի կիրառումը բեռնվածության բարելավման համար // ՀՀ ԳԱԱ և ՀԱՊՀ Տեղեկագիր. Տեխնիկական գիտությունների սերիա. -2015. -Հ.68, № 4. -էջ 429-435:
8. Հովհաննիսյան Ծ.Ս., Սիրադեղյան Ս.Ա., Կիրակոսյան Գ.Տ. Հեռահաղորդակցական ցանցերի օպերատիվ կառավարման եղանակի մշակում //Հայաստանի ճարտարագիտական ակադեմիայի Լրաբեր.-2015. -Հատոր 12, N 4. -էջ 718-722:
9. Հովհաննիսյան Ծ.Ս., Սիրադեղյան Ս.Ա., Կիրակոսյան Ռ.Գ. Հեռահաղորդակցական ցանցերում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգի նախագծում // ՀՀ ԳԱԱ և ՀԱՊՀ Տեղեկագիր.Տեխնիկական գիտությունների սերիա. – 2016. -Հատոր 69, N4. -էջ 373-380:

ԾԱՂԻԿՍՏԵՓԱՆԻՀՈՎՀԱՆՆԻՍՅԱՆ

ԿՈՐՊՈՐԱՏԻՎ ՀԵՌԱՀԱՂՈՐԴԱԿՑԱԿԱՆ ՑԱՆՑԵՐԻ ՕՊԵՐԱՏԻՎ ԿԱՌԱՎԱՐՄԱՆ ՄԻՋՈՑՆԵՐԻ ՈՒՍՈՒՑՈՒՄԸ

ԱՄՓՈՓԱԳԻՐ

Թեմայի արդիականությունը: Ժամանակին համընթաց զարգանումենն բարդանում կորպորատիվ հեռահաղորդակցական ցանցերը (ԿՀՑ): Դրանց զարգացմանը նպաստում են նոր տեխնոլոգիաների և սարքավորումների կիրառումը, ԿՀՑ-ի թողունակության և անվտանգության մակարդակի բարձրացումը, կորպորատիվ հեռահաղորդակցական ցանցի օգտատերերի քանակի ավելացումը և այլն: Նման պայմաններում կտրուկ մեծանում է ԿՀՑ-ով անցնող տրաֆիկը: Ցանցի օպերատորների համարհետզհետե դժվարանում է հսկել յուրաքանչյուր հաղորդվող փաթեթի հսկողականգործընթացը:

ԿՀՑ-ներում ինֆորմացիոն հոսքերի ծավալների մեծացման և ոչ արդյունավետ կառավարման կազմակերպման ու իրականացման պատճառով հաճախ տարբեր կազմակերպությունների բնականոն աշխատանքը խաթարվում է, որի հետևանքով կազմակերպությունները կրում են տեղեկատվական և ֆինանսական վնասներ: Նշված տիպի վնասներից խուսափելու համար անհրաժեշտ է մշակել ԿՀՑ-ների օպերատիվ կառավարման միջոցներ, որոնք հնարավորություն կտան հայտնաբերել տեղի ունեցող անոմալիաները և նվազագույնի հասցնել դրանք: Անոմալիաների հայտնաբերումը կիրառվում է անվտանգության, հասանելիության, ծառայության որակի, վիրուսային ծրագրերի հայտնաբերման համար:

Ներկայումս անոմալիաների հայտնաբերման համար մեքենայական ուսուցման համակարգերը լայն կիրառում ունեն տարբեր ոլորտներում, ուստիատենախոսության շրջանակներում կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման միջոցների ինքնուսուցվող համակարգի դիտարկումը և մշակումը արդիական է: Կորպորատիվ հեռահաղորդակցական ցանցում նշված համակարգի ներդրումը հնարավորություն կտա ոչ միայն հայտնաբերել արդեն իսկ հայտնի պատճառներով առաջացող անոմալիաներ, այլ նաև նախկինում չհայտնաբերվածները:

Հետազոտման օբյեկտը: Ատենախոսության հետազոտման օբյեկտը ԿՀՑ-ներն են և դրանց արդյունավետ օպերատիվ կառավարման կազմակերպումն ու իրականացումը:

Գիտական նորույթը: Հետազոտություններից ստացվել են հետևյալ գիտական արդյունքները.

1. Հիմնավորվել էԿՀՑ-ների կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման միջոցների իրականացումը մեքենայական ուսուցման համակարգով, ինչը բարձրացնում է ցանցերի

հուսալիությունը, աշխատունակությունը և շահագործման արդյունավետությունը:

2. ԿՀՑ-ների օպերատիվ կառավարման գործընթացում խնդիրների լուծման արդյունավետությունը բարձրացնելու համար մշակվել է մեթոդ, որի օգտագործման դեպքում յուրաքանչյուր խնդրի համար որոնվում է արդեն գոյություն ունեցող լուծումներից այն միակը, որն արդեն հաջողությամբ կիրառվել և փորձարկվել է:
3. Մշակվել ԷԿՀՑ-ների կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման համար ինքնուսուցվող համակարգի միջոցով անոմալիաների հայտնաբերման ալգորիթմը:
4. Մշակվել է ԿՀՑ-ների կորպորատիվ հեռահաղորդակցական ցանցերի օպերատիվ կառավարման միջոցների համար ցանցերում անոմալիաների արագ հայտնաբերման և մշակման ավտոմատացված բաց երկխոսային համակարգ, որի կիրառումը բարձրացնում է ցանցի հուսալիությունը, աշխատունակությունը, շահագործման արդյունավետությունը և նվազեցնում է ծանրաբեռնվածությունը:

ԱՏԵՆԱԽՈՍԱԿԱՆ ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

1. Հիմնավորվել է ԿՀՑ-ների օպերատիվ կառավարման խնդիրների լուծման համար առաջարկվող ցանցերի անվտանգության ղեկավարման համակարգի օգտագործման անհրաժեշտությունը, որն ապահովում է ցանցերի աշխատանքի հուսալիություն և կատարում է հոսթերի սկանավորում [1,2,6]:
2. ԿՀՑ-ներում անոմալիաների հայտնաբերման արհեստական բանականության մեթոդներից պետք է կիրառել հենասյունային վեկտորային մեթոդը, քանի որ այն տալիս է ցանցերի համար անոմալիայի հայտնաբերման ավելի բարձր արդյունք[3, 4, 8]:
3. Նախագծվել է ԿՀՑ-ում մեքենայական ուսուցման միջոցով անոմալիաների հայտնաբերման համակարգը[9]:
4. Մշակվել է ԿՀՑ-ների օպերատիվ կառավարան երկխոսային CTNOCAS (CorporativeTelecommunication Networks Operative Control Automated System) բաց ճարտարապետությամբ ավտոմատացված համակարգը, որն աշխատում է ցանցերի նախագծման WNST ավտոմատացված համակարգի հետ[5, 7]:
5. Մշակված CTNOCAS ավտոմատացված համակարգն ունի բաց ճարտարապետություն, որը թույլ է տալիս ավելացնել ոչ միայն համատեղելի սիմուլյատորների քանակը, այլ նաև փոխարինել արդեն գոյություն ունեցող սիմուլյատորները CTNOCAS-ի հետ համատեղելի այլ սիմուլյատորներով [9]:

TSAGHIK STEPAN HOVHANNISYAN
DEVELOPING TOOLS FOR OPERATIONAL MANAGEMENT OF CORPORATE TELECOMMUNICATION NETWORKS

Urgency of investigation. Corporate telecommunication networks (CTN) continue to develop. Development is happens due to application of new technologies and equipment, the increase of the CTNs throughput and security level, the increase of users of corporate telecommunication network etc. In such conditions, traffic in corporate telecommunication networks is growing rapidly. For nerwork operators it is becoming very hard to control each transferred packet.

Sometimes, thenormal operation of different organizations is distorted because of the increase in information flows and inefficient implementation and management of CTNs, and, as a result, organizations bear financial and information losses. To avoid such losses there is a need to develop tools for operative management of corporate telecommunication networks which will allow to detect anomalies in networks and to minimizer them. In order to avoid such cases there is a need to develop mechanisms which will allow to detect anomalies occurring inside telecommunicaton corporate networks and to carry out preventive and recovery actions. Recently, anomaly detection in telecommunication networks is widely in discussed in sciientific and commercial areas. Anomaly detection is used for detecting security, availability, service quality, malware detection issues.

For normal operation of telecommunication networks and for providing the required level of the service quality, it is necessary not only to have information about the current state of the network, but also to be able to predict it. At present, machine learning systems fora anomaly detection are widely used in different areas, hence the examination and development of self-learning system for operative management of corporate telecommunication networks in the scope of dissertation is actual. Integration of this system into corporate telecommunication network will allow not only to identify anomalies, which arise because of known reasons but also those which hadn't been detected previously.

The goal of investigation. The objects of the dissertation are CTNs, and the organization and implementation of their effective operative management.

The scientific novelty

As a result of the research, the following scientific results are obtained:

1. The implementation of the computer-aided learning system for the operational control of the CTN has been substantiated, which increases the reliability, and efficiency of the network operation;

2. A method to improve the efficiency of solving problems in the process of operational management of the CTN has been developed, by using which, for each task, the only existing solution that has already been successfully applied and tested, will be applied;

3. An algorithm for detecting anomalies through a self-learning system for the operational management of the CNT has been developed;

4. An open interactive automated system for the rapid detection and processing of anomalies in the network for CTNs, operative management tools are developed. The use of this system increases the reliability, efficiency of the network operation, and reduces its congestion.

The main results and conclusions

1. The necessity of using the network security management system proposed for solving the tasks of the operational control of the CTN, which ensures the reliability of the networks, and conducts the scanning of the flows is justified[1,2,6].

2. From the methods of artificial intelligence for detecting anomalies in the CTN, we need to apply the support vector method, because it yields better results for the detection of anomalies in the network[3, 4, 8].

3. A system for detecting anomalies in the CTN which uses machine learning has been designed[9].

4. An automated interactive CTNOCAS (**C**orporative**T**elecommunication **N**etworks **O**perative **C**ontrol **A**utomated **S**ystem)system is developed, which has an open architecture, and for network design works with WNST,-an automated system[5, 7].

5. The developed automated CTNOCAS system has an open architecture which is allowing not only to increase number of supported simulators, but also replace existing simulators with others which are compatible with CTNOCAS.[9].

ՏՊԱՔԱՆԱԿԸ՝ 100 ՕՐԻՆԱԿ