МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
(СибГУТИ)

УРАЛЬСКИЙ ТЕХНИЧЕСКИЙ ИНСТИТУТ СВЯЗИ И ИНФОРМАТИКИ (ФИЛИАЛ) в г. ЕКАТЕРИНБУРГЕ
(УрТИСИ СибГУТИ)

УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ (УрГУПС), г. ЕКАТЕРИНБУРГ

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР), г. ТОМСК

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОГНИТИВНАЯ ЭЛЕКТРОСВЯЗЬ

Сборник научных трудов IX Всероссийской научно-практической конференции

Екатеринбург
2023

Научные направления конференции:

- **Инфокоммуникационные технологии и системы связи**
- **Современные технологии передачи информации**

Партнёры:

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

СибГУТИ

СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ (СибГУТИ), г. НОВОСИБИРСК

ТУСУР | TUSUR UNIVERSITY

Томский государственный университет систем управления и радиоэлектроники

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР), г. ТОМСК

УрГУПС

Уральский государственный университет путей сообщения

УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ (УрГУПС), г. ЕКАТЕРИНБУРГ

УДК 378+621.391
ББК 74.58 + 32.88-01
Информационные технологии и когнитивная электросвязь. IX Всероссийская научно-практическая конференция;
Сб. науч. ст. в 1 т. / Под ред. Шувалова В.П.;
Сост.: М.П. Карачарова
УрТИСИ СибГУТИ, 2023. 191 с.

В сборник включены доклады, выполненные в рамках IX Всероссийской научно-практической конференции «Информационные технологии и когнитивная электросвязь» по актуальным научным направлениям совершенствования и перспективного развития современных инфокоммуникационных технологий и систем связи, информационной безопасности, информационных технологий и защите информации.

Материалы статей, вошедшие в сборник, даны в авторской редакции.

Представленный сборник предназначен для научных работников, аспирантов, студентов и специалистов, работающих в области современных инфокоммуникационных технологий.

Сборник включен в национальную библиографическую базу данных научного цитирования РИНЦ.

Научное издание
Рецензирование: к.т.н., доцент Н.В. Будылдина; ст. преподаватель кафедры ИТиМС Д.А. Овчинников
Оформление: М.П. Карачарова
Подписано в печать 25.05.2023.
Вышло в свет 13.06.2023.
620109, Россия, г Екатеринбург, ул. Репина, д. 15

СОДЕРЖАНИЕ

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ИНФОРМАЦИИ

СЕКЦИЯ 1. ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ

Е.А. Арефьева, А.М. Кобелев, С.А. Титов

АНАЛИЗ АВАРИЙНЫХ СИТУАЦИЙ НА СЕТЯХ СОТОВОЙ СВЯЗИ

Уральский институт Государственной противопожарной службы
Министерства Российской Федерации по делам гражданской обороны,
чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Россия

Ключевые слова: система связи, базовая станция, анализ аварий, основные причины.

В статье приведен анализ аварийных ситуаций на базовых станциях сотовой связи, выделены основные причины. Рассмотрено возможное негативное влияние станций на окружающую среду и организм человека. Представлены различные способы мониторинга и обнаружения нарушений.

E.A. Arefeva, A.M. Kobelev, S.A. Titov

ANALYSIS OF EMERGENCY SITUATIONS ON CELLULAR NETWORKS

Ural Institute of the State Fire Service Ministry of the Russian Federation for Civil Defense,
Emergency Situations and Elimination of Consequences of Natural Disasters, Russia

Keywords: communication system, base station, accident analysis, root causes

The article provides an analysis of emergency situations at cellular base stations, highlights the main causes. The possible negative impact of stations on the environment and the human body is considered. Various methods for monitoring and detecting violations are presented.

В современном мире мобильная связь обеспечивает передачу текстовых, голосовых и других сообщений между передвигающимися абонентами. Обмен данными и сигналы на разных частотах происходит через специальные базовые станции, которые располагаются на земле или крышах строений. С помощью беспроводных маршрутизаторов, радиосигнал передается от станции к абоненту, что и дает возможность связаться с человеком на любом расстоянии.

Базовая станция – это центр соты, создающая регламентированную зону обслуживания и обеспечивающая передачу данных. Сама базовая станция – это комплекс из антенн, радио модуля и блока питания. Антенны – это обязательный элемент устройства, они принимают и передают сигнал, а также, от них зависит качество мобильной связи, радио модуль усиливает и обрабатывает сигнал, а электроэнергией снабжает блок питания. Антенны располагают на зданиях, возвышенных местностях или вышках до 300 метров [4].

Для связи с сетью (соседними станциями) проводят оптоволокно, в случае, когда это затруднительно, дополнительно устанавливается антенна релейной связи, которая напоминает спутниковые антенны.

Рисунок 1. Базовая вышка сотовой связи

Проведя анализ аварий, связанных с вышками сотовой связи, можно заметить, что они происходят довольно часто и имеют множество различных причин [5].

Например, аварии, связанные с погодными и климатическими условиями, по количеству являются наиболее вероятным.

Так, 7 ноября 2021 года на Сахалине упала вышка сотовой связи, установленная на крыше здания, из-за сильного порывистого ветра. Пострадавших от падения металлической конструкции нет, но часть жителей города остались без связи.

3 августа 2021 года по той же причине сильного порыва ветра в Старошайговском районе упала вышка сотовой связи с обрывом троса, расположенная в населенном пункте (Рис. 2). Пострадавших нет.

Рисунок 2. Последствия падения вышки сотовой связи

Также, отмечены случаи нарушения работы вышек на производственных предприятиях.

Например, случай пожара 14-15 февраля 2003 года в здании Замоскворецкого телефонного узла, причиной которого стало «попадание высокого напряжения на оборудование абонентских номеров вследствие возгорания кабеля электропитания», без связи осталось примерно 40 тысяч жителей. Во время этого на вышке находились рабочие, после падения ими были получены смертельные травмы.

Также, вероятными причинами нарушений работы сотовых станций являются взрывы климатических телекоммуникационных шкафов (Рис. 3). Такие шкафы представляют собой неразборную конструкцию, внутри которой установлена стойка для оборудования, система кондиционирования и датчиков [1].

Рисунок 3. Последствия взрыва климатического телекоммуникационного шкафа

В связи со сложившейся ситуации в стране, отмечены нарушения работы базовых сотовых станций по причине диверсий и террористических атак.

В ходе специальной военной операции в Херсонской области обстрелы со стороны войск украинской армии вызвали масштабные аварии на магистральной сети, в результате которых были разрушены основные узлы связи. Без мобильной связи остались более 500 тысяч абонентов.

А в приграничном районе Брянской области на вышку сотовой связи беспилотником была сброшена граната, но на высоте 80 метров боеприпас был успешно обезврежен и взрыва удалось избежать.

Крое того, по мнению жителей, вред от вышек сотовой связи намного больше, чем польза. Считается, что излучение от вышек, расположенных рядом с домом влияет на человека и может привести к негативным последствиям в виде болезней или патологий различных органов [3].

Примером этого можно рассмотреть случай, когда россиянин самостоятельно деформировал опору вышки сотовой связи, излучение которой, по его мнению, негативно влияло на урожай, находившийся на его участке, расположенном недалеко от вышки.

По подтверждениям Всемирной организации здравоохранения и множеству научных исследований негативного влияния сигнала сотовых сетей на организм человека не обнаружено, радиоволны для человека не несут опасности, они не влияют на ДНК и мутации клеток. Также, санитарные службы проверяют возможную суммарную мощность электромагнитного поля перед установкой базовой станции, после чего выдается разрешение на строительство.

Таким образом, в статье проведен анализ аварий, связанных с нарушениями работы вышек сотовой связи, выявлены основные причины их возникновения: плохие погодные условия, нарушения эксплуатации оборудования, следствие нештатных ситуаций на производствах и взрывы телекоммуникационных климатических шкафов. Базовые станции, как и любое оборудование, требуют периодического обслуживания и профилактики. Для обнаружения нарушений применяется дистанционная система мониторинга оборудования, что позволяет своевременно узнать о поломке. Для мониторинга общей работы сотовых сетей существует специальная мобильная аппаратура, которая позволяет проводить оценку качества сигнала. Также, мониторинг сетей компании осуществляют с помощью имитатора базовой станции. Его используют для поиска, идентификации и обнаружения нарушений, а также прослушивания абонентов сотовой связи [2].

Список литературы:

1. Бабков В.Ю., Цикин И.А. Сотовые системы мобильной радиосвязи: учеб. пособие. СПб. БХВ-Петербург, 2013. 433 с.
2. Березкин Е.Ф. Надежность и техническая диагностика систем: Учебное пособие. М.: НИЯУ МИФИ, 2012. С. 244. сертации на соискание ученой степени кандидата технических наук. Москва. 2009
3. Гришин Ю.П., Ипатов В.П., Казаринов Ю.М. Радиотехнические системы: Учеб. для вузов по спец. "Радиотехника". М.: Высш. шк., 1990. 496с.
4. Тай За У. Антенные системы базовых станций сотовой связи третьего поколения. Автореферат.
5. Терентьев Д. Аварии на объектах связи. Первая миля. 2011.

П.И. Артемьев, И.А. Осипова

РАЗЛИЧИЯ И ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ РЕЛЯЦИОННЫХ И ГРАФОВЫХ БАЗ ДАННЫХ В СОВРЕМЕННЫХ ПРИЛОЖЕНИЯХ СОЦИАЛЬНЫХ СЕТЕЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО
«Сибирский государственный университет телекоммуникаций и информатики»в
г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: реляционные базы данных, графовые базы данных, социальные сети, базы данных, сравнительный анализ, разработка приложений, модели данных, хранение данных, обработка данных

Были рассмотрены вопросы о различиях и преимуществах использования реляционных и графовых баз данных в разработке приложений социальных сетей. В статье были описаны особенности каждого типа баз данных, а также был проведен сравнительный анализ. Были проанализированы примеры успешного применения графовых баз данных в приложениях социальных сетей, что подчеркнуло их значимость в данной области.

P.I. Artemev, I.A. Osipova

DIFFERENCES AND ADVANTAGES OF USING RELATIONAL AND GRAPH DATABASES IN MODERN SOCIAL NETWORKING APPLICATIONS

Ural Technical Institute of Communications and Informatics (branch)
"Siberian State University of Telecommunications and Informatics" in
Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: relational databases, graph databases, social networks, databases, benchmarking, application development, data models, data storage, data processing.

Questions were addressed about the differences and benefits of using relational and graph databases in the development of social networking applications. The article described the features of each type of database, and also carried out a comparative analysis. Examples of successful application of graph databases in social networking applications were analyzed, which emphasized their importance in this area.

Введение

В современном мире базы данных играют важную роль в обработке и хранении информации. Реляционные базы данных являются одним из наиболее распространенных типов баз данных и используются во многих сферах, включая банковское дело, управление персоналом и торговлю. В то же время, графовые базы данных, которые используют графовую модель данных, набирают популярность благодаря своей способности хранить и обрабатывать связи между данными.

Одной из ключевых особенностей приложений социальных сетей является хранение и обработка связей между пользователями и другими объектами, такими как сообщения, фотографии и т.д. Поэтому, выбор оптимального типа базы данных играет важную роль в разработке эффективных и масштабируемых приложений социальных сетей. В данной статье мы рассмотрим, какие типы баз данных наиболее подходят для решения задач, связанных с хранением и обработкой связей в приложениях социальных сетей.

Обзор современных приложений социальных сетей и их особенности в контексте баз данных.

Современные приложения социальных сетей стали частью повседневной жизни многих людей и представляют собой сложные системы, которые обрабатывают огромные объемы данных. Они позволяют пользователям создавать профили, находить друзей, обмениваться сообщениями, публиковать фотографии, просматривать новости и многое другое.

Одной из особенностей приложений социальных сетей является необходимость хранения и обработки связей между пользователями и другими объектами [6]. Эти связи могут быть представлены в виде графа, где узлами являются пользователи и объекты, а ребрами - связи между ними. Например, связь между пользователями может быть представлена в виде "друзей", "подписчиков" и т.д., а связь между пользователем и фотографией может быть представлена в виде "лайков", "комментариев" и т.д.

Для хранения и обработки таких связей в приложениях социальных сетей могут использоваться различные типы баз данных, включая реляционные и графовые базы данных. Каждый тип базы данных имеет свои преимущества и недостатки, и выбор конкретного типа базы данных зависит от конкретных задач и требований приложения. В следующих разделах мы рассмотрим различия и преимущества реляционных и графовых баз данных в контексте приложений социальных сетей.

Основные различия между реляционными и графовыми базами данных и их влияние на разработку приложений социальных сетей.

Реляционные и графовые базы данных имеют существенные различия в своей структуре и способе организации данных. В реляционной базе данных данные хранятся в виде таблиц, где каждая строка представляет отдельную запись, а каждый столбец представляет отдельный атрибут. В графовой базе данных данные хранятся в виде графа, где каждый узел представляет объект, а каждое ребро - связь между объектами [2].

Одним из основных преимуществ графовых баз данных является их способность эффективно хранить и обрабатывать сложные связи между объектами. Это особенно важно для приложений социальных сетей, где связи между пользователями и другими объектами играют важную роль. Графовые базы данных позволяют быстро находить связи между объектами и выполнять сложные запросы на основе этих связей.

С другой стороны, реляционные базы данных часто используются для хранения и обработки структурированных данных, где связи между объектами не так важны. Одним из преимуществ реляционных баз данных является их широкая поддержка и использование стандартного языка SQL для работы с данными.

Выбор между реляционными и графовыми базами данных в приложениях социальных сетей зависит от конкретных требований и задач приложения. Некоторые приложения могут использовать обе типа баз данных, чтобы оптимизировать различные запросы на основе структуры данных и типа связей.

Преимущества использования графовых баз данных в сравнении с реляционными в современных приложениях социальных сетей.

Графовые базы данных имеют несколько преимуществ по сравнению с реляционными базами данных при работе с данными в приложениях социальных сетей.

Во-первых, графовые базы данных эффективно работают с данными, которые содержат сложные связи между объектами. В приложениях социальных сетей связи между пользователями и другими объектами часто являются сложными и многоуровневыми. Например, в приложении для знакомств пользователи могут иметь различные типы связей между собой, такие как "друзья", "знакомые", "коллеги" и т.д. Графовые базы данных позволяют быстро находить связи между объектами и выполнять сложные запросы на основе этих связей [1].

Во-вторых, графовые базы данных обеспечивают более гибкий подход к хранению и обработке данных. В отличие от реляционных баз данных, где данные хранятся в таблицах с фиксированным количеством столбцов и строк, графовые базы данных позволяют гибко определять связи между объектами и хранить данные в соответствии с этими связями. Это позволяет разработчикам быстро и эффективно изменять структуру базы данных при необходимости.

В-третьих, графовые базы данных обеспечивают более быстрый доступ к данным. В приложениях социальных сетей скорость доступа к данным играет важную роль. Графовые базы данных позволяют быстро находить связи между объектами и выполнять сложные запросы на основе этих связей, что ускоряет обработку данных и повышает производительность приложения.

В-четвертых, графовые базы данных могут быть более легкими и масштабируемыми. Приложения социальных сетей часто имеют миллионы пользователей и огромное количество данных [3]. Графовые базы данных позволяют легче масштабироваться и обрабатывать большие объемы данных, что делает их привлекательным выбором для приложений социальных сетей.

Таким образом, использование графовых баз данных в современных приложениях социальных сетей может быть более эффективным и гибким выбором, особенно при работе с большим объемом связанных данных и необходимостью быстрого доступа к ним. Графовые базы данных обеспечивают удобный способ моделирования сложных отношений между пользователями и объектами, а также позволяют быстро находить пути и анализировать связи между ними. Кроме того, графовые базы данных могут быть более гибкими в изменении структуры данных и обеспечивать более простую масштабируемость. Однако, реляционные базы данных также имеют свои преимущества и могут быть эффективными в определенных случаях. В конечном итоге, выбор между реляционными и графовыми базами данных зависит от конкретных потребностей приложения и особенностей данных, с которыми оно работает.

Примеры успешного использования графовых баз данных в приложениях социальных сетей.

Существует множество примеров успешного использования графовых баз данных в приложениях социальных сетей. Одним из таких примеров является Facebook, который использует графовую базу данных для моделирования отношений между пользователями и объектами, такими как фотографии, сообщения и комментарии. Это позволяет Facebook быстро находить связи между пользователями и показывать более релевантный контент на основе их взаимодействий в социальной сети [4].

Другой пример - LinkedIn, который использует графовую базу данных для поиска наиболее подходящих контактов для пользователей. LinkedIn использует графовую модель для анализа отношений между пользователями на основе их профессиональных навыков, опыта работы и образования, чтобы рекомендовать наиболее подходящих контактов для своих пользователей.

Еще один пример - Twitter, который использует графовую базу данных для моделирования отношений между пользователями на основе их взаимодействий в социальной сети, таких как твиты, ретвиты, лайки и подписки. Это позволяет Twitter быстро находить твиты и пользователей, которые могут быть наиболее интересны для конкретного пользователя, и показывать их в ленте новостей.

Эти примеры показывают, что графовые базы данных могут быть эффективным и мощным инструментом для обработки и анализа сложных связанных данных в приложениях социальных сетей.

Заключение

В заключение, можно сказать, что выбор между реляционными и графовыми базами данных в приложениях социальных сетей зависит от многих факторов, таких как тип данных, объем информации и сложность запросов. В то время как реляционные базы данных хорошо подходят для хранения структурированных данных, графовые базы данных предоставляют более гибкую структуру хранения связей между данными.

Стоит отметить, что графовые базы данных активно применяются в различных приложениях социальных сетей, например, в LinkedIn, Facebook, Twitter и других. Они обеспечивают быстрый доступ к информации, упрощают процесс анализа данных и помогают создавать более точные и интуитивно понятные предложения для пользователей.

Несмотря на то, что графовые базы данных все еще относительно новые в мире разработки приложений социальных сетей, они уже показали свою эффективность и преимущества по сравнению с реляционными базами данных. В будущем мы можем ожидать еще большего применения графовых баз данных в приложениях социальных сетей и их более широкое

использование в других областях.

Список литературы:

1. Робинсон, И., Уэббер, Дж., и Эйфрем, Э. Графовые базы данных. О'Рейли Медиа, Инк. // 2015.
2. Шапошник, Л. Neo4j: база данных Graph для создания интеллектуальных приложений. ООО "Пэкт Паблишинг" // 2018.
3. Дайер, младший. Моделирование графических данных для NoSQL и SQL. Публикации по технике. // 2017.
4. Энглс, Р., и Гутьеррес, К. Обзор графовых моделей баз данных. Вычислительные исследования ACM (CSUR), // 2018. 50-68с.
5. Яно, К., и Китагава, Х. Проектирование и внедрение системы управления базами данных графов. В материалах 2-й Международной конференции по системам баз данных для передовых приложений// 2018. 425-430с.
6. Эйфрем, Э. Графовые базы данных и будущее крупномасштабного управления данными. Сообщения ACM //2018. 44-61с.
7. Зильбершатц, А., Корт, Х.Ф., и Сударшан, С. Понятия системы баз данных. Образование Макгроу-Хилл. // 2019.

Р.И. Баимов, А.Н. Рагозин

ОПТИМИЗАЦИЯ АМПЛИТУДНОГО РАСПРЕДЕЛЕНИЯ НА ЭЛЕМЕНТАХ ЛИНЕЙНОЙ ФАЗИРОВАННОЙ АНТЕННОЙ РЕШЕТКИ В СОСТАВЕ РАДИОПЕЛЕНГАТОРА ИСТОЧНИКА РАДИОИЗЛУЧЕНИЯ

Южно - Уральский государственный университет ФГАОУ ВО "ЮУрГУ (НИУ)", г. Челябинск, Россия

Ключевые слова: фазированная антенная решетка, суммарная диаграмма направленности, разностная диаграмма направленности, амплитудное весовое распределение, радиопеленгатор.

Рассматривается линейная фазированная антенная решетка (ЛФАР) в составе моноимпульсного радиопеленгатора. При моноимпульсном методе пеленгования источника радиоизлучения требуется формировать суммарную и разностную диаграммы направленности (ДН) ЛФАР. В работе проведен выбор наилучшего амплитудного весового окна на элементах ЛФАР по критерию минимизации максимального уровня боковых лепестков суммарной и разностной ДН при минимальном угловом расширении главного лепестка суммарной ДН ЛФАР.

R.I. Baimov, A.N. Ragozin

OPTIMIZATION OF THE AMPLITUDE DISTRIBUTION ON THE ELEMENTS OF A LINEAR PHASED ARRAY ANTENNA AS PART OF A RADIO DIRECTION FINDER OF A RADIO SOURCE

South Ural State University "SUSU (NRU)", Chelyabinsk, Russia

Keywords: phased array antenna, total radiation pattern, difference radiation pattern, amplitude weight distribution, direction finder.

A linear phased array antenna (AFAR) as part of a monopulse direction finder is considered. With the monopulse method of bearing the radio source, it is required to form a total and difference radiation pattern (DN) of the LFAR. The paper selects the best amplitude weight window on the AFAR elements according to the criterion of minimizing the maximum level of the side lobes of the total and difference DN with a minimum angular expansion of the main lobe of the total DN of the LFAR.

Введение:

В настоящее время актуальной задачей является пеленгация (измерение угловых координат) источников радиоизлучения (ИРИ), реализуемая в различных радиотехнических системах, например в угломерных системах посадки летательных аппаратов [1,2].

Задача выбора весового окна амплитудного распределения на элементах линейной фазированной антенной решетки (ЛФАР) по критерию ширина луча – уровень боковых лепестков диаграммы направленности рассмотрена в работе [1]. При моноимпульсном методе пеленгования источника радиоизлучения (ИРИ) требуется формировать суммарную и разностную ДН ЛФАР. Необходимо произвести выбор наилучшего амплитудного весового окна на элементах ЛФАР по критерию минимизации максимального уровня боковых лепестков суммарной и разностной ДН при минимальном угловом расширении главного лепестка суммарной ДН ЛФАР.

Исследование весовых распределений:

Весовые распределения [1,3] в ФАР определяют величину сигналов, которые передаются в каждый элемент антенной решетки. Это позволяет оптимизировать ДН и уменьшить побочные излучения, определяемые боковыми лепестками ФАР.

На рис. 1, 2 и 3 приведены результаты расчётов нормированных суммарной и разностной ДН ЛФАР для используемых в исследовании весовых распределений амплитуд на элементах ЛФАР.

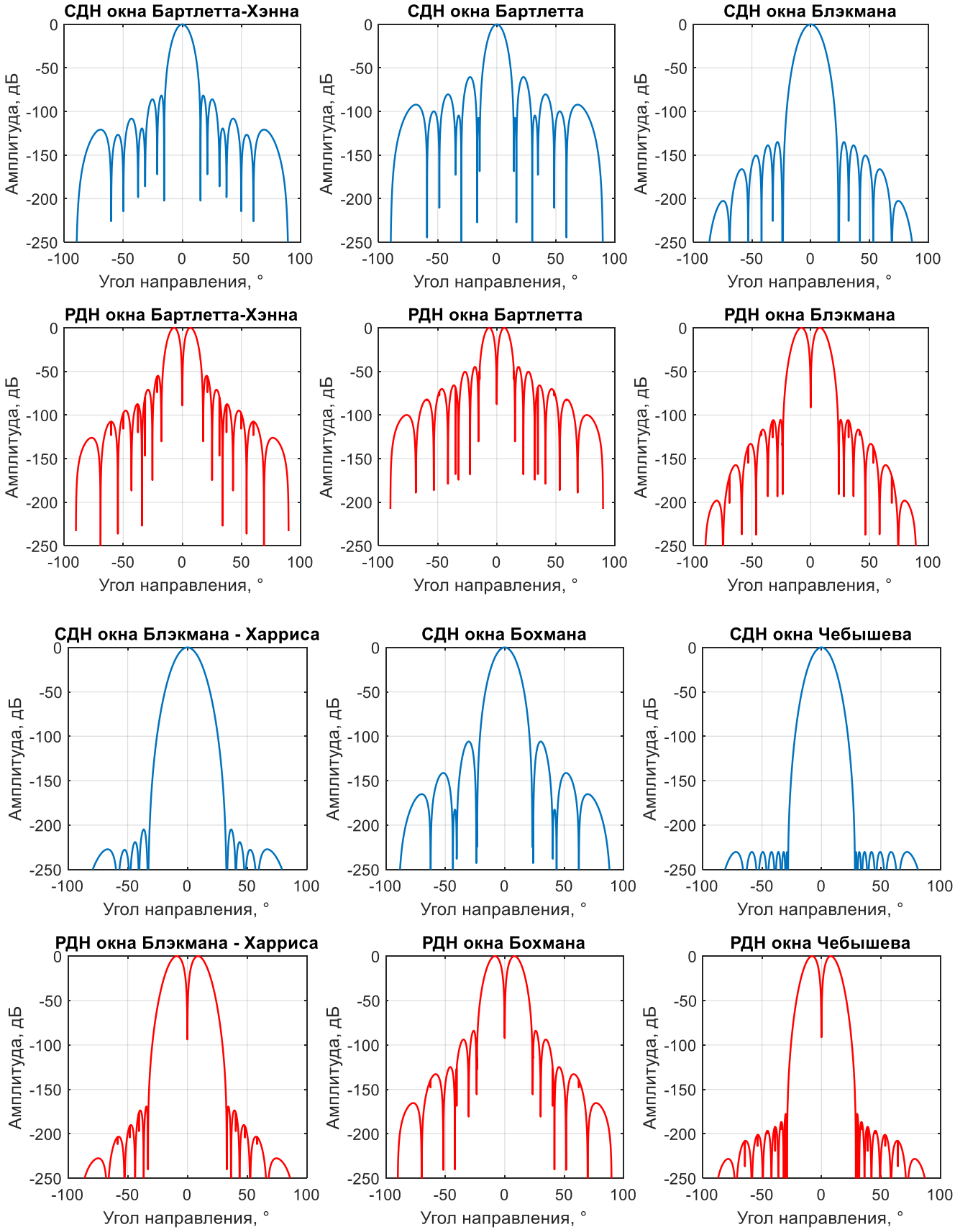


Рис. 1. Суммарная и разностная ДН ЛФАР для различных весовых распределений на элементах ЛФАР

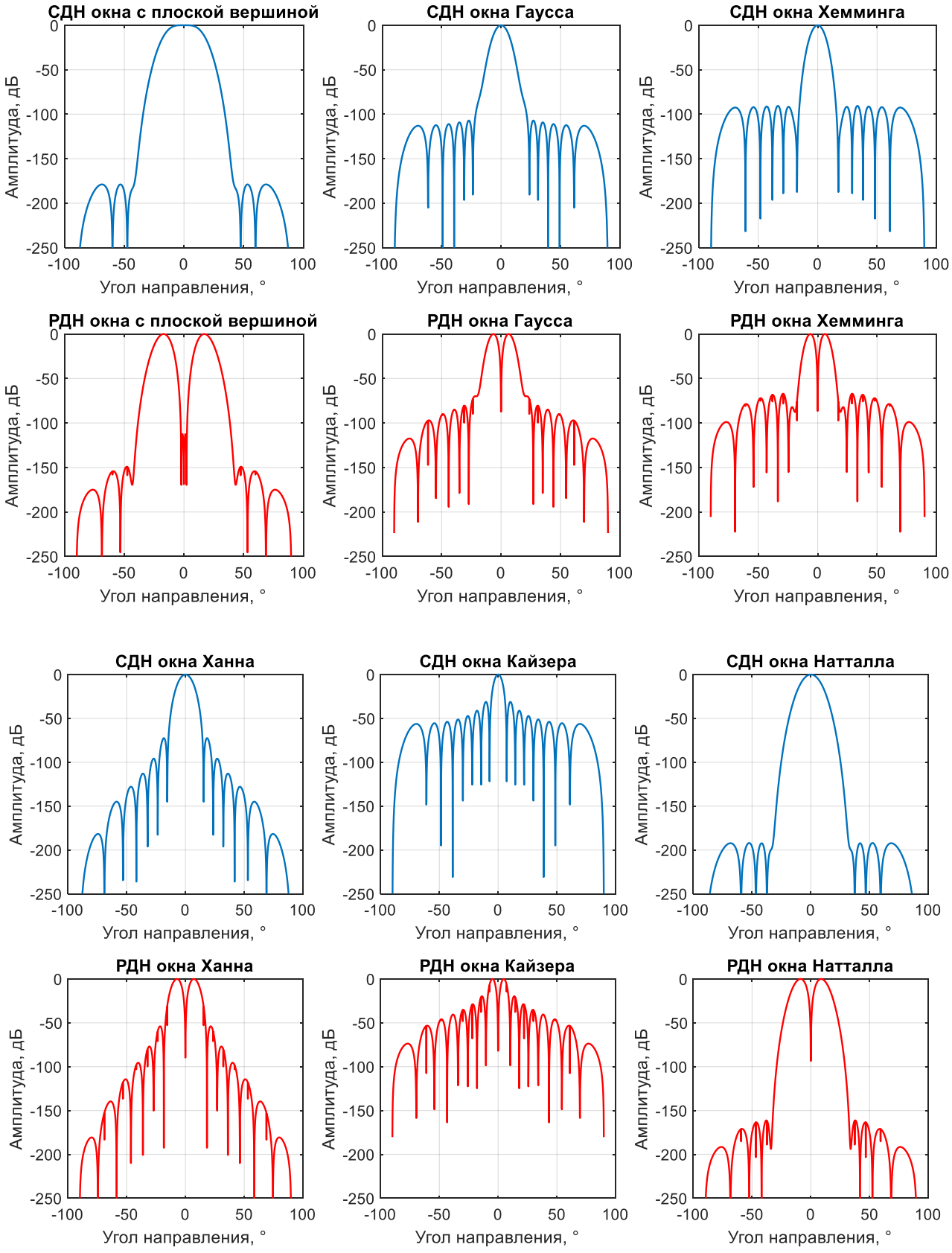


Рис. 2. Суммарная и разностная ДН ЛФАР для различных весовых распределений на элементах ЛФАР

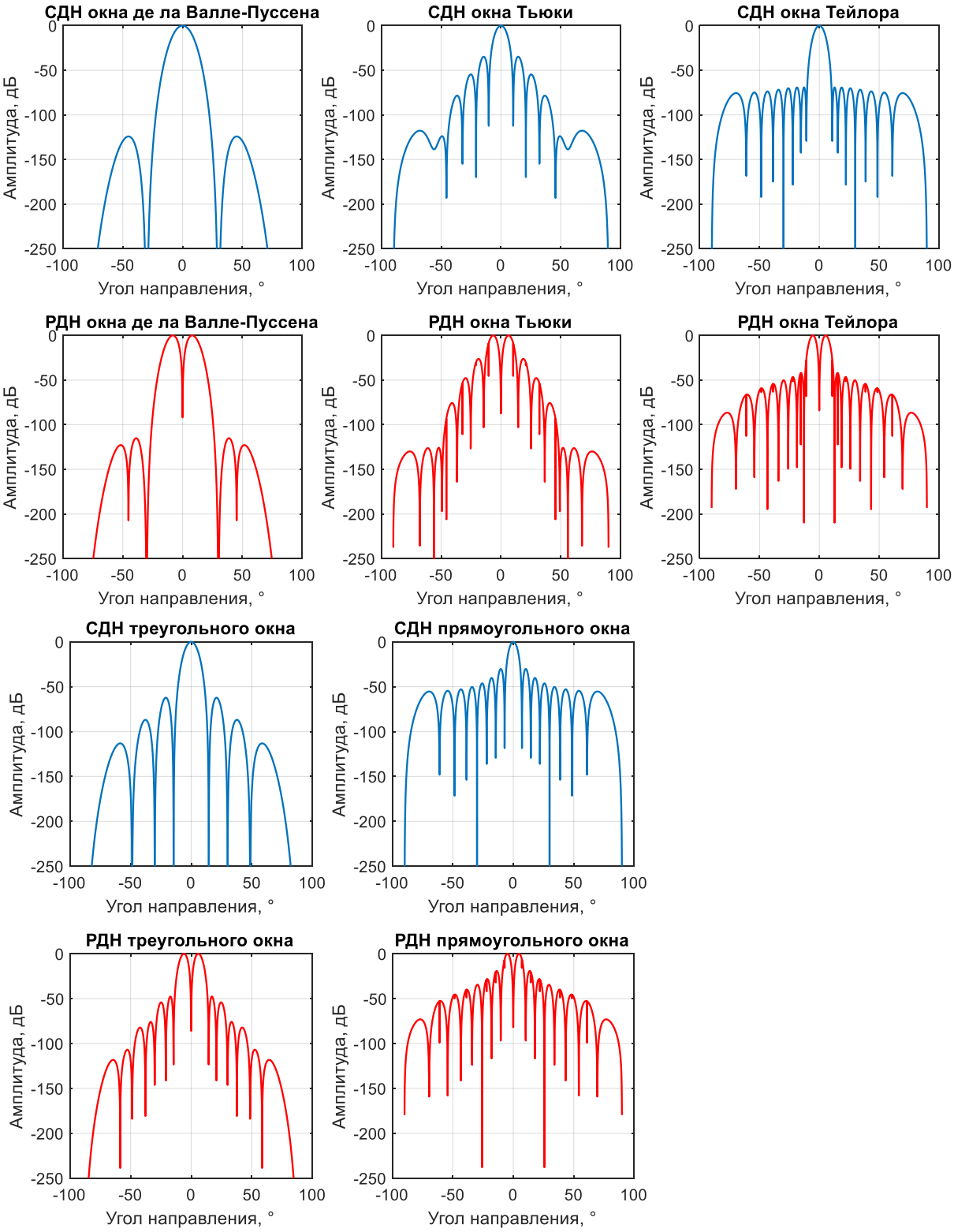


Рис.3. Суммарная и разностная ДН ЛФАР для различных весовых распределений на элементах ЛФАР

Результаты анализа уровней боковых лепестков суммарной и разностной ДН ЛФАР, а также ширины главного лепестка ДН суммарной ЛФАР сведены в таблицу 1.

Таблица 1 — сравнение весовых окон

Весовое окно	Ширина главного лепестка, град.	Уровень боковых лепестков суммарной ДН, дБ	Уровень боковых лепестков разностной ДН, дБ

Бартлетта-Хэнна	30,8	-87,8795	-56,7936
Бартлетта	29	-65,5698	-44,7595
Блэкмана	47,2	-150,168	-106,187
Блэкмана - Харриса	65,8	-211,892	-173,792
Бохмана	46,4	-113,892	-84,3231
Чебышева	57,8	-241,626	-186,715
С плоской вершиной	95	-184,798	-154,249
Гаусса	47,6	-115,23	-85,1014
Хемминга	33,8	-92,6809	-78,1719
Ханна	30,8	-83,9374	-54,1258
Кайзера	14,6	-39,2116	-20,1668
Натталла	74,8	-195,439	-165,78
де ла Валле-Пуссена	59,4	-124,321	-115,107
Тьюки	20,6	-41,3018	-27,132
Тейлора	21,6	-78,8118	-47,9313
Треугольное	29	-69,299	-50,1888
Прямоугольное	14,4	-32,324	-19,377

Заключение: При моноимпульсном методе пеленгования источника радиоизлучения требуется формировать суммарную и разностную ДН ЛФАР. Уровень боковых лепестков суммарной и разностной ДН ЛФАР определяет помехозащищённость моноимпульсного пеленгатора источника радиоизлучения. Ширина главного лепестка суммарной ДН ЛФАР определяет точность и разрешающую способность моноимпульсного радиопеленгатора. В ходе проведённого исследования по результатам, приведённым в таблице 1, показано, что весовое распределение Тейлора реализует критерий минимизации максимального уровня боковых лепестков суммарной и разностной ДН ЛФАР при минимальном угловом расширении главного лепестка суммарной ДН ЛФАР.

СПИСОК ЛИТЕРАТУРЫ:

1. Баимов, Р. И. Выбор весового окна амплитудного распределения на элементах линейной фазированной антенной решетки по критерию ширина луча - уровень боковых лепестков диаграммы направленности / Р. И. Баимов, А. Н. Рагозин // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики : Сборник научных трудов III Международной научно-практической конференции, Екатеринбург, 25–26 января 2023 года / Под редакцией В.П. Шувалова, сост. М.П. Карачарова. – Екатеринбург: Уральский государственный университет путей сообщения, 2023. – С. 72-77. – EDN HMYRDD.
2. Рагозин, А. Н. Определение угловых координат источника радиоизлучения в системах радионавигации / А. Н. Рагозин // НАУКА ЮУрГУ. СЕКЦИИ ТЕХНИЧЕСКИХ НАУК: материалы 74-й научной конференции, Челябинск, 19 апреля 2022 года/ Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет. – Челябинск: Издательский центр ЮУрГУ, 2022. – С. 343-349.
3. Хэррис Ф. Дж. Использование окон при гармоническом анализе методом дискретного преобразования Фурье // ТИИЭР. Т. 66. No 1. Январь 1978.С. 60 – 96

К.А. Батенков

МЕТОДЫ ПОДСЧЕТА КОЭФФИЦИЕНТА ОШИБОЧНЫХ БИТОВ В ЦИФРОВЫХ ТРАКТАХ

РТУ МИРЭА, Россия

Ключевые слова: коэффициент ошибочных битов, события ошибок, битовая ошибка, сбой, цифровая система передач.

Представлено описание трех методов подсчета коэффициента ошибочных битов. Отмечается, что наибольшее распространение в современной практике получил второй метод, однако его применение обычно не обеспечивает автоматического учета точности измерений, что необходимо учитывать при проведении эксплуатационных тестов.

K.A. Batenkov

METHODS FOR CALCULATING COEFFICIENT OF ERRONEOUS BITS IN DIGITAL PATHS

RTU MIREA, Russia

Keywords: error bit rate, error events, bit error, failure, digital transmission system.

The description of three methods for calculating the coefficient of erroneous bits is presented. It is noted that the second method has become the most widespread in modern practice, but its application usually does not automatically account for the accuracy of measurements, which must be taken into account when conducting operational tests.

Существует три способа расчета коэффициента ошибочных битов (рис. *1*).

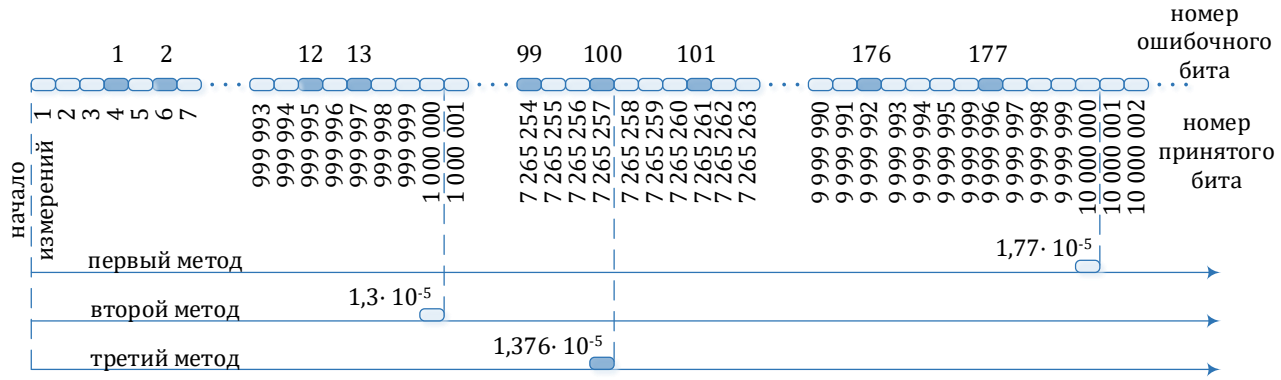


Рис. 1. Методы измерения коэффициента ошибочных битов

В первом методе подсчет коэффициента ошибочных битов производится после приема ста ошибок впервые, что автоматически приводит к высокой точности измерения (лучше 10 %). В тоже время от начала измерения до момента получения итогов необходимо определенное (иногда довольно большое) время: $r_b = \frac{177}{10^7} = 1{,}77 \cdot 10^{-5}$ (рис. *1*).

Во втором методе рассчитывается коэффициент ошибочных битов после начала измерения и количество принятых битовых ошибок не учитывается. В данном случае для точности измерений подсчет коэффициента ошибочных битов выполняется после появления заданного числа битов, а точность измерения обуславливается пороговым значением числа принятых битов. Обычно считается, что точность где-то на порядок больше обратной величины количества анализируемых битов (в примере рис. *1* точность измерения близка по величине к 10^{-5} после первоначального расчета). Этот метод в отличие от первого обеспечивает заданное время

отображения первых результатов измерений, не зависящее от количества ошибок: $r_b = \frac{13}{10^6} = 1{,}3 \cdot 10^{-5}$ (рис. *1*). Подобная методика расчета оказывается наиболее эффективной и имеет широкое распространение. Негативной стороной этой методики является требование учета числа принятых и переданных битов псевдослучайной последовательности в ходе анализа результата. Данное обстоятельство возникает вследствие вычисления отношения без задания точности измерений для произвольного момента времени. Так, при общем числе принятых битов 10^7 точность оценки параметра соответствует 10^{-6}, но даже если прибор отображает меньшие значения, то достоверность не оказывается выше [1, 2].

В третьем методе, применяемом в некоторых индикаторах, расчет коэффициента ошибочных битов выполняется после приема ста ошибочных битов: $r_b = \frac{100}{7265257} = 1{,}376 \cdot 10^{-5}$ (рис. *1*). Данный метод оказывается вариацией первого метода с похожей негибкостью в идентификации результатов эксплуатационных измерений и требованием ожидания до индикации итогов измерений.

В целом, наиболее широко в современной практике используется второй метод, но его применение часто не позволяет автоматически учитывать точность измерений, что необходимо иметь в виду при проведении эксплуатационных промеров [3, 4, 5, 6, 7].

СПИСОК ЛИТЕРАТУРЫ:

1. Батенков К.А. К вопросу оценки надежности двухполюсных и многополюсных сетей связи // Успехи современной радиоэлектроники. 2017. С. 604.
2. Батенков К.А. Моделирование непрерывных каналов связи в форме операторов преобразования некоторых пространств // Труды СПИИРАН. 2014. № 1 (32). С. 171-198.
3. Бакланов И.Г. Методы измерений в системах связи / И. Г. Бакланов. – М. : Эко-трендз, 1999. – 204 с.
4. Винокуров В.М. Цифровые системы передачи : учеб. Пособие / В.М. Винокуров; Федеральное агентство по образованию, Томск. гос. ун-т систем упр. и радиоэлектроники, Ин-т доп. образования, факультет повышения квалификации. – Томск : Томск. гос. ун-т систем упр. и радиоэлектроники, 2012. – 160 с.
5. Нормы на электрические параметры цифровых каналов и трактов магистральной и внутризоновых первичных сетей : Утв. М-вом связи РФ 01.10.96. – М: МК-Полиграф, 1996. – 72 с.
6. Rec. G.707 / Y.1321. Network node interface for the synchronous digital hierarchy (SDH). – 2007–01. – Geneva : ITU-T, 2008. – 196 p.
7. Rec. G.828. Error performance parameters and objectives for international, constant bit rate synchronous digital paths. – 2000–03. – Geneva : ITU-T, 2001. – 24 p.

В.В. Бенцель, Н.В. Будылдина

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТОПОЛОГИЧЕСКИХ РЕШЕНИЙ ДЛЯ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Уральский технический институт связи и информатики (филиал) ФГОБУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: Топология, JellyFish, Клоз, Fat Tree, Flattened Butterfly

В статье рассматриваются различные топологии построения сетей, их особенности, преимущества, которые они предоставляют, недостатки, связанные с их построением, эксплуатацией. В основном, среди инженеров наиболее известна трёхуровневая топология, стандартизированная компанией Cisco, представляющая собой частный случай обобщённой древовидной топологии. При растущих требованиях к пропускной способности, отказоустойчивости и общему качеству сети необходимо обратить внимание на архитектуру этих сетей на моменте их проектирования и понимать преимущества и недостатки используемых топологий. Фундаментальные топологии звезда, кольцо, древовидная топология, куб – в данной статье не рассматриваются, внимание уделено топологиям, сформированным на их основе.

V.V. Bentsel, N.V. Budyldina

OVERVIEW OF DPC NETWORK TOPOLOGIES

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: Topology, JellyFish, Clos, Fat Tree, Flattened Butterfly

The article discusses various topologies for building networks, their features, the advantages they provide, the disadvantages associated with their construction and operation. Basically, among engineers, the three-level topology standardized by Cisco is the most famous, which is a special case of a generalized tree topology. With increasing demands on bandwidth, fault tolerance, and overall network quality, it is necessary to pay attention to the architecture of these networks at the time of their design and understand the advantages and disadvantages of the topologies used. Fundamental topologies star, ring, tree topology, cube - are not considered in this article, attention is paid to topologies formed on their basis.

1 Трёхуровневая модель

Трёхуровневая модель является частным видом древовидной топологии построения сетей. Уровни делятся на: уровень доступа, агрегации (или распространения) и ядра. Уровень доступа отвечает за подключение оконечного оборудования или рабочей станции. На данном уровне используется оборудование L2, в преобладающем большинстве случаев основным используемым функционалом в таком оборудовании является ограничение широковещательных пакетов, для избегания флуда пакетов, сегментирование VLAN, поддержка SNMPv2 или SNMPv3. По причине такого низкого требования к оборудованию производители выпускают специальную линейку недорого оборудования. Следующим уровнем является уровень агрегации. На данном уровне устанавливается уже более дорогостоящее и производительно оборудование. На данном уровне требованием к оборудованию становится наличие протоколов динамической маршрутизации, технологии расширения количества L2-доменов (QinQ, VXLAN) и более производительная коммутационная матрица. Самое дорогостоящее и высокопроизводительное оборудование, с самым богатым функциональным наполнением располагается на уровне ядра. Данный уровень обрабатывает весь трафик сети.

Графическое изображение трёхуровневой топологии представлено на рисунке 1.1.

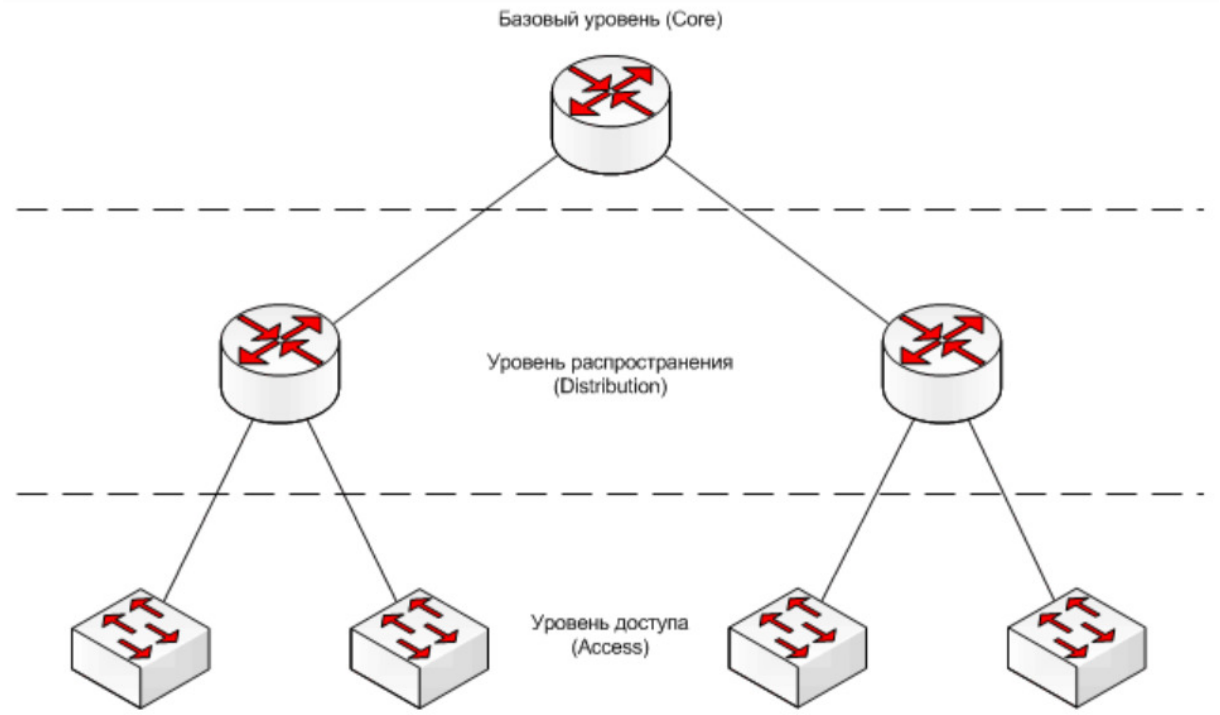


Рисунок 1.1 - Топология трёхуровневой модели

2 Топология сети Клоза или сети Fat Tree

В 1953 году Чарльз Клоз разработал технологию организации сети, где количество входов равно количеству выходов. Стоит упомянуть, что данная топология была разработана для телефонных сетей и характеризовалась, как неблокируемая. На 2.1 графическое представление, именуемое Crossbar:

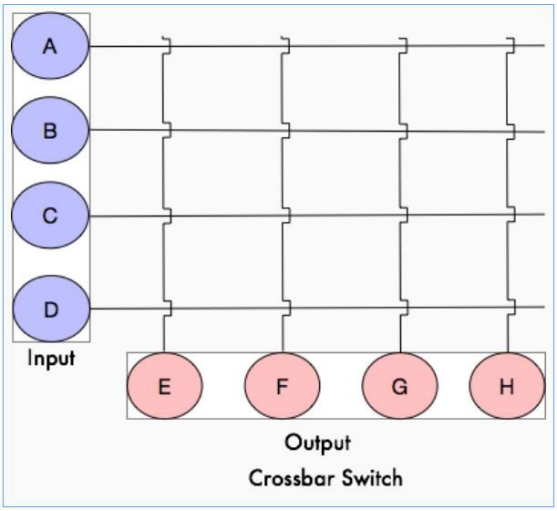


Рисунок 2.1 - Топология Fat Tree

Чарльз предложил разделить входы и выходы дополнительным уровнем коммутации, который позволит перестраивать соединения между входами и выходами по запросу. Это и назвали сетью Клоза (рисунок 2.2):

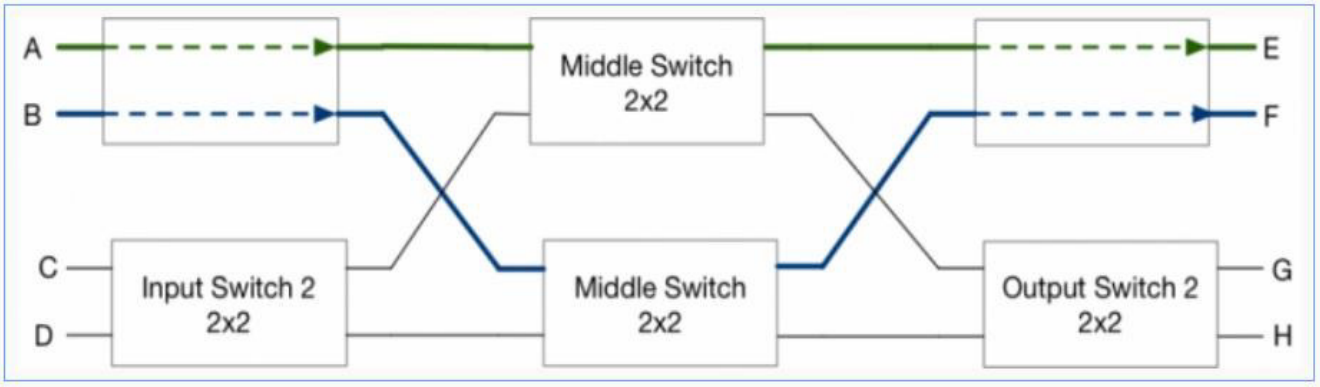


Рисунок 2.2 - Сеть Клоза

При такой сети количество соединений определяется по формуле 2.1 [1]:

$$M = 6n^{\left(\frac{3}{2}\right)-3n} \tag{2.1}$$

где M – количество точек коммутации;
n – число точек подключения;

На рисунке 2.3 представлена сравнительная характеристика по количеству точек коммутации при использовании метода Crossbar и сети Клоза.

TABLE I — CROSSPOINTS FOR SEVERAL VALUES OF N

N	Square Array N^2	Three-Stage Array $6N^{3/2} - 3N$
4	16	36
9	81	135
16	256	336
25	625	675
36	1,296	1,188
49	2,401	1,911
64	4,096	2,880
81	6,561	4,131
100	10,000	5,700
...	.....	.....
1,000	1,000,000	186,737
10,000	100,000,000	5,970,000

Рисунок 2.3 - Сравнительная характеристика.

Из рисунка видно, что при наличии 36 точек подключения количество соединений, необходимых для неблокируемости сети, т.е когда каждый вход имеет доступ к каждому выходу, требуется меньше, чем при использовании метода Crossbar.

Типичный вид трёхуровневой сети Клоза представлен на рисунке 2.4. Более же распространённый и привычный вид такой сети представлен на рисунке 2.5 и именуется Folded Clos, потому что, по сути, складывается вдвое.

Другое название такой сети - Fat Tree. Вместо весьма интеллектуального, а, соответственно, и склонного к ошибкам и багам уровня агрегации, появляется примитивный уровень коммутации - Spine, задача которого - очень быстро переложить пакет с одного Leaf на другой. К Leaf'ам

подключаются машины. Сами Leaf’ы подключаются к каждому Spine’у. А Spine’ы соответственно ко всем Leaf’ам. Таким образом, между любой парой машин будет существовать большое количество равноценных путей (по количеству спайнов) с всегда одинаковым числом хопов - 3 для сети, изображённой выше. Выход же во внешний мир или в другие ДЦ обычно реализуется через отдельные коробки, которые с точки зрения фабрики выглядят как Leaf-коммутаторы, однако гораздо более функциональные. Называются они Edge-Leaf (рисунок 2.6).

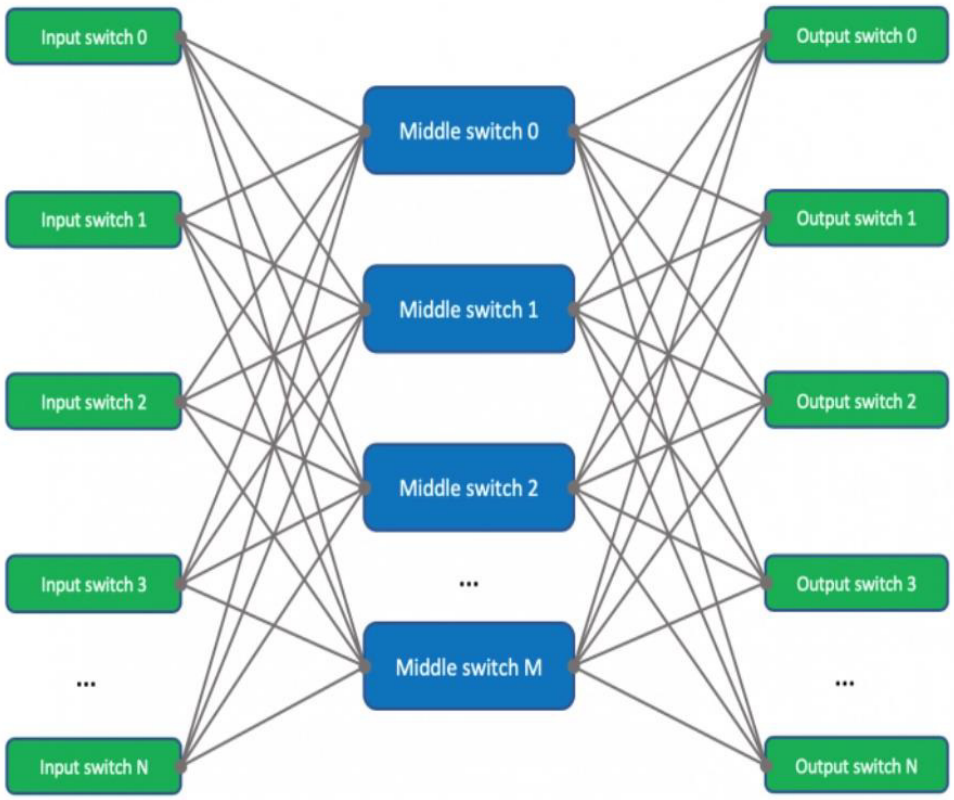


Рисунок 2.4 - Трёхуровневая сеть Клоза

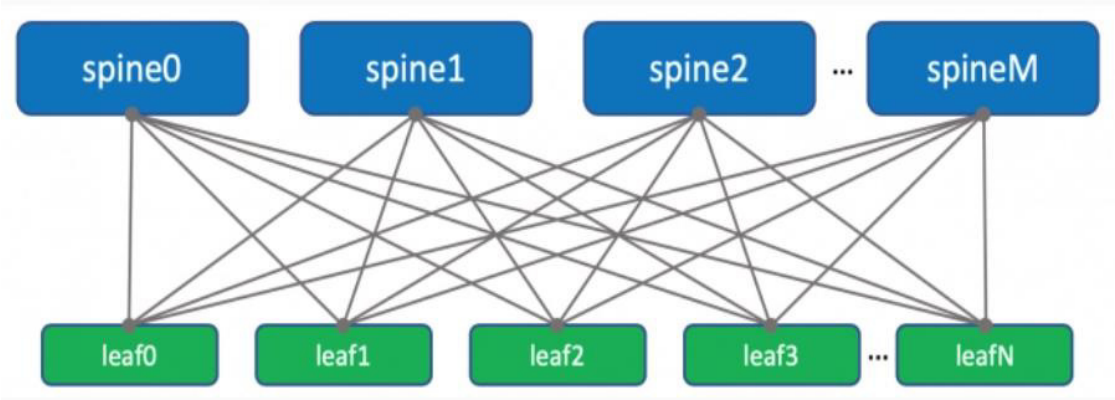


Рисунок 2.5 - Сеть Клоза в привычном видении

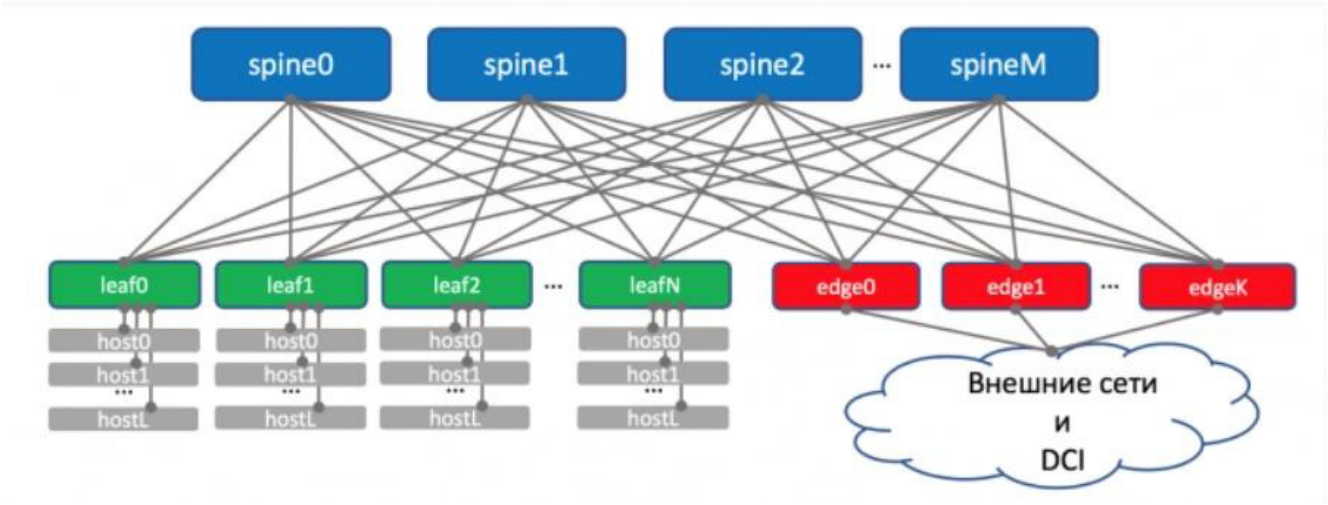


Рисунок 2.6 - Структура Edge-Leaf

3. Многоуровневая топология сети Клоза

При рассмотрении, например, пятиуровневой модели, с учётом того, что при первом рассмотрении имеем два уровня доступа, значит, будет три уровня промежуточных уровня. По аналогии с рисунком 2.4 трёхуровневой модели, пятиуровневая модель представлена на рисунке 3.1.

На самом деле, стандартизированы вычисления по сетям Клоза для различного количества уровней сети. В таблице 3.1 представлены вычислительные методы [2]:

Таблица 3.1 – Методология расчёта сети Клоза при L-уровнях

	Fat-tree with L levels	**Two level Fat Tree L=2**	**Three Level Fat Tree L = 3**	**Four Level Fat Tree L=4**
Number of Core switches	$\left(\frac{k}{2}\right)^{L-1}$	$\frac{k}{2}$	$\left(\frac{k}{2}\right)^{2}$	$\left(\frac{k}{2}\right)^{3}$
Number of Hosts supported	$2\left(\frac{k}{2}\right)^{L}$	$2\left(\frac{k}{2}\right)^{2}$	$2\left(\frac{k}{2}\right)^{3}$	$2\left(\frac{k}{2}\right)^{4}$
Total Switches	$(2L-1)\left(\frac{k}{2}\right)^{L-1}$	$3(\frac{k}{2})$	$5\left(\frac{k}{2}\right)^{2}$	$7\left(\frac{k}{2}\right)^{2}$
Number of Edge Switches	$2\left(\frac{k}{2}\right)^{L-1}$	k	$2\left(\frac{k}{2}\right)^{2}$	$2\left(\frac{k}{2}\right)^{3}$
Number of Pods	$2\left(\frac{k}{2}\right)^{L-2}$	NA	k	$k^2/2$

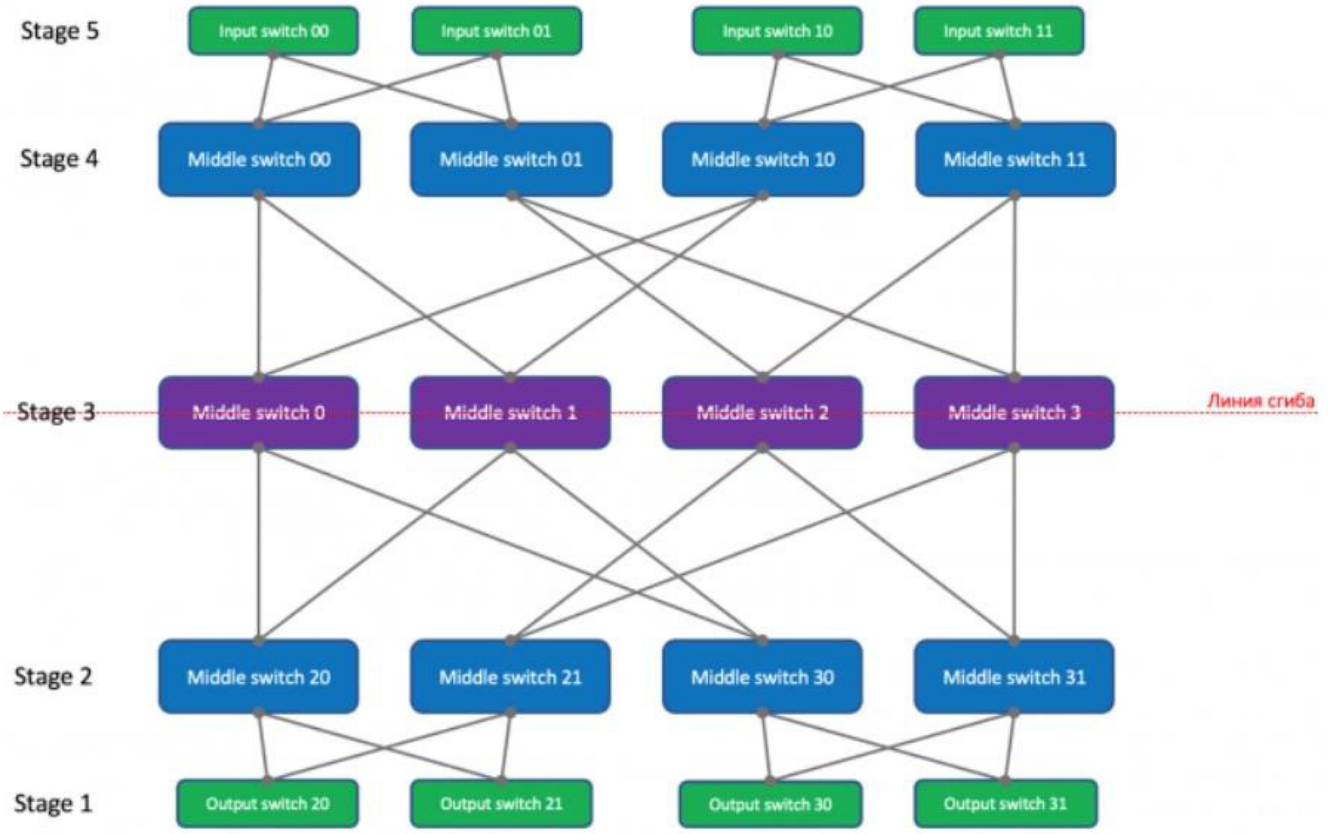


Рисунок 3.1 - Пятиуровневая модель сети Клоза

После сложения сети вдоль третьего уровня получим следующую схему, представленную на рисунке 3.2:

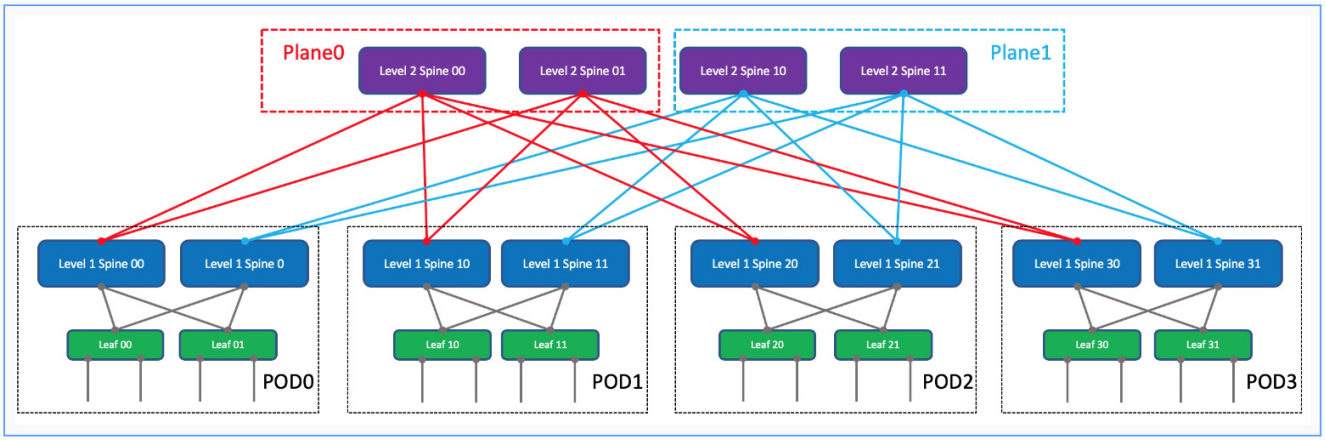


Рисунок 3.2 - Folded Close пятиуровневой модели

В итоге получаем сегменты PoD – Point of Delivery. Данные сегменты являются универсальными. Сеть можно масштабировать, по аналогии с игрой в конструктор, т.е. при необходимости достаточно заказать идентичный блок и подключить его к общей структуре сети.

3 Топология Flattened Butterfly

Данная топология ориентирована на организацию сети в ЦОД для суперкомпьютеров, в которых установлены высокопроизводительные процессоры с огромным количеством, сравнительно с серверами под отдельные услуги, процессов.

Первоначально для сетей суперкомпьютеров использовали сети Клоза. Но данная сеть была не оптимальна для требуемого времени отклика. В сети Клоза запрос будет проходить вдвое больше хопов, чем нужно.

Топология Flattened Butterfly была представлена лишь в 2007 году на международном симпозиуме по компьютерной архитектуре (ISCA). Через год была представлена обновлённая архитектура Flattened Butterfly – Dragonfly [3].

В качестве примера, на рисунке 3.1 представлен пример полносвязной топологии Flattened Butterfly:

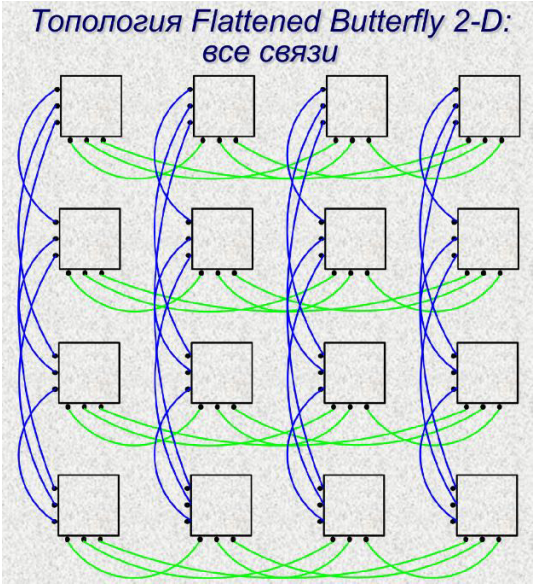


Рисунок 3.1 - Пример одной из реализации Flattened Butterfly

Более подробно топология описана в источнике [5]

4 Топология JellyFish

JellyFish – это случайный регулярный граф. Регулярный граф – граф, в котором каждый узел имеет тот же вес, что и соседи, а случайный регулярный граф равномерно выбирается из пространства всех графов.

Как это принято обычно, узлом является коммутатор. В JellyFish построение случайного графа основано на коммутаторе ToR (Top of Rack).

Каждый коммутатор ToR i имеет некоторое количество портов k_i, некоторые из них r_i используются для подключения к другому коммутатору ToR. Остальные порты k_i-r_i используются для подключения серверов. Таким образом, при n количестве стоек общее количество серверов M, которые можно подключить равняется:

$$M = n(\mathrm{ki} - \mathrm{ri}) \tag{5.1}$$

Коммутация в данной топологии определяется, во - первых, сначала сервера равномерно распределяются по коммутаторам, после чего выбирается количество уровней сети. Дальше процесс удобней описать на примере. Таким образом, предположим, что у нас 16 серверов, 20 коммутаторов, 4-х уровневая модель. Первый уровень представляет собой подключенные сервера (коммутатор доступа). Остаётся ещё три уровня. Вот тут коммутатор соединяется с тремя другими коммутаторами, у которых всё ещё нет трёх соединений с соседями по тому же принципу.

Исследование автора данного источника [4] показывает, что в случае парка тысяч серверов данная топология показывает более эффективное показатели использования пропускной способности. Однако, исследование теоретическое. На практике реализация не приведена. Не рассмотрены вопросы отказоустойчивости, нет точного ответа - на сколько случайные графы близки к оптимальным показателям пропускной способности, на сколько зависит от используемого оборудования. С точки зрения проектирования сети могут возникнуть проблемы с коммутацией. Не исследован вопрос разнородности оборудования (разное количество портов,

скорость соединения). Так же в плане маршрутизации и управления неясны модели конфигурирования, так как данная модель сильно отлична от чёткого разграничения уровней.

На рисунке 5.1 представлено теоретическое сравнение использование пропускной способности при абсолютной однородности оборудования, без учёта его физического размещения [4].

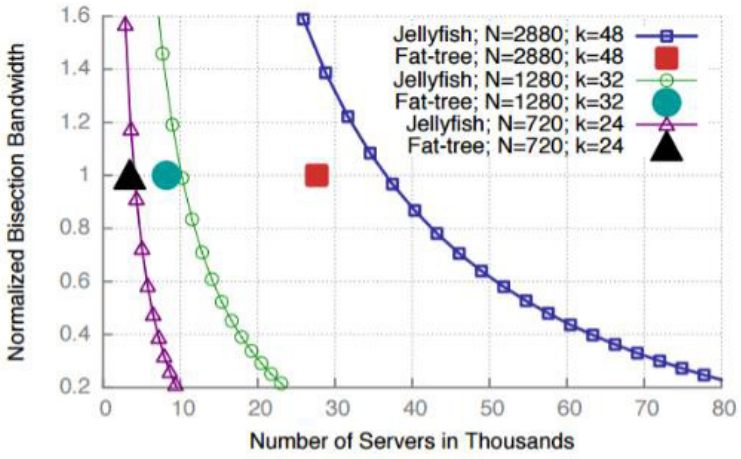


Рисунок 5.1 - Теоретическое сравнение топологий

На рисунке 5.2 представлено графическое сравнение топологий Fat Tree и JellyFish в рамках рассмотренного ранее примера:

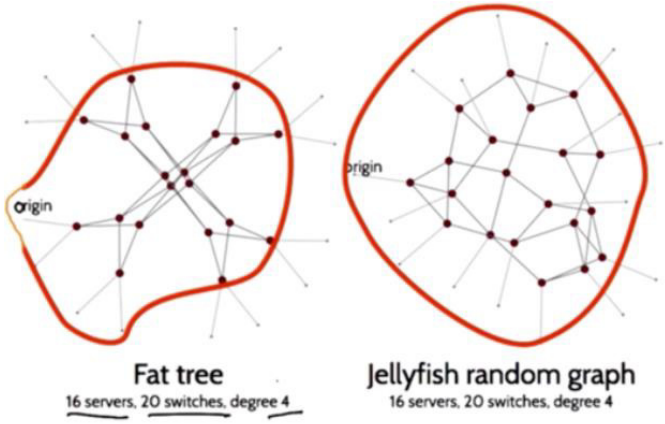


Рисунок 5.2 - Графическое сравнение топологий.

СПИСОК ЛИТЕРАТУРЫ:

1. Марат Сибгатулин. Как построить Google [Электронный ресурс] – Режим доступа: https://nag.ru/material/36318
2. Diptanshu Singh. Demystifying DCN Topologies: Clos/Fat Trees – Part2 [Электронный ресурс] – Режим доступа: https://packetpushers.net/demystifying-dcn-topologies-clos-fat-trees-part2
3. Nevil Savage. Flattened Butterfly Network Lets Data Fly Through Supercomputers and Multicore Processors [Электронный ресурс] – Режим доступа: https://spectrum.ieee.org/flattened-butterfly-network-lets-data-fly-through-supercomputers-and-multicore-processors
4. Bo Yoo, Mauricio Narvaez. CS244 ‘17: JELLYFISH: NETWORKING DATA CENTERS RANDOMLY [Электронный ресурс] – Режим доступа: https://reproducingnetworkresearch.wordpress.com/2017/06/02/cs244-17-jellyfish-networking-data-centers-randomly/
5. Kim J., Dally W.J., Abts D. Flattened Butterfly. A Cost-Efficient Topology for High-Radix Networks. 34th International Symposium on Computer Architecture (ISCA 2007), San Diego, California, USA, June 9-13, 2007, ACM, 2007. P. 126-137

В.В. Бенцель, Н.В. Будылдина

ТЕНДЕНЦИИ РАЗВИТИЯ СЕТЕЙ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Уральский технический институт связи и информатики (филиал) ФГОБУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: Развитие, ЦОД, SDN, VXLAN, overlay-сети, архитектура, контроллер.

В статье рассматривается тенденция развития сетей ЦОД, причины развития сетевой инфраструктуры и увеличения доменов L2. Основным направлением является переход к программно-ориентированным сетям SDN с разделением функций управления и передачи пользовательского трафика для повышения гибкости современных сетей передачи данных. Рассмотрена технология построения сетей SDN – VXLAN, формат кадра, особенности стандарта и его использования. В современных реалиях традиционные принципы построения ЦОД всё чаще не обеспечивают технологического функционирования, резервирования и показателей отказоустойчивости. По этому процесс перехода к новой архитектуре является логичным продолжением развития сетевых технологий.

V.V, Bentsel, N.V. Budyldina

DATA CENTER NETWORKS DEVELOPMENT TRENDS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: Development, data center, SDN, VXLAN, overlay networks, architecture, controller

The article discusses the development trend of data center networks, the reasons for the development of network infrastructure and the increase in L2 domains. The main direction is the transition to software-oriented SDN networks with separation of user traffic control and transmission functions to increase the flexibility of modern data transmission networks. The technology of building SDN networks - VXLAN, frame format, features of the standard and its use are considered. In modern realities, the traditional principles of building a data center increasingly do not provide technological functioning, redundancy and fault tolerance. Therefore, the process of transition to a new architecture is a logical continuation of the development of network technologies.

По мере роста пользовательского спроса на качество предоставляемых услуг, времени отклика, скорости обработки запросов, разнообразие предлагаемых сервисов растёт и количество информационных систем, каждая из которых стремиться предложить пользователям что-то новое, отличиться от своих конкурентов на рынке, а вместе с количеством сервисов растут и развиваются транспортные сети. Разрабатываются и внедряются на транспортные сетевые инфраструктуры новые технологии, протоколы, топологические решения в области построения сетей. По мере роста требования к качеству предоставляемых услуг у разработчиков информационных систем повышаются требования к качеству транспортной инфраструктуры, к которой они подключают свои сервера.

Так как вся информационная инфраструктура размещается в центрах обработки данных (ЦОД), то речь стоит вести именно о развитии сетей для их размещения.

Относительно недавно сети ЦОД представляли собой высокоскоростную, масштабируемую локальную сеть, в которой располагались все сервера. Все сервера размещались централизованно, в рамках одной площадки, которая гарантированно обеспечивала необходимый уровень доступности, безопасности и отказоустойчивости. На самом деле, такая

архитектура существует до сих пор в небольших организациях. Однако же постепенно происходит переход на архитектуру географически разнесённых ЦОД с целью повышения уровня резервирования, или же разделения по качеству обслуживания, одни словом – децентрализация.

С целью соответствия экспоненциально растущему потоку данных из разных источников происходит развитие новых возможностей серверов, как для хранения, так и для обработки всё более сложных сервисных взаимодействий. Традиционные технологии и архитектурные решения в построении и обслуживания ЦОД на данный момент всё меньше соответствуют развивающимся требованиям к эффективности, рациональности и удобству работы. Данный факт стал причиной появления технологии программно-определяемых сетей (SDN). Благодаря данной технологии стало возможным разделять плоскости управления и пользовательского трафика, конфигурировать логически централизованное управление, а также расширяет возможности сетей для приложений верхних уровней. Наиболее подходящим применением технологии SDN служит внедрение в инфраструктуры ЦОД с высокопроизводительным функционалом, разветвлённой адресацией, требующей централизованного управления, развёртывания большого парка виртуальных машин, их миграцию. Коротко говоря, SDN – технология, обеспечивающая технологическое развитие облачных решений и определяющая будущее сетей ЦОД [1].

В основе концепции SDN лежат следующие два принципа:

- Перенос слоя управления из сети устройств в центральное внешнее устройство – контроллер сети. В сетевых устройствах остаётся только механизм продвижения, действующий на основе решений, принимаемых слоем управления в контроллере сети;
- Унификация механизма продвижения и интерфейса между механизмом продвижения и контроллером. Унификация механизма продвижения стирает различия между коммутатором и маршрутизатором, работающими по технологии SDN, по этой причине такие устройства обычно называют просто «устройства продвижения».

На рисунке 1 представлена сеть коммутаторов, находящихся под управлением центрального элемента – контроллера. Операционная система контроллера обеспечивает функционирование управления сетью: построение топологии сети, отслеживание состояния коммутаторов, их интерфейсов, обеспечение удобного графического интерфейса для администратора сети. Поверх сетевой ОС также работают приложения, обеспечивающие различные функции, такие как трафик инжиниринг, поддержка VPN, защита от атак и т.д..

В каждом коммутаторе SDN реализованы два модуля:

- Модуль таблиц продвижения;
- Модуль интерфейса с контроллером.

В отличие от традиционных коммутаторов, самостоятельно формирующих таблицы продвижения, коммутаторы SDN получают их в готовом виде от контроллера [2].

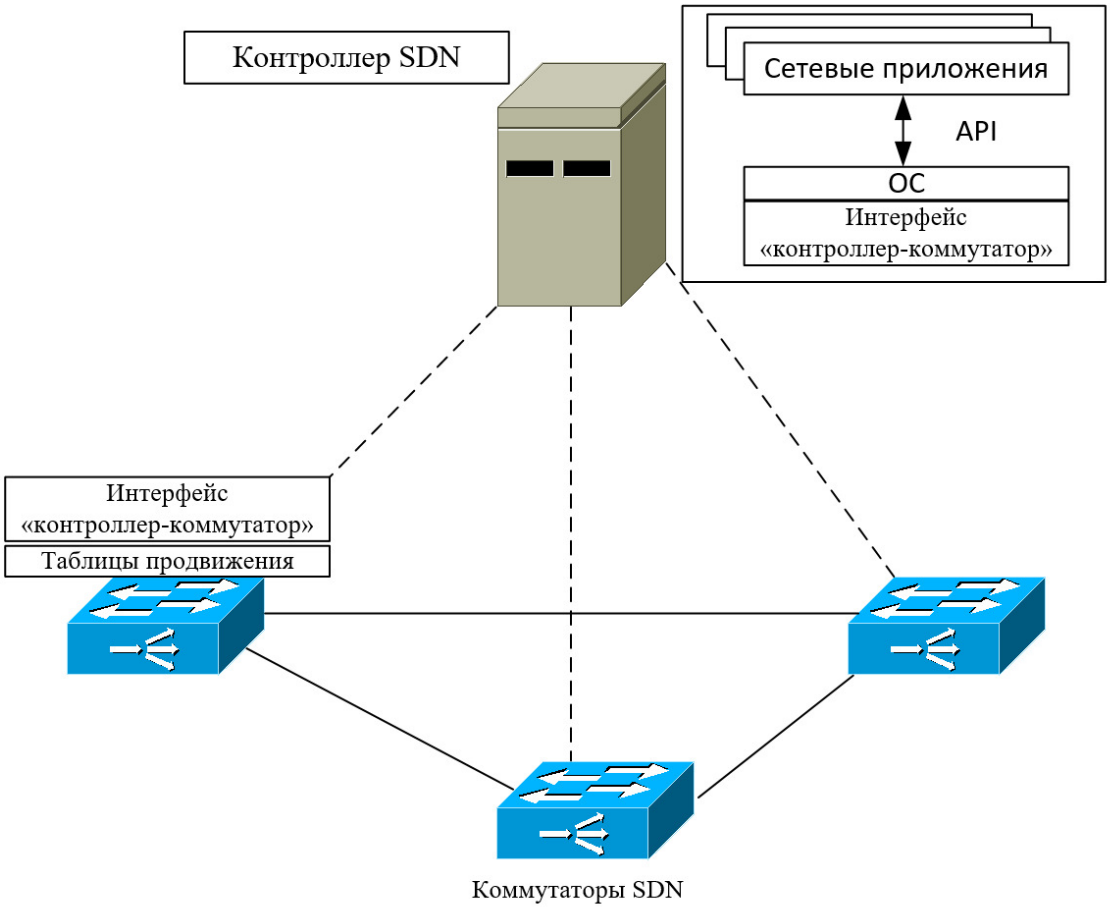


Рисунок 1 - Сеть коммутаторов, находящихся под управлением контроллера SDN

По той причине, что все политики передаются централизованно, в SDN предусмотрена возможность виртуализации и гибкого планирования сетевых ресурсов. Сама виртуализация инфраструктурной сети основана на идее построения overlay-сети, а именно посредством технологии VXLAN. Данная технология overlay-сети позволяет избежать ограничений, накладываемых на серверную инфраструктуру, когда речь заходит о физическом разнесении по разным площадкам, позволяет организовать большой L2 домен для совместного его взаимодействия всех сервисов, для которых это необходимо.

Например, для повышения отказоустойчивости был сконфигурирован кластер из двух серверов – основной и резервный. В распоряжении есть две площадки ЦОД. Технология VXLAN позволяет разнести две ноды сервера по разным площадкам и сохранить связность между ними для оперативного переключения, в случае, даже если одна из площадок ЦОД полностью выйдет из строя.

В технологии VXLAN расширение домена L2 происходит благодаря инкапсуляции MAC-in-UDP. Данный метод инкапсуляции позволяет оперировать преимуществами протоколов маршрутизации для обеспечения резервирования каналов передачи данных, а также для балансировки нагрузки. Получается, что становится возможным строить L2 домены с преимуществами сетевого уровня L3, применяя технологии инжиниринга трафика. Во многих статьях также приводиться преимущество VXLAN перед VLAN по размеру поля идентификатора – 24 бита, против 12. Даже в RFC [3] отмечается данное преимущество. Однако не стоит забывать о стандарте 802.1.ad, который позволяет всем привычный VLAN ID тег инкапсулировать в ещё один. При технологии QinQ мы также можем расширить количество уникальных L2 доменов более чем до шестнадцати миллионов, как и в случае использования VXLAN и также оперировать технологиями трафик инжиниринга на уровне L3.

Технология VXLAN стандартизирована в августе 2014 года и подробно описана в RFC-7348.

На рисунке 2 представлена структура пакета VXLAN:

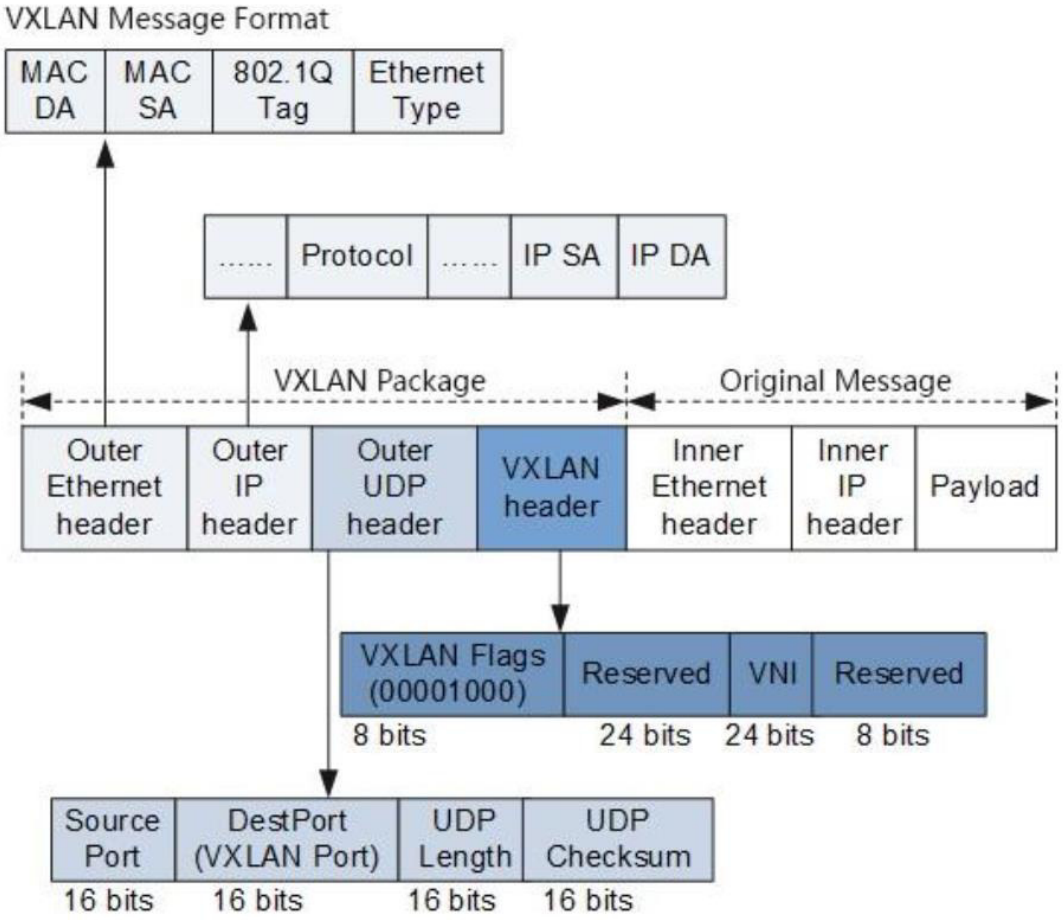


Рисунок 2 - Структура VXLAN-пакета

Так как VXLAN - по сути своей туннель, то как и в привычном VPN происходит установка соединения между двумя удалёнными узлами, а точнее оконечными точками, что позволяет установить туннель VTEP (VXLAN tunnel endpoints), что и позволяет организовывать логические overlay-сети поверх уже существующих, а так как происходит инкапсуляция оригинальных пакетов в новый заголовок VXLAN, то изменения, которые необходимо внести в существующую инфраструктуру минимальны.

Идентификатором потока же служит протокол UDP, а именно порт, используемый транспортным протоколом. Благодаря этому на транзите нет необходимости заглядывать внутрь пакета для соблюдения последовательности. Данная задача ложится на граничные коммутаторы.

Использование протокола UDP обусловлено тем, что протокол TCP предназначен для гарантированной доставки, а значит в случае, если пропал пакет, необходимо будет выждать таймаут, после которого передача пакета будет инициирована снова. Так как VXLAN – технология overlay-сети, то не стоит забывать, что на underlay-сети уже используется протокол TCP. Получается, что у нас будет реализован транспорт TCP поверх TCP, что в случае возникновения даже малочисленных потерь приведёт к простою сети. К тому же, TCP не предназначен для установления соединений Point-to-Multipoint, а это необходимо для поддержания связности между коммутаторами SDN, особенно в случаях, когда в топологии сети отсутствует контроллер SDN, и связность между устройствами прописана статически.

СПИСОК ЛИТЕРАТУРЫ:

1. Денис Сереченко, директор по развитию бизнеса Huawei Enterprise Business Group в России. Переход от обычной сети ЦОД к SDN [Электронный ресурс] – Режим доступа : https://habr.com/ru/company/huawei/blog/337918/

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – СПб.: Питер, 2020 – 1008 с.: ил. – (Серия «Учебник для вузов).
3. RFC-7348. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 networks / M. Mahalingam [Электронный ресурс] – Режим доступа: https://www.rfc-editor.org/rfc/rfc7348

К.И. Брагин, Д.В. Агапитов, Я.А. Колташев

ОБУЧЕНИЕ С ПОДКРЕПЛЕНИЕМ В ЗАДАЧЕ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ БЕСПРОВОДНОЙ СЕТИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: машинное обучение, управление радиоресурсами, обучение с подкреплением, сети мобильной связи, беспроводная связь, планировщик сети.

В статье раскрываются аспекты задачи управления беспроводной сетью, в частности вопрос распределения радиоресурсов между пользователями и доступа к среде передачи. Кроме того, в этом заключается эффективность предотвращения перегрузки сети, гибкость и масштабируемость. За механизм планирования доступа к среде передачи данных в радиоканале между устройством пользователя и базовой станцией отвечает алгоритм планировщика - MAC Scheduler. Данный механизм возможно усовершенствовать с помощью машинного обучения, особенно, принципов глубокого обучения с подкреплением.

K.I. Bragin, D.V. Agapitov, Y.A. Koltashev

REINFORCEMENT LEARNING IN RESOURCE ALLOCATION OF WIRELESS NETWORK

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTICI SibSUTIS), Russia

Keywords: machine learning, resource scheduling, radio resource allocation, mobile communications, wireless communication, reinforcement learning, scheduler.

The article reveals the main aspects of the wireless network management task, in particular, the issue of radio resources allocation between users and medium access control. In addition, it takes the success of preventing network congestion and ensuring its flexibility and scalability. The scheduling algorithm, MAC Scheduler, is responsible for the mechanism of scheduling access to the data transmission medium in the radio channel between the user's device and the base station. This mechanism can be improved with the help of machine learning, especially the principles of deep learning with reinforcement.

Алгоритмы машинного обучения уже давно применяются для решения широкого спектра задач в телекоммуникациях. Примером является моделирование и оценка параметров каналов. Искусственный интеллект (ИИ) используется для извлечения характеристик канала в частотной, временной и даже пространственных областях. Обученная модель способна прогнозировать изменение канала, что даёт точную информацию о состоянии канала в сценариях глубоких замираний или доплеровского сдвига, часто встречающихся в городской застройке и при наличии высокомобильных клиентов. К таким относится как беспилотный транспорт, поезда, так и абонент, передвигающийся на автомобиле по междугородней трассе. Для таких задач могут применяться рекуррентные нейронные сети (англ. Recurrent neural network, RNN), например LSTM (Long-short term memory). RNN эффективно решают задачи, где требуется обработка временных рядов, отслеживание изменений во времени и даже предсказание значений переменных.

Беспроводной канал подвержен замираниям и зашумлению, что предъявляет высокие требования к обработке сигналов. Учитывая, что сигнал сгенерирован на основе ортогонального частотного разделения (OFDM модуляции) с квадратурной амплитудной модуляцией, в задачах

декодирования применимы свёрточные нейронные сети (англ. Convolutional neural network, CNN). Это позволяет уменьшить ошибки распознавания символов, увеличить чувствительность приемников и дальность связи.

В беспроводных сетях применяется простой прием в технике модуляции сигнала - адаптивность. Чем дальше клиентский терминал от базовой станции, тем ниже уровень принимаемого сигнала и порядок модуляции. Это снижает пропускную способность канала, но позволяет передавать данные на большее расстояние. Процесс применим ко всем активным пользователям, работающим в сети. У каждого разная скорость передвижения, различные частотные и временные характеристики канала, следовательно, необходим алгоритм «дирижер», реализующий функции управления и контроля. Данный алгоритм является функцией канального уровня и реализуется в рамках MAC-протокола.

Распределение ресурсов и организация доступа к среде - ключевые функции беспроводной системы на уровне MAC. Эффективный алгоритм динамического распределения ресурсов существенно влияет на коэффициент полезного использования радиоинтерфейса [1].

Задача управления и распределения ресурсов - марковский процесс принятия решений и относится к многокритериальной оптимизации, уходит корнями в теорию расписаний (англ. scheduling), раздел дискретной математики, занимающийся проблемами упорядочивания. Данный раздел является частью теории операций и используется в различных областях, таких как производство, транспорт, телекоммуникации, медицина и другие. Теория расписаний исследует как повысить эффективность и производительность системы путем определения оптимального порядка выполнения задач и нахождения оптимальных вариантов использования ресурсов. Так, перед любым планировщиком ставится задача дискретной оптимизации: построить расписание, минимизирующее стоимость и время выполнения работ. Задачи теории расписаний делятся на две основные группы: задачи с прерываниями и задачи без прерываний. Заметна параллель с теорией массового обслуживания - исследующей рациональный выбор структуры системы обслуживания и процесса обслуживания на основе изучения потоков требований на обслуживание, поступающих в систему и выходящих из неё, длительности ожидания и длины очередей.

Любую беспроводную сеть можно описать как систему массового обслуживания, так как она предназначена для обработки большого числа запросов от множества пользователей. Каждый пользователь создает персональный запрос (например, звонок или отправка сообщения) и ждет, пока его запрос будет обработан. Система обрабатывает запросы в режиме реального времени.

Также сотовая сеть обладает параметры производительности, которые могут быть измерены в терминах задержки, пропускной способности и надежности. Различные элементы сети, такие как базовые станции и коммутационное оборудование, играют важную роль в обеспечении высокого уровня производительности и качества обслуживания для множества пользователей.

Система сотовой связи является примером системы массового обслуживания со случайным потоком вызовов, случайной продолжительностью их обслуживания (сеансов) и конечным числом каналов обслуживания (каналов связи). Известно, что система телефонной связи исторически была первым примером системы массового обслуживания, в частности, первой математически корректной работой по теории массового обслуживания называют работу Агнера Крарупа Эрланга «Теория вероятностей и телефонные разговоры».

Таким образом, сотовая сеть является примером сложной системы массового обслуживания, которая обеспечивает своим пользователям надежное и высококачественное обслуживание в режиме реального времени.

Тем не менее, задача распределения ресурсов связана с теорией расписаний, которая занимается планированием и оптимизацией используемых ресурсов. Теория массового обслуживания занимается анализом процессов обслуживания в системах с неопределенным потоком заявок, и несколько отличается от задачи распределения ресурсов. Однако, теория массового обслуживания также полезна при оценке производительности систем, что может помочь в оптимизации распределения ресурсов. Поставленная задача является комплексной и находится на стыке сразу нескольких разделов математики и информатики. В этом есть и положительные стороны, алгоритм, который способен решить поставленную проблему будет

гибок, что позволит использовать его для распределения ресурсов центрального или графического процессора любой вычислительной машины.

Механизм оптимизации доступной пропускной способности радиоканала и контроль за качеством обслуживания пользователей, путем распределения доступа к радиоканалу в соответствии с приоритетами и текущей загрузкой заложен в MAC Scheduler (Medium access control scheduler). Цель алгоритма управления частотными ресурсами в сотовой сети - управление доступом мобильных устройств к радиоканалам (частотам) и выделение им определенных частотных ресурсов в зависимости от уровня загрузки сети. Алгоритм работает следующим образом:

– сбор и анализ информации о загрузке соты - сеть анализирует уровни загрузки частотных ресурсов на всех сотах в режиме реального времени;

– определение потребностей каждого мобильного устройства - сеть получает данные о потребностях каждого мобильного устройства в частотных ресурсах (например, данные о скорости передачи данных и размере передаваемых пакетов);

– распределение частотных ресурсов - на основе данных о загрузке соты и потребностей каждого мобильного устройства сеть выделяет определенные частотные ресурсы для каждого устройства;

– мониторинг процесса и корректировка; сеть постоянно мониторит процесс распределения частотных ресурсов и корректирует его при необходимости, чтобы оптимизировать производительность и доступность сети для всех пользователей.

Алгоритм управления частотными ресурсами в сотовой сети также может быть улучшен с помощью технологий, таких как множественный доступ с пространственным разделением (MIMO) и алгоритмами автоматического блокирования повторной передачи (ARQ) [2]. Принципиальную схему работы MAC Scheduler можно увидеть на рисунке 1.

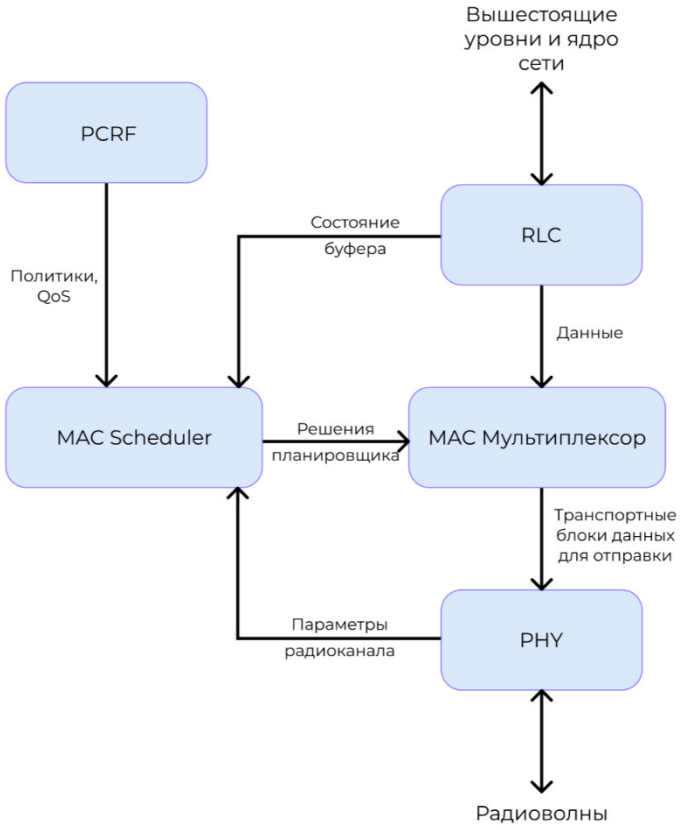


Рис. 1. - Принципиальная схема работы MAC Scheduler.

На схеме: политики и QoS, получаются с модуля PCRF (Policy and Charging Rules Function); уровень PHY отправляет информацию о состоянии канала; уровень RLC работает с буфером; основываясь на перечисленных пунктах, планировщик принимает решение на основе специальных алгоритмов, таких как Round Robin, Proportional Fair, Maximum C/I и других.

Открытым остается вопрос того, какие алгоритмы машинного обучения способны помочь в решении задачи нахождения оптимальных вариантов использования радиоресурсов сети. Некоторые из широко используемых алгоритмов обучения представлены далее:

1) линейное программирование, метод оптимизации, задача которого найти оптимальное решение линейной оптимизации, т.е. поиск максимального или минимального значения линейной функции при условии, что ограничения на переменные являются линейными;

2) генетические алгоритмы (англ. Generative adversarial network, сокращенно GAN), имитирующие принципы эволюции и естественного отбора, совершенствуясь от поколения к поколению;

3) алгоритмы глубокого обучения, нейросетевые алгоритмы хорошо работают с большими данными и успешно выявляют скрытые взаимосвязи, что может дать больше оптимальных вариантов использования ресурсов;

4) алгоритмы кластеризации, могут группировать данные, что может помочь оптимизировать работу на основе общих признаков канала и временного характера;

5) байесовские сети, моделируют вероятности событий и могут позволить предсказывать оптимальное распределение на основе приоритетов трафика и политик.

Ряд исследований полагаются на обучение с учителем, либо на обучение без учителя. Однако, при обучении с учителем необходимо провести разметку данных, а объем данных может быть достаточно большим. При обучений без учителя, необходимо сформулировать целевые переменные, и то, к какому уровню оптимизации следует стремиться. Как сказано ранее, задачи на уровне MAC весьма чувствительны к изменениям состояния канала, а вариативность сценариев велика [3]. В предыдущей работе [4] было отмечено, что среди исследователей данной задачи отмечается интерес к методам обучения с подкреплением (ОП), а конкретно deep reinforcement learning (DRL). Выбор алгоритмов обучения с подкреплением, сочетающихся с принципами глубокого обучения обоснован той самой вариативностью состояний системы. Классификацию алгоритмов обучения с подкреплением можно изучить на рисунке 2. Отметим, что генетические алгоритмы многие исследователи относят к ОП.

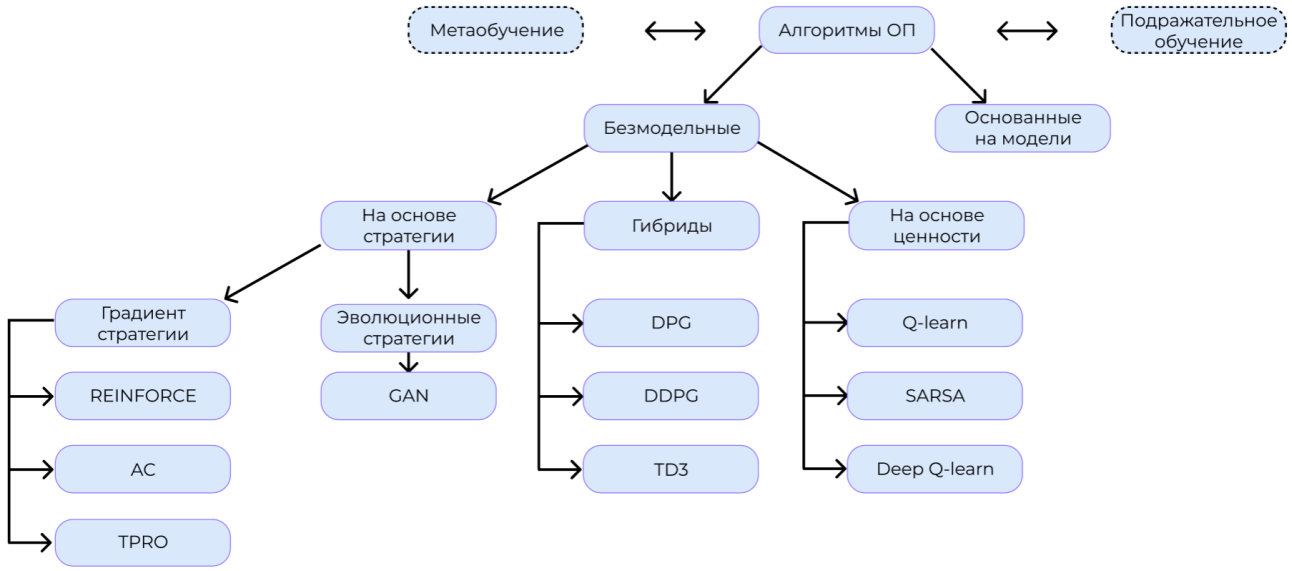


Рис. 2. – Классификация алгоритмов обучения с подкреплением.

В контексте управления сетевой нагрузкой обучение с подкреплением может использоваться для определения наилучшей стратегии управления трафиком и снижения задержек при передаче данных. Обучение с подкреплением - это метод машинного обучения, который заключается в обучении агента принимать решения в определенной среде на основе накопленного опыта и полученных вознаграждений. Агент, работающий в такой среде, может принимать решения на основе полученных вознаграждений, которые определяются, например, исходя из количества переданных данных и скорости передачи. В [5] агент DRL помогает выстроить порядок использования тайм-слотов и координировать передачу. Обучение с

подкреплением может быть более эффективным, чем другие методы машинного обучения, так как позволяет агенту адаптироваться к изменениям в среде и принимать решения на основе актуальной информации.

Интерес представляют работы, где обучение с подкреплением используется в качестве планировщика MAC на базовой станции. Подавляющее большинство из них - зарубежные. Например, в [6] удалось достичь оптимальной производительности при полной загрузке буфера, получено увеличение до 30% по сравнению с традиционными алгоритмами, основанными на пропорциональной справедливости (англ. proportional fair) и не полном буфере.

Методы машинного обучения способны не только выстроить оптимальную стратегию реагирования сети на ту или иную ситуацию, но также предоставить прогноз. Из собранных на сети данных можно многому научиться. Это позволит создать интеллектуальный MAC контроллер для оперативного регулирования параметров радиоинтерфейса в любой сети. Данный контроллер играет важную роль в обеспечении отказоустойчивости сети, принимает множество ключевых решений на протяжении всего жизненного цикла системы связи, формирует и управляет лучом (технология beamforming), регулирует использование спектра и адаптацию модуляционно-кодовых схем, выделяет ресурсы канала пользователям, а также управляет мощностью.

Традиционные методы решения вышеупомянутых проблем на основе теории оптимизации представляют собой NP-полную задачу и слишком сложны в реализации. При переходе к системе машинного обучения с подкреплением важно решить и проблему взаимодействия базовых станций друг с другом. Решения, принимаемые внутри соты приведут только к локальной оптимизации, поэтому, стоит задуматься о многоагентной системе. Координация распределения радиоресурсов между множеством базовых станций будет способствовать повышению общих показателей сети [3].

Однако, стоит заметить, что для использования машинного обучения в задаче регулирования сети и распределения радиоресурсов необходимо иметь большой объем данных и мощных вычислительных ресурсов. Особенно, требуется учитывать различные факторы, такие как безопасность и конфиденциальность данных, коммерческая тайна, а также соответствие стандартам и правилам регулирования сетевой нагрузки.

СПИСОК ЛИТЕРАТУРЫ:

1. Андреев А.В., Дроздова В.Г. Имитационное моделирование вероятностно-временных характеристик MAC-протокола LTE-Advanced с поддержкой агрегации несущих. Вестник СибГУТИ. 2017;(3):76-85.
2. A. D. Channagire and A. D. Mane, "Performance Analysis of Long Term Evolution (LTE) Medium Access Control (MAC) Scheduler for Real-Time Heterogeneous Data Traffic," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 2019, pp. 1016-1023.
3. Вэнь Тонг, Пейин Чжу, Сети 6 G. Путь от 5 G к 6 G глазами разработчиков. От подключенных людей и вещей к подключенному интеллекту / пер. с англ. В. С. Яценкова. - М.: Д М К Пресс, 2022. - 624 с.
4. Брагин, К. И. Применение алгоритмов машинного обучения для управления ресурсами в мобильных сетях 5G / К. И. Брагин, С. А. Тычинкин // Инфокоммуникационные технологии: актуальные вопросы цифровой экономики : Сборник научных трудов III Международной научно-практической конференции, Екатеринбург, 25–26 января 2023 года / Под редакцией В.П. Шувалова, сост. М.П. Карачарова. – Екатеринбург: Уральский государственный университет путей сообщения, 2023. – С. 88-91.
5. M. P. Mota, D. C. Araujo, F. H. C. Neto, A. L. de Almeida and F. R. Cavalcanti, «Adaptive modulation and coding based on reinforcement learning for 5G networks», in Proc. 2020 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2020, pp. 1-6.
6. C. Xu, J. Wang, T. Yu, C. Kong, Y. Huangfu, R. Li, Y. Ge, «Buffer-aware wireless scheduling based on deep reinforcement learning», in Proc. 2019 IEEE Globecom Workshops. IEEE, 2019, pp. 1-6.

Д.И. Бурумбаев, Н.М. Барбин

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СПЕКТРОФОТОМЕТРОВ ДЛЯ ИЗМЕРЕНИЯ СВОЙСТВ ЖИДКОСТИ

Уральский технический институт связи и информатики ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (филиал) в г. Екатеринбурге, Россия

Ключевые слова: спектрофотометры, оптические свойства жидкости, диапазон измерения, спектроскопия, анализ свойств.

В статье приведено краткое описание принципов работы спектроскопических методов анализа. Рассмотрена принципиальная схема спектрофотометра, описан перечень преимуществ. Определен список параметров, по которому производится сравнительный анализ. Сделано заключение о выборе среди представленных приборов.

D.I. Burumbaev, N.M. Barbin

COMPARATIVE ANALYSIS OF SPECTROPHOTOMETERS FOR MEASURING LIQUID PROPERTIES

Ural Technical Institute of Communications and Informatics Siberian State University of Telecommunications and Informatics (branch) in Yekaterinburg, Russia

Keywords: spectrophotometers, optical properties of liquid, measuring range, spectroscopy, properties analysis.

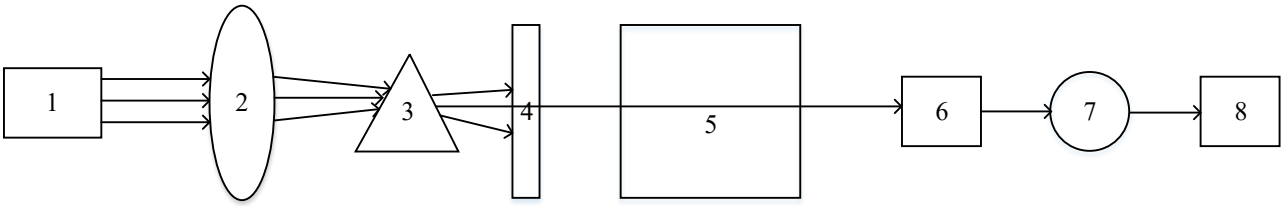
The article provides a brief description of the principles of operation of spectroscopic analysis methods. The schematic diagram of the spectrophotometer is considered, a list of advantages is described. A list of parameters is defined, according to which a comparative analysis is performed. A conclusion was made about the choice among the presented devices.

Спектроскопические методы анализа основаны на способности атомов и молекул вещества испускать, поглощать или рассеивать электромагнитное излучение. Изменение интенсивности электромагнитного излучения после взаимодействия с веществом связано с качественным и количественным составом вещества, что обуславливает широкое распространение и интенсивное развитие методов спектроскопии в анализе [1].

Спектрофотометрический метод является абсорбционным методом и основан на измерении поглощения света. Процесс измерения происходит косвенно: сравнивается интенсивность излучения источника, падающего на жидкость и пройденного через нее. Изменение интенсивности может быть связано не только светопоглощением, но и рассеянием и отражением.

Для проведения спектрофотометрического анализа используется спектрофотометр – это высокоточный прибор, предназначенный для измерения параметров. К ним относятся спектральная зависимость степени поглощения, пропускания, оптическая плотность и концентрация растворов, веществ посредством видимого, инфракрасного, ультрафиолетового излучения. Принципиальная схема устройства представлена на рисунке 1.

Спектрофотометры работают на основе закона Бугера-Ламберта-Бера, который описывает взаимодействие света с жидкими и твердыми материалами. Когда свет проходит через рабочую жидкость, он поглощается частицами вещества, находящимися в растворе. Количество света, поглощенного жидкостью, зависит от ее концентрации, длины волны света и коэффициента экстинкции, который является характеристикой определенного вещества.



1) Источник света;
2) Линза;
3) Монохроматор;
4) Дифракционная решетка
5) Кювета с жидкостью;
6) Фотоэлемент;
7) Детектор;
8) Дисплей;

Рис. 1 – Принципиальная схема спектрофотометра

Спектрофотометры могут быть использованы для измерения различных свойств жидкостей, таких как: концентрация, качество воды, кинетические свойства воды.

Спектрофотометры имеют ряд преимуществ по сравнению с другими методами измерения свойств жидкостей:

1) Высокая точность и чувствительность: спектрофотометры могут измерять концентрации веществ в жидкостях на очень низком уровне. Они также обладают высокой точностью и повторяемостью измерений.

2) Быстрота и удобство: измерения с помощью спектрофотометров занимают относительно мало времени и не требуют сложной подготовки образцов. Они также могут быть легко интегрированы в автоматизированные системы анализа.

3) Возможность многократного использования: многие спектрофотометры позволяют измерять несколько образцов одновременно и использовать один и тот же инструмент для измерения различных параметров.

4) Широкий диапазон измерений: спектрофотометры могут измерять свойства жидкостей на широком диапазоне длин волн и концентраций, что делает их универсальным инструментом для различных областей науки и промышленности.

Для проведения сравнительного анализа спектрофотометров был выделен ряд характеристик, по которым необходимо произвести сравнения. Наиболее важные из них:

1) спектральный диапазон – это диапазон длин волн, в котором измеряются или наблюдаются электромагнитные волны. Спектральный диапазон важен для правильного выбора спектрофотометра для конкретных измерений, так как различные образцы могут иметь оптические свойства в разных диапазонах длин волн.

2) установка длины волны – важный параметр, который определяет оптимальную длину волны, в которой работает предоставленный образец. Бывает автоматическая и ручная.

3) погрешность – отклонение результатов измерения от истинных значений. Чем меньше погрешность, тем лучше прибор.

4) возможность подключения к компьютеру. При наличии такой возможность, существенно упрощается обработка результатов измерения.

5) стоимость оборудования.

Также в сравнении указывались другие параметры, которые не существенно влияют на результаты измерения, но влияют на удобство работы за прибором.

Для сравнения были выбраны три прибора отечественного производства: ПЭ-5300ВИ [2], УФ-1100 (Эковью) [3], В-1200 тм Эковью [3]. Результаты сравнения представлены в таблице 1.

Таблица 1 – Результат сравнения спектрофотометров

Наименование параметров	ПЭ-5300ВИ	УФ-1100 (Эковью)	В-1200 тм Эковью
Спектральный диапазон, нм	325-1000	200-1050	315-1050
Оптическая схема спектрофотометра	однолучевая	однолучевая	однолучевая

Диапазон показаний коэффициентов направленного пропускания, %	от 0,0 до 200,0	от 0,0 до 200,0	от 0,0 до 200,0
Пределы допускаемой абсолютной погрешности при измерении коэффициентов направленного пропускания, %	0,5	а) в спектральном диапазоне от 400 до 800, нм - ±0,5 б) в остальном спектральном диапазоне – ±1,0	а) в спектральном диапазоне от 400 до 800, нм - ±0,5 б) в остальном спектральном диапазоне – ±1,0
Установка длины волны	ручная	автоматическая	автоматическая
Погрешность установки длины волны, не более, нм	±2	±1,0	±1,0
Цифровой выход	USB	RS-232	USB
Напряжение питания частотой (50±1) Гц, В	85-250	220	220
Габаритные размеры, (Д х Ш х В), не более, мм	440 х 320 х 175	450×360×160	450х380х180
Стоимость, руб.	127 000	176 000	143 000

Таким образом, в результате проведенного анализа спектрофотометров, из представленных моделей, был выбран В-1200 тм Эковью от производителя ООО «Промышленные Экологические Лаборатории», так как данный прибор при средней цене имеет необходимый диапазон частот, обмен данными с компьютером, автоматическую установку длины волны и небольшую погрешность для полученных результатов.

Список литературы:

1) Дмитриевич И.Н., Пругло Г.Ф., Фёдорова О. В., Комиссаренков А.А. Физико - химические методы анализа. Ч.II. Оптические методы анализа: учебное пособие для студентов заочной формы обучения / СПбГТУРП. - СПб., 2014. - 39 с.
2) Официальный сайт ООО «ПО Компонент»: http://komponent-nov.ru/equipment/spectrum/detail.php?ID=1083
3) Официальный сайт ООО "Промышленные Экологические Лаборатории": https://pe-lab.ru/

Е.И. Гниломедов, И.И. Шестаков, Д.Ю. Овчинников

ОРГАНИЗАЦИЯ СИСТЕМЫ ЭЛЕКТРОПИТАНИЯ ОБОРУДОВАНИЯ В УЧЕБНОЙ ЛАБОРАТОРИИ ВОЛНОВОГО СПЕКТРАЛЬНОГО МУЛЬТИПЛЕКСИРОВАНИЯ УРТИСИ СИБГУТИ

Уральский технический институт связи и информатики (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге

Ключевые слова: электропитание, DWDM, NEC-4200, выпрямитель.

В статье рассматриваются вопросы организации электропитания оборудования DWDM NEC-4200 в лаборатории. В качестве источника электропитания задействована система УЭПС-2. В статье произведён анализ источника электропитания, разработана схема трассы прокладки кабелей электропитания и заземления. Для системы УЭПС-2 произведено исследование нагрузки при постепенном включении корзин четырёх стоек оборудования DWDM NEC-4200/ результатом исследования является график зависимости тока потребления от количества питающих корзин. График зависимости показывает, что для нормального функционирования оборудования DWDM NEC-4200 потребуется три блока ВББ 48/30-2К.

E.I. Gnilomedov, I.I. Shestakov, D.Y. Ovchinnikov

ORGANIZATION OF THE POWER SUPPLY SYSTEM FOR EQUIPMENT IN THE WAVELENGTH DIVISION MULTIPLEXING LABORATORY AT UTICI SSUTI

Ural Technical Institute of Communications and Informatics (branch) of the Federal State Budgetary Educational Institution of Higher Education «Siberian State University of Telecommunications and Informatics» in Yekaterinburg

Keywords: power supply, DWDM, rectifier.

The article discusses issues related to organizing the power supply of DWDM NEC-4200 equipment in a laboratory. The UEPS-2 system is used as the power source. The article analyzes the power source, develops a scheme for laying power cables and grounding. An investigation of the load is conducted for the UEPS-2 system by gradually turning on the four racks of DWDM NEC-4200 equipment, and the result is a graph showing the dependence of current consumption on the number of power baskets. The dependence graph shows that three blocks of VBV 48/30-2K will be required for normal functioning of the DWDM NEC-4200 equipment.

Современные телекоммуникационные системы представляют собой транспортные сети и сети доступа, основным оборудованием этих сетей являются станционные коммутаторы и мультиплексоры, для стабильной работы которых требуется не только организация качественных линий связи, но и системы электропитания.

Для того, чтобы студенты могли понять в процессе обучения, что такое система электропитания, как она организуется и функционирует, на кафедре многоканальной электрической связи УрТИСИ СибГУТИ было принято решение о создании «Лаборатории плотного волнового спектрального мультиплексирования», для которой будет организована система электропитания в рамках выпускной квалификационной работы.

Самый простой и доступный способ организации электропитания станционного оборудования — прямое подключение телекоммуникационного оборудования оператора связи к электросети сети 220В, однако у такой реализации есть существенный недостаток – это низкая надежность. Для повышения надежности системы электропитания применяется первый уровень обеспечения надежности – применение источника бесперебойного питания (ИБП). ИБП можно

подразделить на монтируемые в телекоммуникационную стойку и устанавливаемый в виде отдельного устройства похожего на телекоммуникационный шкаф высотой до двух метров. В состав ИБП входят аккумуляторные батареи, платы контроля и управления, платы стабилизации напряжения, платы резервирования. Основным недостатком применения ИБП является то, что они не могут обеспечить длительную работу аппаратуры в условиях отсутствия основных источников электроэнергии [1].

Так, для организации электропитания оборудования DWDM NEC-4200 в лаборатории, с реализацией всех возможных источников электропитания, проведен анализ этих источников, и в качестве источника электропитания будет задействована сеть 380В. Так, оборудование DWDM NEC-4200 планируется подключить к сети 380В через отдельно стоящее устройство электропитания связи (УЭПС) предназначенное для электропитания аппаратуры связи в буфере с аккумуляторной батареей и без неё постоянным током номинального напряжения 48 В, и включающая в себя систему стабилизации по напряжению, току и мощности, систему управления и мониторинга. В УЭПС подобного класса возможно установка аккумуляторных батарей, но учитывая особенности организации системы электропитания - образовательное учреждение, а не узел связи, необходимости в применении аккумуляторных батарей нет. [2]

Подключение УЭПС к сети 380В будет выполнено через посредством проектируемого электрического кабеля питания ВВГ с диаметром жил 2 мм через проектируемый автомат на 40А. Подключение оборудования DWDM к УЭПС будет выполнено двужильными кабелями ВВГпнг, которые будут проложены по проектируемому кабель-росту.

Таким образом реализованная система электропитания будет наглядным примером для студентов в процессе проведения лабораторных работ. В данной системе можно будет выполнять такие процессы, как просмотр состояния УЭПС, возможность управления, конфигурирование. Это позволит повысить знания и навыки выпускников УРТИСИ СИБГУТИ.

На основании поставленной задачи для реализации лаборатории плотного волнового спектрального мультиплексирования для запуска оборудования DWDM разработана схема электропитания на базе которой выполнено подключение УЭПС к сети 380В и к оборудованию. Схема электропитания представлена на Рисунке 1.

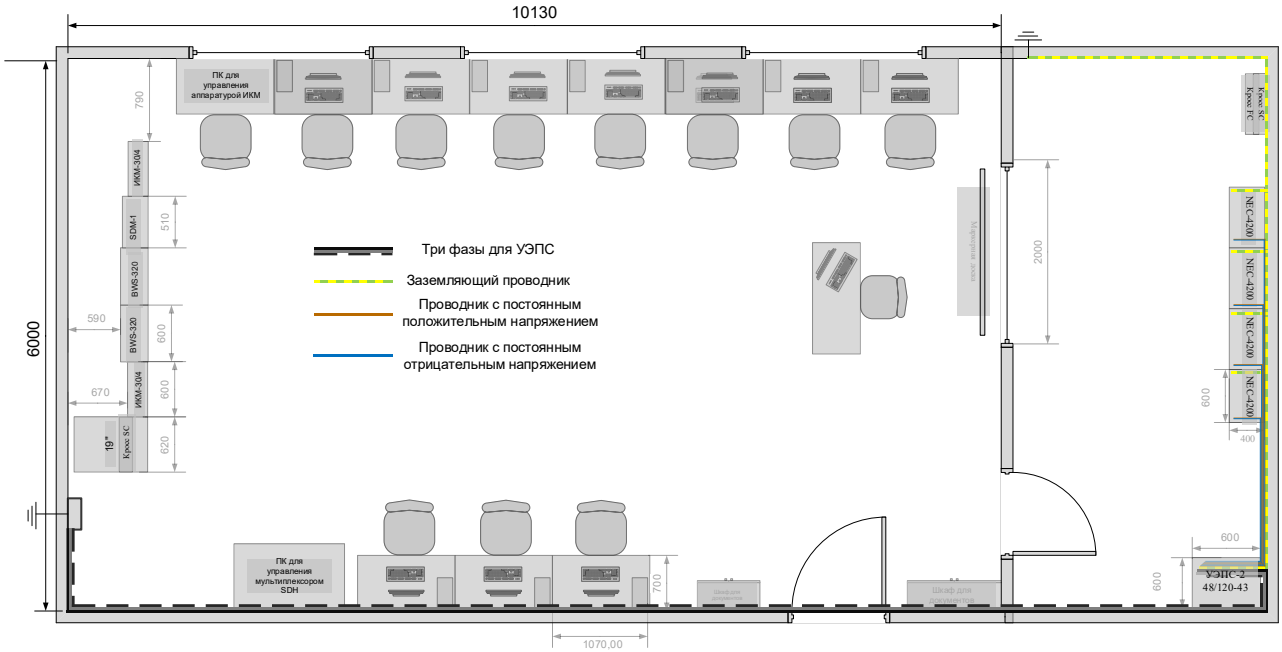


Рис. 1 – Схема электропитания оборудования DWDM

В работе рассмотрено исследование нагрузки на систему электропитания в зависимости от количества включенных корзин четырёх стоек DWDM NEC-4200, общее количество корзин составляет 12.

Результатом исследования являются численные значения нагрузки, которые представлены в таблицы 1 и 2, а также график зависимости, представленный на Рисунке 2.

Таблица 1 – Величина тока нагрузки в зависимости от количества работающих корзин

Количество корзин	Ток нагрузки, А
1	9
2	11,5
3	19,8
4	25,2
5	30
6	31,2
7	32,4
8	37
9	44,7
10	51,7
11	58
12	63

Таблица 2 – Количество горящих индикаторов на выпрямителе в зависимости от нагрузки

	Один выпрямитель	Два выпрямителя		Три выпрямителя		
	1-й ВБВ	1-й ВБВ	2-й ВБВ	1-й ВБВ	2-й ВБВ	3-й ВБВ
Количество горящих делений на выпрямителе	3	1	2	1	1	1
	4	2	2	1	1	1
	7	3	4	2	2	2
	10	5	5	3	3	3
	—	6	6	4	4	3
	—	6	6	4	4	3
	—	6	6	4	4	4
	—	7	7	5	4	4
	—	8	9	6	6	5
	—	10	10	7	6	6
	—	11	12	8	8	8
	—	—	—	8	8	8

Из таблицы 2 видно, что один выпрямитель обеспечивает питание только четырёх корзин, два выпрямителя - 11 корзин, а три выпрямителя - все 12 корзин. Теоретически, три выпрямителя могут обеспечить питанием до 16-18 корзин, в зависимости от потребляемой корзинами мощности.

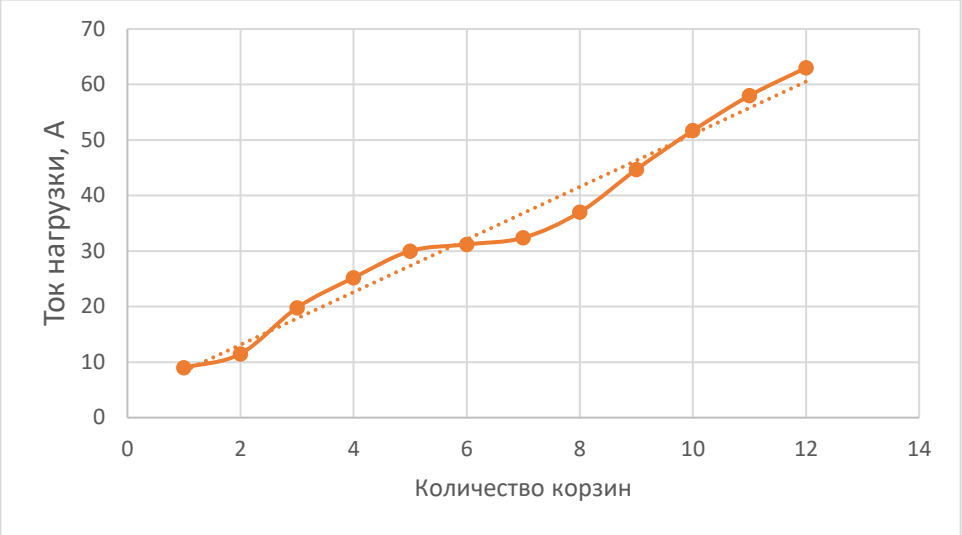


Рис. 2 ─ Отношение тока нагрузки к количеству включенных корзин

Для стабильной работы четырёх стоек рекомендуется задействовать все выпрямительные блоки, это позволит продлить их срок службы и обеспечит стабильную работу.

СПИСОК ЛИТЕРАТУРЫ:

1. Система бесперебойного и гарантированного электроснабжения (СБГЭ). [Электронный ресурс] - Режим доступа: https://www.estech.ru/poleznaya_informatsiya/prochie-stati/sistema-besperebojnogo -i-garantirovannogo-elektrosnabzheniya
2. Устройства электропитания связи УЭПС-2(К)-М [Электронный ресурс] - Режим доступа: https://promsd.ru/files/tech_opisanie_UEPS-2%28K%29-M.pdf

Е.И. Гниломёдов, И.С. Коновалов

РАЗРАБОТКА ПРОГРАММНОГО СИМУЛЯТОРА АППАРАТА ДЛЯ СВАРКИ ОПТИЧЕСКИХ ВОЛОКОН

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: программный симулятор, аппарат для сварки оптических волокон, 3D моделирование, программирование, обучение.

В работе рассмотрены вопросы разработки программного симулятора для сварки оптических волокон, описан его функционал, возможность его применения на учебных занятиях.

E.I. Gnilomedov, I.S. Konovalov

DEVELOPMENT OF A SOFTWARE SIMULATOR OF A DEVICE FOR WELDING OPTICAL FIBER

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: software simulator, optical fiber splicer, 3D modeling, programming, training.

The paper discusses the development of a software simulator for welding optical fibers, describes its functionality, the possibility of its use in training sessions.

Отрасль связи является одной из самых быстроразвивающихся отраслей, где применяются самые последние достижения науки и техники. С одной стороны, услуги связи для потребителей, основа для цифровой экономики и цифрового государственного управления, с другой - это инфраструктура сетей связи, которая завязана на такие смежные отрасли, как микроэлектроника и производство оборудования, разработка программных продуктов, информационная безопасность, прочее. Инфраструктура отрасли используется как платформа для развития современных сквозных технологий, таких как: передача больших данных, интернет вещей, промышленный интернет, сети радиодоступа. Развитие отрасли связи является приоритетной задачей, для решения которой, требуются хорошо резервированные сети связи, обеспечивающие надежный обмен информацией по раздельным потокам с разной скоростью разными протоколами взаимодействия [1].

В качестве линий связи, обеспечивающих передачу сообщений между оконечными устройствами, узлами связи на сетях в настоящее время используются волоконно-оптические линии связи (ВОЛС)., обладающие максимальной пропускной способностью и помехозащищенностью. Монтаж ВОЛС является сложной задачей и требует от персонала высокой квалификации. Применяемые в процессе монтажа и обслуживания инструменты и приборы, являются высокоточными, прецизионными аппаратами, в связи с чем имеющие высокую стоимость.

Обучение выполнению работ с применением подобной аппаратуры, требует больших вложений от учебных заведений, несет определенные риски в плане выхода из строя дорогостоящей техники в следствие недостаточной квалификации обучающихся при выполнении практических и лабораторных работ, которые являются важным элементом формирования навыков к определённым видам работ в процессе практической подготовки обучающихся, одной из основных форм организации учебного процесса при реализации образовательных программ высшей школы. Выходом из подобной ситуации является применение на первоначальном этапе освоения монтажного оборудования программных

симуляторов реальной аппаратуры. В частности, симуляторов аппаратов для сварки оптического волокна, применяемых при проведении монтажных работ на ВОЛС. Кроме того, программные симуляторы возможно использовать при проведении занятий в дистанционном режиме, когда затруднено использование реального оборудования.

Использование виртуальных симуляторов позволяет решать следующие задачи [2]:

− ознакомление обучаемого с внешним видом прибора, его устройством и режимами работы;

− отработка навыков выполнения основных операций на виртуальной модели как на реальном приборе;

− фиксирование ошибочных действий и контроль устранения таковых.

Основной задачей при разработке симулятора аппарата для сварки оптических волокон является создание максимально подобного виртуального интерактивного образа устройства и его интерфейса, реалистичное функционирование всех элементов управления, а также их адекватную физическую реакцию на действия обучаемого. Программный симулятор аппарата для сварки оптических волокон предназначен для обучения работе со сварочным аппаратом «Fudjikura FSM-30S», рис. 1.

Рисунок 1 – Внешний вид аппарата Fudjikura FSM-30S

В симуляторе реализована 3D модель данного аппарата, заложен функционал, позволяющий изучить конструкцию, внешний вид, основные органы управления. Основной целью разработки была реализация действий, основных операций, выполняемых монтажником при работе на реальном аппарате. В частности, операция зачистки оптического волокна, его скола, укладки в направляющие узлы, процедура сварки, процедура защиты получившегося сростка с помощью комплекта деталей защиты сростка. Разработка модели производилась с использованием среды 3D моделирования SketchUp Free, как самое простое бесплатное

программное обеспечение для 3D-моделирования. Программирование основных операций произведено с использование языка программирования JavaScript. Выбор языка связан с возможностью создать продукт, работающий на всех устройствах, оснащенных интернет браузерами. На рис. 2 представлена блок-схема алгоритма работы программного симулятора.

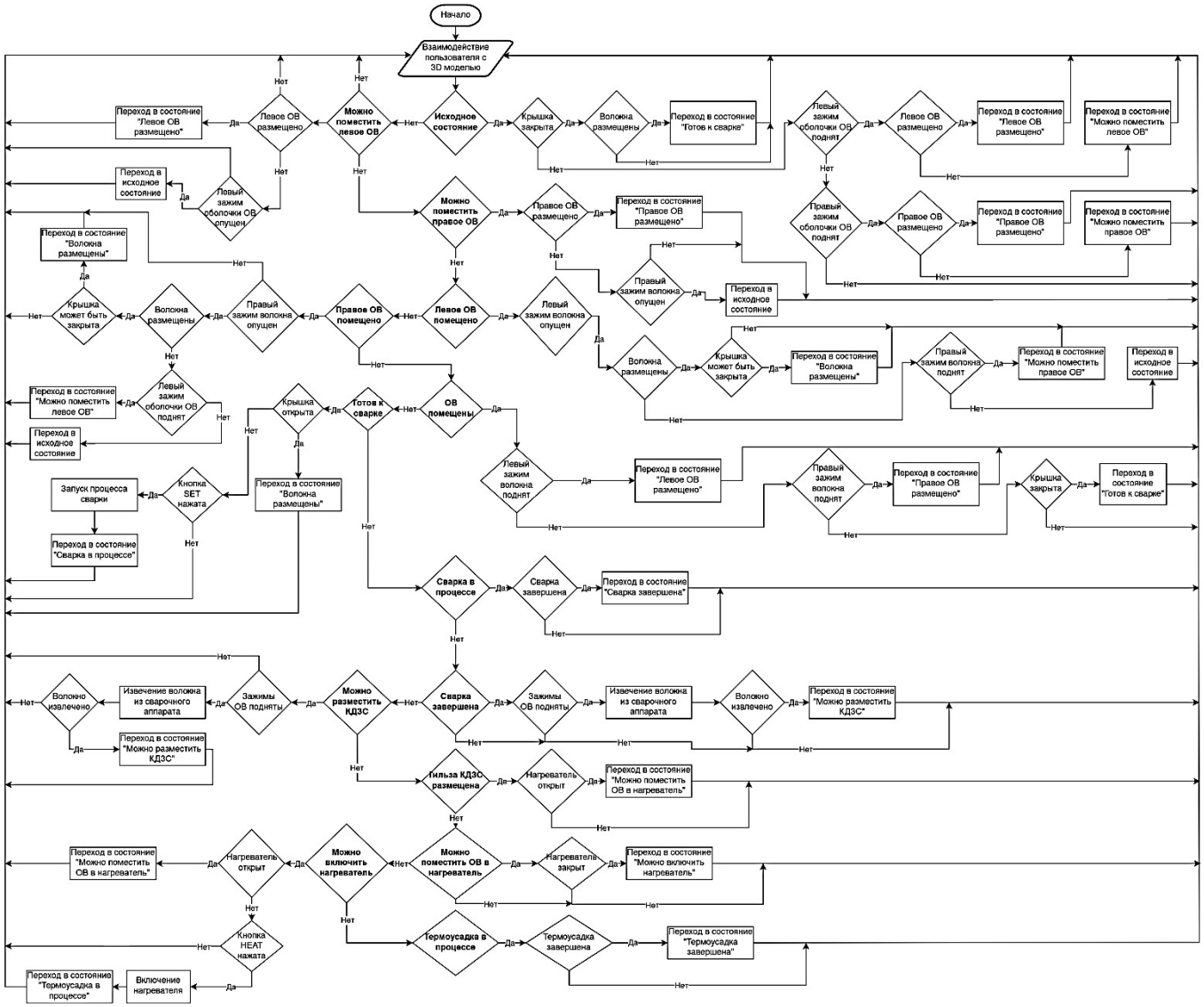


Рисунок 2 – Блок-схема алгоритма работы программного симулятора

Программный код оформлен в виде отдельных Fiber.js и InteractiveElement.js, которые подключаются к веб-страницам [3]. В результате, на экране браузера формируется изображение сварочного аппарата, а также возможно выполнение действий по монтажу оптического волокна, используя компьютерную мышь. Для удобства пользователя и понимания выполняемых действий, все основные операции сопровождаются появляющимися на экране подсказками, кроме того, есть возможность вызова глобального руководства пользователя на любом этапе работы с симулятором. Все процессы работы анимированы, что полностью погружает обучающегося в действия, выполняемые на реальном аппарате. Для более подробного исследования узлов устройства и его органов управления, программой предусматривается плавное приближение и удаление изображения с помощью колеса управления манипулятора. Активные к действию узлы при наведении курсора подсвечиваются другим цветом, с одновременным появлением возле курсора окна подсказки, поясняющей что необходимо сделать. Пример интерфейса работы с программным симулятором сварочного аппарата показан на рис.3.

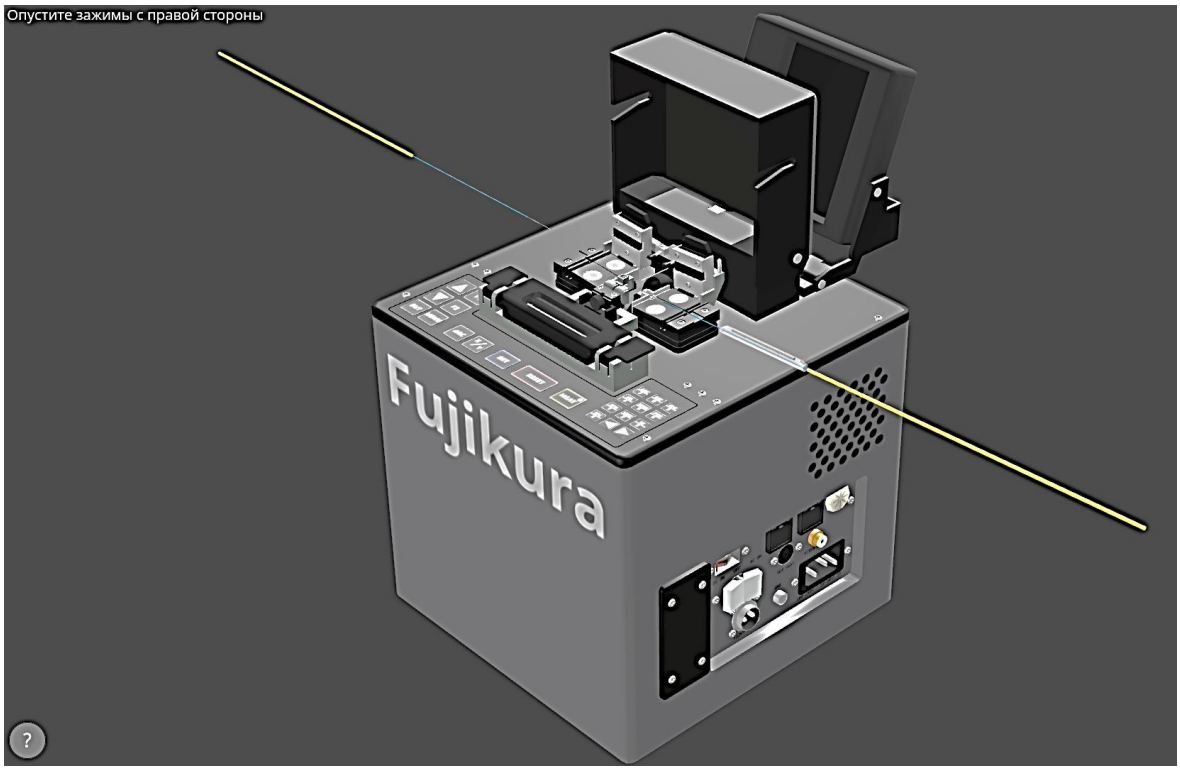


Рисунок 3 – Интерфейс программного симулятора

Таким образом использование программного симулятора для сварки оптических волокон модели Fudjikura FSM-30S в процессе проведения лабораторных и практических занятий при подготовке специалистов для отрасли связи, позволит улучшит процесс изучения студентами соответствующих разделов специальных дисциплин, повысить интерес обучающихся за счет наглядности представляемого материала, обезопасить оборудование от неквалифицированных действий студентов на первоначальном этапе освоения реального сварочного аппарата.

Разработанный программный продукт предполагается использовать при проведении практических занятий со студентами инфокоммуникационных вузов, при обучении основным приемам монтажа волоконно-оптических линий связи, на этапе теоретического изучения специализированного оборудования для монтажа ВОЛС, что в целом позволит значительно повысить качество подготовки выпускников направления «Инфокоммуникационные технологии и системы связи»

СПИСОК ЛИТЕРАТУРЫ:

1. Новости цифровой трансформации, телекоммуникаций, вещания и ИТ, https://www.comnews.ru/content/224892/2023-03-21/2023-w12/svyaz-rossii-poluchit-strategiyu
2. Дзюбенко, О.Л. Виртуальные симуляторы в системе высшего военного образования: монография / О.Л. Дзюбенко, М.В. Мищенко, А.О. Коженков. – М.: РУСАЙНС, 2020. – 146 с.
3. JavaScript. Основы программирования: учебно-методическое пособие. –Елец: Елецкий государственный университет им. И.А. Бунина, 2020 – 116 с.

М.О. Головлев, А.Л. Глебец, А.Н. Рагозин

АНАЛИЗ БИОМЕДИЦИНСКИХ ДАННЫХ С ПРИМЕНЕНИЕМ ЦИФРОВОЙ НЕЙРОСЕТЕВОЙ МОДЕЛИ НА ОСНОВЕ КАРТ КОХОНЕНА И АЛГОРИТМА КЛАСТЕРИЗАЦИИ К-СРЕДНИХ

Федеральное государственное автономное образовательное учреждение высшего образования «Южно-Уральский государственный университет (Национальный исследовательский университет)» (ФГАОУ ВО ЮУрГУ (НИУ)), Россия

Ключевые слова: самоорганизующуюся карта Кохонена, искусственная нейронная сеть, анализ биомедицинских данных.

В работе исследована возможность установления взаимосвязи между биомедицинскими показателями человека и его физиологическим состоянием – тревожности, утомления, болезни ОРВИ. На основе полученных данных – биомедицинских показателей – предложена модель цифровой системы определения дней болезненного состояния человека. Рассматривается подход, основанный на применении искусственной нейронной сети – самоорганизующихся карт Кохонена и алгоритма кластеризации k-средних.

M.O. Golovlev, A.L. Glebets, A.N. Ragozin

BIOMEDICAL DATA ANALYSIS BY THE USAGE OF A DIGITAL NEURAL NETWORK MODEL BASED ON KOHONEN MAP AND K-MEANS CLUSTERING ALGORITHM

Federal State Autonomous Educational Institution of Higher Education “South Ural State University (national research university)” (FSAEIHE SUSU (NRU)), Russia

Keywords: self-organizing Kohonen maps, artificial neural network, biomedical data analysis.

The article explores the possibility of establishing the interdependence between biomedical indicators of a person and his physiological state – anxiety, fatigue, ARVI disease. A model of the digital system for determining the days of a person's morbid state based on the obtained biomedical data (biomedical indicators) is proposed. The approach based on the usage of artificial neural network (self-organizing Kohonen maps) and k-means clustering algorithm is considered.

В работе рассматривается цифровая нейросетевая система обработки биомедицинских показателей человека. Система предназначена для распознавания паттернов тревожности и утомления в физиологическом состоянии человека.

При решении указанной задачи в процессе моделирования применяется подсистема приложения MATLAB SOM Toolbox, предоставляющая обширные возможности тестирования самоорганизующихся искусственных нейронных сетей (карт Кохонена) [1].

Концепция предлагаемой системы включает:

1. Первичную обработку исходных данных, предназначенную для приведения всех полученных исходных показателей к готовому для последующего анализа виду;
2. Кластеризацию данных, с применением искусственной нейронной сети Кохонена (карты Кохонена) [2];
3. Применение алгоритмов кластеризации для разбиения обученной карты Кохонена на области, соответствующих нормальным данным, то есть данным, соответствующим здоровому состоянию человека, и аномальным данным, то есть данным, соответствующим отклонению от нормы физиологического состояния человека;
4. Определение дней, когда человек находился в состоянии отклонения физиологического состояния от нормы.

Рассмотрим каждый из этапов в отдельности.

Анализ и группировка исходных данных.

В качестве исходных данных были приняты биомедицинские показатели людей, полученные в различные дни и время суток. Показатели сгруппированы в таблицы по времени, дате, идентификатору пациента.

Исходные данные включают следующие показатели: пульс, температура, показатель двигательной активности, уровень насыщения крови кислородом, показатель функционального напряжения нервной системы, два показателя сопротивления кожного покрова.

Однако не все показатели получены одновременно, среди них также имеются пропуски, то есть недостающие записи. В следствие различной размерности показателей в исходных данных, разработан алгоритм дополнения пропущенных значений.

Привязка ко времени снятия показателей позволяет точно определить, когда был пропущен тот или иной показатель. Далее, используется алгоритм интерполяции с методом ближайшего соседа для заполнения пропущенных или неопределенных значений.

В результате обработки исходных данных, принято решения использовать 5 биомедицинских показателей, 4 из которых присутствуют в каждом исходном файле, назовем их стандартными, это – показатель функционального напряжения нервной системы, температура, два показателя сопротивления кожного покрова. Пятый показатель является вариативным, в зависимости от наличия в исходных данных, и представляет собой данные об измерении пульса, либо данные о двигательной активности.

Для последующего анализа происходит объединение обработанных данных одного пациента, полученных за несколько дней, в единую матрицу.

Кластеризация данных с применением карт Кохонена.

В качестве контрольных данных будем считать таблицы, отражающие показатели человека, подверженного состоянию тревожности. Анализу подвергаются 4 стандартных показателя, пятым показателем в данном случае будут данные о пульсе.

Сформируем матрицу, содержащую показания человека в дни, когда его истинное состояние неизвестно. Количество анализируемых измерений (записей) составляет 4087 за 35 дней.

Применим самоорганизующуюся нейронную сеть Кохонена (карту Кохонена), кластеризующую данные с неизвестным состоянием человека. Карта имеет размер 30x30 нейронов с гексагональной топологией размещения этих нейронов. В процессе обучения карты (по данным с неизвестным состоянием человека) происходит автоматическая настройка весов нейронов для отображения обучающих данных. По завершению обучения карты Кохонена выводятся демонстрационная унифицированная матрица расстояний между нейронами карты Кохонена и карта попаданий обучающих примеров в кластеры карты Кохонена (рис. 1).

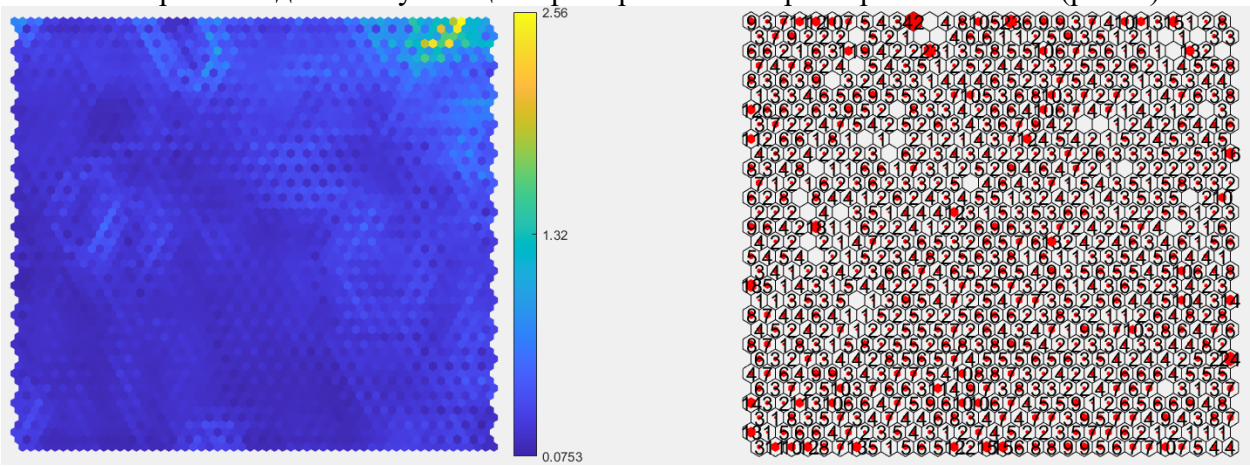


Рис. 1. Унифицированная матрица расстояний между нейронами карты Кохонена (слева) и карта попаданий обучающих примеров в кластеры карты Кохонена (справа)

Применение алгоритмов кластеризации к обученной карте Кохонена.

Далее необходимо разбить на кластеры уже обученную карту Кохонена (для выявления схожих по структуре участков карты). Для этого могут быть применены различные алгоритмы кластеризации. Будем использовать для указанной цели алгоритм k-средних.

Оптимальное количество кластеров на карте определим путем вычисления индекса Дэвиса-Болдина. Минимальное значение индекса соответствует наиболее оптимальному количеству кластеров. В рассматриваемом случае оптимальное количество кластеров составило 13. Границы соответствующих кластеров на обученной карте Кохонена представлены на рис. 2.

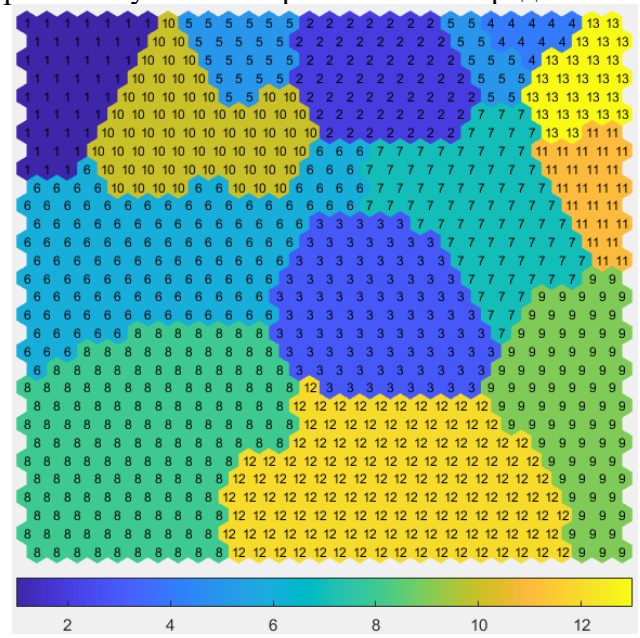


Рис. 2. Анализ структуры карты Кохонена с помощью алгоритма k-средних

Далее необходимо воспользоваться контрольными данными, отражающими показатели человека, подверженного состоянию тревожности. В частности, необходимо соотнести данные с известным состоянием человека с картой Кохонена, обученной на данных с неизвестным состоянием человека. Для этого строится карта попаданий контрольных данных в сформированные алгоритмом k-средних кластеры карты Кохонена (рис. 3).

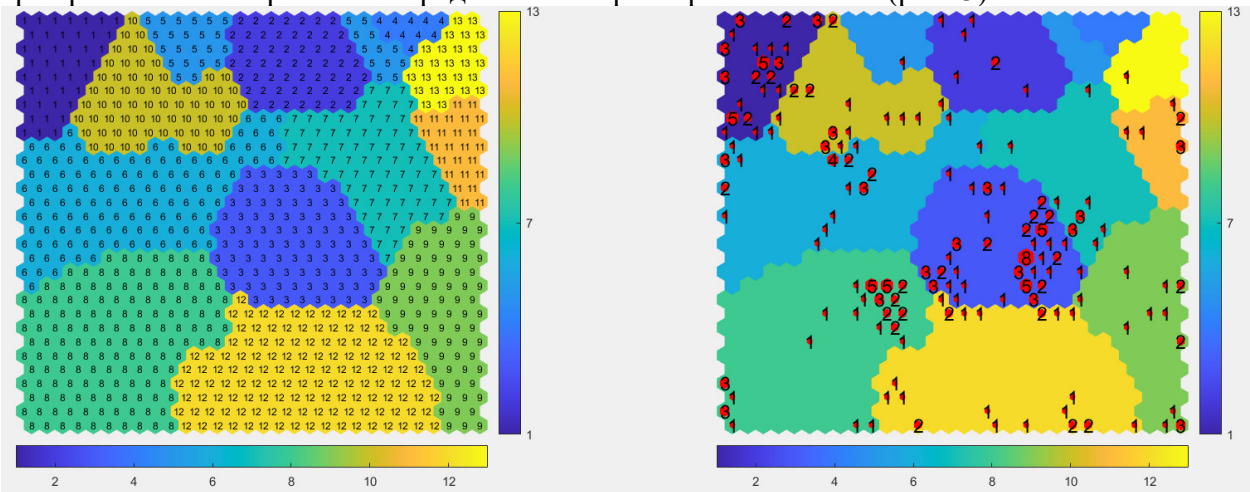


Рис. 3. Кластеры карты Кохонена, выявленные алгоритмом k-средних, (слева) и распределение контрольных данных по кластерам карты Кохонена, выявленных алгоритмом k-средних (справа)

Определение дней, когда человек находился в состоянии болезни.

Для определения дней, когда человек находился в состоянии болезни, требуется вычислить относительный показатель, отражающий число контрольных записей (с показаниями больного человека), приходящихся на один нейрон того или иного кластера. В связи с этим необходимо выполнить подсчет количества нейронов, входящих в каждый кластер карты.

По относительному показателю возможно определение «аномальных» кластеров, то есть кластеров, которые предположительно отражают данные, связанные с болезнью. Для рассматриваемого случая определяем из сформированных 13 кластеров «аномальные», используя критерий – превышение величины 2-х средних от значения относительного показателя, вычисленного для каждого из 13 кластеров. Таким образом, были определены «аномальные» кластеры №1 и №3 (рис. 3).

После того, как были определены «аномальные» кластеры карты, необходимо определить те записи из анализируемых данных, которые попали в указанные «аномальные» кластеры. Далее необходимо агрегировать данные по всем исследуемым дням в единую таблицу (рис. 4). Она должна включать:

1. Перечень анализируемых дней (периодов) с неизвестным состоянием человека;
2. Общее число записей (измерений) в каждый из исследуемых дней (периодов);
3. Предполагаемое число «аномальных» записей в каждый из исследуемых дней (периодов). Данный показатель определяется по числу записей, попавших в «аномальные» кластеры;
4. Процент «аномальности» каждого исследуемого дня (периода), как отношение числа «аномальных» измерений к общему числу измерений.

Day_Time	Total_measurement	Abnormal_measurement	Percent_of_abnormality
2022.03.05_12,14	134	2	1,492537313
2022.03.07_07-40-01	99	3	3,03030303
2022.03.08_13,43	132	83	62,87878788
2022.03.09_07-42-02	169	4	2,366863905
2022.03.11_13-30-03	110	10	9,090909091
2022.03.13_08-31-26	87	10	11,49425287
2022.03.14_07-40-11	174	55	31,6091954
2022.03.18_7,36	162	49	30,24691358
2022.03.19_7,52	175	65	37,14285714
2022.03.20_8,35	157	13	8,280254777
2022.03.21_7,50	172	19	11,04651163
2022.03.23_07-40-37	135	10	7,407407407
2022.03.25_07-43-23	174	67	38,50574713
2022.03.26_11-01-54	145	9	6,206896552
2022.03.27_08-49-07	175	57	32,57142857
2022.03.28_07-57-13	168	2	1,19047619

Рис. 4. Таблица агрегированных данных

Для выявления конкретных дней, отражающих болезненное состояние человека, возможно применение различных пороговых критериев. На основе выбранного критерия будет приниматься решение об учете каждого дня как аномального (отражающего болезненное состояние) или нормального (отражающего здоровое состояние).

Таким образом, указанный подход, с применением нейросети типа карты Кохонена и алгоритма кластеризации k-средних, может быть применен для выявления различных болезненных состояний человека по его биомедицинских показателям.

Данные для проведения исследования были предоставлены *ООО «Нейротехнолоджи» (г. Челябинск).*

СПИСОК ЛИТЕРАТУРЫ:

1. Vesanto J., Himberg J., Alhoniemi E., Parhankangas J. SOM Toolbox for Matlab 5. Espoo, Helsinki University of Technology, 2000. 59 p.
2. Кохонен, Т. Самоорганизующиеся карты / Т. Кохонен; пер. с англ. В.Н. Агеева. – М.: БИНОМ. Лаборатория знаний, 2008. – 655 с.

Н.И. Горлов

МОНИТОРИНГ ПОДВОДНЫХ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ),
г. Новосибирск, Россия

Ключевые слова: мониторинг, оптическая линия связи, когерентный оптический рефлектометр, отношение сигнал/шум, терминальное оборудование.

В статье проанализированы основные принципы и структурные схемы включения оборудования мониторинга подводных волоконно-оптических линий связи. Представлены результаты сравнения функциональных возможностей пассивного и активного методов мониторинга. Особую значимость имеют оценки основных метрологических параметров. При этом обоснована необходимость применения когерентного оптического рефлектометра, позволяющего улучшить чувствительность мониторинга до квантового предела за счет гетеродинного детектирования.

N.I. Gorlov

MONITORING OF UNDERWATER FIBER-OPTIC COMMUNICATION LINES

Siberian State University of Telecommunications and Informatics
(SibGUTI), Novosibirsk, Russia

Keywords: monitoring, optical communication line, coherent optical reflectometer, signal-to-noise ratio, terminal equipment.

The article analyzes the basic principles and structural schemes for the inclusion of monitoring equipment for underwater fiber-optic communication lines. The results of comparing the functionality of passive and active monitoring methods are presented. Estimates of the main metrological parameters are of particular importance. At the same time, the necessity of using a coherent optical reflectometer is justified, which makes it possible to improve the sensitivity of monitoring to the quantum limit due to heterodyne detection.

1. Введение

В процессе строительства и технической эксплуатации подводных волоконно-оптических линий связи (ВОЛС) необходимо проводить комплекс измерений с целью определения технического состояния и предупреждения повреждений волоконно-оптических кабелей (ВОК). В перечень обязательных к контролю параметров ВОК относятся вносимые потери, коэффициенты затухания и отражения. Для проведения измерений предлагается применение универсальной измерительной системы для тестирования и мониторинга**.** Оборудование должно быть развернуто на каждой оконечной станции для обеспечения текущего мониторинга с целью технического обслуживания. Мониторинг состояния системы может быть получен путем периодического сбора данных о производительности с подводной станции. Кроме того, для удобства обслуживания оно должно поддерживать или предоставлять интерфейсы для поиска неисправностей.

2. Конфигурации систем мониторинга

Для конфигурации соединения оборудования мониторинга (monitoring equipment) в подводной кабельной системе можно выбрать два различных способа:

•Терминальное передающее оборудование подключается между оборудованием мониторинга и кабельным оконечным оборудованием, см. рис. 1. Сигналы мониторинга и

служебные сигналы объединяются в терминальном передающем оборудовании и передаются в подводную кабельную систему [1].

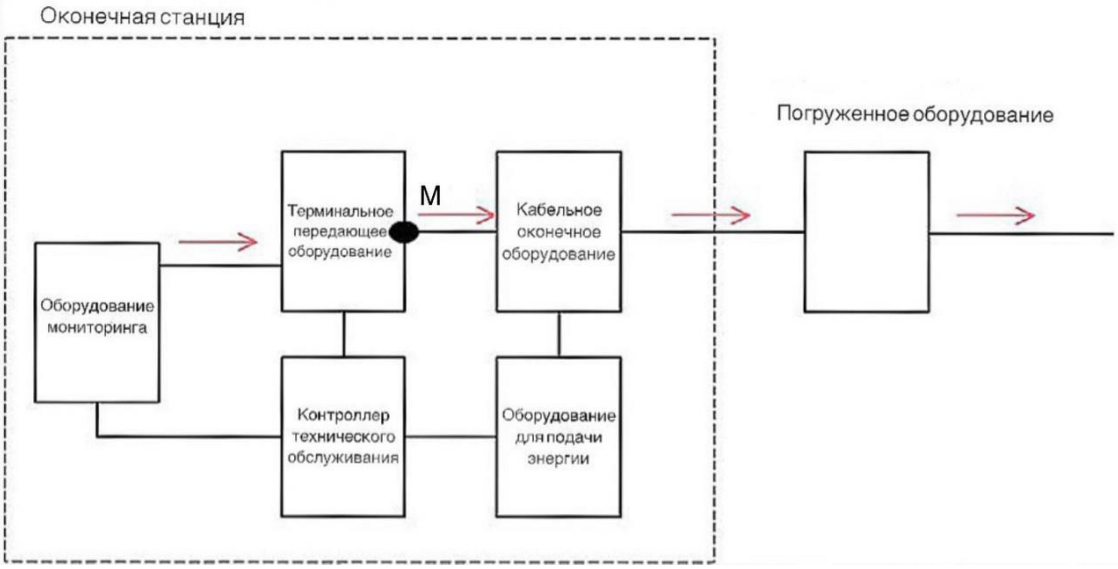


Рис. 1. Схема включения терминального передающего оборудования между оборудованием мониторинга и входом зондируемой кабельной системы

• Оборудование мониторинга подключается между терминальным передающим оборудованием и кабельным оконечным оборудованием (см. рис. 2), сервисные сигналы и сигналы мониторинга объединяются в оборудовании мониторинга и передаются в подводную кабельную систему.

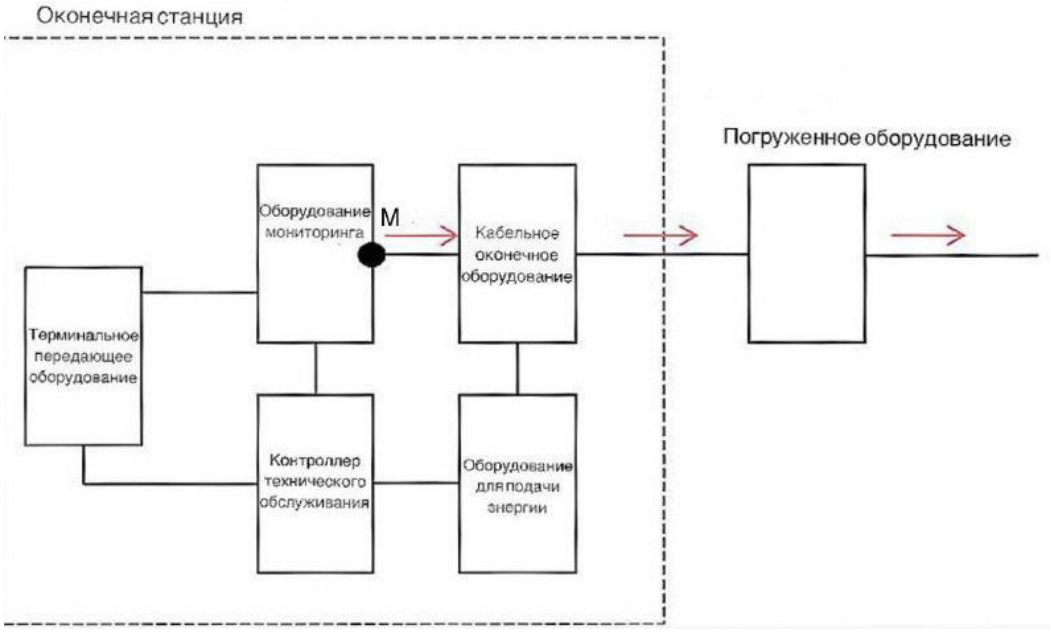


Рис. 2. Схема включения оборудования мониторинга между терминальным передающим оборудованием и входом зондируемой кабельной системы

В точке M выходной интерфейс мониторинга должен соответствовать следующим параметрам:

• выходная мощность зондирующего сигнала, длина волны и ширина импульса (для пассивного мониторинга);

• параметры модуляции (для активного контроля).

Сигналы зонда посылаются на погруженную установку, а возвращенные сигналы анализируются, чтобы отразить состояние работоспособности системы. Например, рассеянный назад свет когерентного рефлектометра, описанного в [2], обнаруживается и обрабатывается, обычно в виде кривых зависимости интенсивности сигнала от расстояния для анализа и

диагностики состояния системы. Одно оборудование для пассивного мониторинга контролирует производительность подводной кабельной системы в одном направлении. Чтобы получить двунаправленную производительность, оборудование для пассивного мониторинга должно быть развернуто на каждой оконечной станции.

При пассивном мониторинге рекомендуется отслеживать изменения состояния в зондируемых оптических путях, такие как обрывы волокон, изменения усиления ретранслятора, а также затухание или отражения волокон. Поскольку пассивный мониторинг получает информацию о состоянии системы косвенным путем, при мониторинге состояния используется сравнение с базовыми показателями. Мониторинг состояния должен использовать те же параметры, что и базовые линии, чтобы обеспечить достоверность сравнения и найти изменения в работе, вызванные повреждениями или неисправностями, которые изменяют состояние системы. Базовые показатели должны быть собраны после надлежащего развертывания системы идолжны обновляться после каждого ремонта или изменения конфигурации системы.

3. Применение когерентного оптического рефлектометра

Метрологические характеристики систем мониторинга значительно улучшаются посредством применения когерентного приема. Он предполагает применение лазерного гетеродина, акусто - оптического модулятора, оптического приемника и калиброванных аттенюаторов. При этом становится возможным существенно увеличить чувствительность фотоприемного устройства. Этот метод приема обратного рассеянного сигнала позволяет также снизить требования по стабильности частоты оптического излучения. Техническая реализация применяемого метода приема иллюстрируется на рисунке 3.

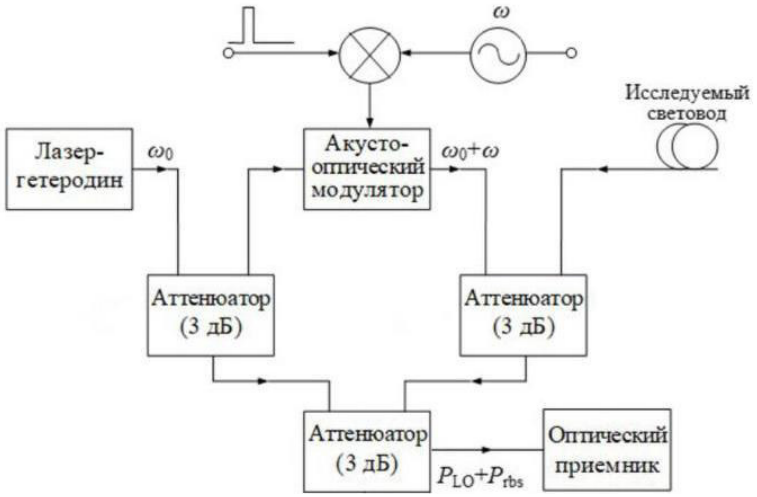


Рис. 3. Техническая реализация когерентного приема

За счет гетеродинного детектирования чувствительность мониторинга увеличивается до квантового предела. Высокоточное разрешение при поиске неисправностей всегда полезно для технического обслуживания. Рекомендуются удобные функции, например, автоматическое определение места повреждения, быстрое определение места повреждения с меньшей погрешностью, но за более короткое время. Подводное оборудование должно иметь обратные пути, как описано в [3], для когерентного приема. При активном мониторинге оборудование мониторинга запрашивает и собирает непосредственно статус производительности погруженного оборудования. Соответствующими параметрами производительности являются входная мощность, выходная мощность, ток насоса и т.д.

4. Основные метрологические характеристики

Абсолютная погрешность измерения координаты неоднородности в оптическом волокне определяется длительностью зондирующего импульса. Как и в некогерентной рефлектометрии, она может быть оценена по формуле:

$$\Delta L_{изм.} = C_0 t_и / 2n_g \,, \qquad (1)$$

где: $\Delta L_{изм.}$- абсолютная погрешность измерения координаты;

C_0 –скорость света в свободном пространстве;

$t_и$ – длительность зондирующего импульса;

n_g – групповой коэффициент преломления сердцевины.

В оптическом приемнике имеют место шумы, обусловленные преимущественно темновым током диода. Гетеродин и другие компоненты оптического приемника тоже вносят свой вклад в результирующую мощность шума. Составляющая шума этих элементов может быть выражена через эквивалентную мощность P_{NEP}. Соотношение сигнал/шум описывается соотношением:

$$\mathrm{SNR} = \frac{2P_{LO}P_{rbs}\left[\frac{e\eta}{\eta\omega}\right]^2}{2eB\left\{i_d + P_{LO}\left[\frac{e\eta}{\eta\omega_0}\right] + P_{NEP}\left[\frac{e\eta}{\eta\omega_0}\right]\right\}}, \quad (2)$$

где e – заряд электрона, $\hbar\omega$ – энергия фотона, η – квантовый выход фотодетектора, P_{LO} – мощность гетеродина, P_{rbs} – мощность регистрируемого сигнала, B – ширина полосы пропускания приемника.

Так как мощность сигнала гетеродина значительно превышает уровень шумов, то она является доминирующей относительно других компонентов. В этой связи отношение сигнал/шум примет следующий вид:

$$\mathrm{SNR} = \frac{\eta P_{rbs}}{\eta\omega_0 B}. \quad (3)$$

Последнее выражение обеспечивает максимальную чувствительность фотоприемного устрйства, которая приближается к квантовомеханическому пределу. Скорость акустооптического модулятора и его способностью генерировать как можно более короткие импульсы предопределют разрешающую способность по пространственной координате системы оптического мониторинга.

5. Заключение

Техническое состояние подводных волоконно - оптических линий связи может быть эффективно оценено посредством периодического сбора данных с помощью системы мониторинга. Когерентная оптическая рефлектометрия является перспективной технологией мониторинга подводных волоконно - оптических линий связи. Она позволяет операторам связи обслуживать большое количество подводных объектов. Дальнейшим развитием в исследуемой области, по мнению автора, являются исследования предельных функциональных возможностей, метрологическое обоснование технических требований к основным компонентам и создание системы метрологического обеспечения систем мониторинга.

СПИСОК ЛИТЕРАТУРЫ:

1. Recommendation ITU-T G.979, “Characteristics of monitoring systems for optical submarine cable systems,” 2012.
2. Xiong J., Wang Z. Single-Shot COTDR Using Sub-Chirped-Pulse Extraction Algorithm for Distrib uted Strain Sensing // Journal of Lightwave Technology, vol. 38, no. 7, april 1, 2020, pp. 2028-2035.
3. IEC61746-1 (2009), Калибровка оптических рефлектометров с временной диаграммой направленности (OTDR) - Часть 1: Рефлектометры для одномодовых волокон.
4. Recommendation ITU-T G.977 (2011), Characteristics of optically amplifiedoptical fibre submarine cable systems.

Н.И. Горлов

АНАЛИЗ ВЛИЯНИЯ ВАРИАЦИЙ МОДУЛЯ ЮНГА НА МОЩНОСТЬ И СДВИГ ЧАСТОТЫ СПЕКТРА РАССЕЯНИЯ БРИЛЛЮЭНА

Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ),
г.Новосибирск, Россия

Ключевые слова: модуль Юнга, рассеяние Бриллюэна, распределенное зондирование по оптическому волокну, изменение мощности и частоты по Бриллюэну, термическая деформация.

В статье проанализировано влияние изменений модуля Юнга сердцевины чувствительного волокна на мощность и изменение сдвига частоты Бриллюэна. Представлена линейная формула между модулем Юнга и параметрами оптического сигнала обратного рассеяния Бриллюэна. Показана возможность измерения температуры и термических деформаций вдоль волокна по результатам распределенного зондирования, основанного на комбинированном эффекте рассеяния Бриллюэна и изменении модуля Юнга в широких диапазонах измеряемых параметров.

N.I. Gorlov

ANALYSIS OF THE INFLUENCE OF YOUNG'S MODULUS VARIATIONS ON THE POWER AND FREQUENCY SHIFT OF THE BRILLOUIN SCATTERING SPECTRUM

Siberian State University of Telecommunications and Informatics (SibGUTI),
Novosibirsk, Russia

Keywords: Young's modulus, Brillouin scattering, distributed optical fiber sensing, Brillouin power and frequency variation, thermal deformation.

The article analyzes the effect of changes in the Young's modulus of the core of a sensitive fiber on the power and the change in the Brillouin frequency shift. A linear formula is presented between the Young's modulus and the parameters of the Brillouin optical backscattering signal. The possibility of measuring temperature and thermal deformations along the fiber based on the results of distributed sensing based on the combined Brillouin scattering effect and the change in Young's modulus in wide ranges of measured parameters is shown.

1. Введение

Волоконно - оптические распределенные сенсорные системы на основе рассеяния Бриллюэна вызвали большой интерес благодаря их потенциальным возможностям одновременного измерения и обнаружения изменений температуры и деформации. Особенно они широко используются для контроля изменений температуры и деформации не только в подземных, воздушных и подводных кабелях связи, а также в аэрокосмической и нефтяной промышленности и гражданских инженерных сооружениях, таких как мосты, туннели, большие здания и т.д. В этих системах, используя информацию об изменении частоты Бриллюэна и изменении мощности Бриллюэна для оптического сигнала обратного рассеяния в чувствительном волокне, можно легко получить требуемые данные, относящиеся к тепловым характеристикам окружающей среды. Поскольку модуль Юнга сердцевины кремнеземного волокна зависит как от температуры, так и от деформации, для определения этих двух параметров вдоль чувствительного волокна также можно использовать изменения модуля Юнга. Распределенные сенсорные системы основаны на взаимодействии фотонов с генерируемыми термически акустическими волнами и обнаружении обратного рассеянного оптического сигнала.

2. Температурные и деформационные зависимости изменения мощности и сдвига частоты Бриллюэна

Предполагая, что мощности оптического сигнала, распространяющегося в прямом направлении вдоль волокна, и сигнала обратного рассеяния равны, мощность сигнала Бриллюэна может быть задана как функция времени t [1]

$$P_B(t) = 0{,}5P_0\tau\gamma_B S\nu_g e^{(-\gamma_R \nu_g t)},$$

где P_0 - пиковая мощность сигнала лазерной накачки, τ - длительность импульса, y_B и y_R - коэффициенты обратного рассеяния Бриллюэна и Рэлея соответственно, S - коэффициент захвата, v_g - групповая скорость света, распространяющегося в волокне, t – текущее время. Используя уравнение t = 2z / vg, мощность Бриллюэна P_B может быть получена как функция расстояния z, как в [2, 3]

$$P_B(z) = 0{,}5P_0\tau\gamma_B S\nu_g e^{(-2\gamma_R z)}.$$

Хотя коэффициент обратного рассеяния Бриллюэна y_B имеет прямую зависимость от изменений температуры окружающей среды, коэффициент обратного рассеяния Рэлея y_R не имеет такой прямой зависимости [1]. Следовательно, влияние изменений температуры на мощность сигнала Бриллюэна происходит через y_B, который может быть записан как [2, 3]

$$\gamma_B = \frac{8\pi^3 n^8 p^2 kT(\rho v_a^2)^{-1}}{3\lambda_0^4},$$

где n - показатель преломления сердцевины волокна, p - коэффициент фотоупругости (Поккеля) (~ 0,286), k - постоянная Больцмана (1,38 × 10-23 Дж/°К), T - температура волокна в пересчете на °K, ρ - плотность кремнеземного волокна (ρ = 2330 кг/м3), v_A - скорость акустической волны в стекле, а λ_0 - длина волны света, попадающего в волокно (λ_0 = 1550 нм) [2, 3].

В механизме рассеяния Бриллюэна оптическая волна, накачиваемая лазерным источником в волокно, взаимодействует с термически генерируемыми акустическими волнами в среде и, следовательно, рассеивается под углом θ [2]. Термически генерируемые акустические волны имеют широкополосный частотный спектр. Когда оптическая волна, накачиваемая в волокно, совпадает по фазе с акустической волной, т.е. когда возникает условие Брэгга, сдвиг частоты Бриллюэна происходит на определенную величину. Это значение равно частоте акустической волны f_a.

Акустическая частота fa, удовлетворяющая условию Брэгга, может быть описана как

$$f_a = \frac{2n}{\lambda_0}\nu_a \sin\frac{\theta}{2},$$

где θ - угол между оптической волной, накачанной в волокне, и рассеянной волной Бриллюэна.

В оптических волокнах рассеянная оптическая волна направляется только в прямом или обратном направлениях. Если оптическая волна рассеивается в направлении, противоположном направлению накачиваемой волны, т.е. когда θ = 180º, то акустическая частота fa максимизируется. Поскольку сдвиг частоты Бриллюэна V_B равен акустической частоте fa, то можно записать [4]

$$V_B = \frac{2n}{\lambda_0}\nu_a.$$

Поскольку мощность Бриллюэна PB и сдвиг частоты Бриллюэна VB изменяются с изменением температуры и деформации, уравнения, описывающие температурные и деформационные зависимости изменения мощности Бриллюэна (ΔP_B) и изменения сдвига частоты Бриллюэна (ΔV_B), могут быть заданы в виде [2]

$$\Delta P_B = K_T^P \Delta T + K_\epsilon^P \Delta \epsilon,$$

$$\Delta V_B = K_T^V \Delta T + K_\epsilon^V \Delta \epsilon,$$

где K_T^P и K_ϵ^P - коэффициенты температуры и деформации изменения мощности Бриллюэна, соответственно, K_T^V и K_ϵ^V - коэффициенты температуры и деформации изменения частоты Бриллюэна, соответственно, ΔT и $\Delta \epsilon$ - изменения температуры и деформации, происходящие вдоль чувствительного волокна, соответственно.

Характеристики датчиков распределенных волоконно-оптических сенсорных систем оцениваются с помощью разрешения температуры и термической деформации. Соответствующие разрешения для температурных и термодеформационных образований, возникающих вдоль чувствительного волокна, могут быть вычислены с помощью [2]

$$\delta_T = [|K_\epsilon^P \delta V| + |K_\epsilon^V \delta P|]/\left[\left|K_\epsilon^V K_T^P - K_\epsilon^P K_T^V\right|\right],$$
$$\delta_\epsilon = \left[\left|K_T^P \delta V\right| + \left|K_T^V \delta P\right|\right]/\left[\left|K_\epsilon^V K_T^P - K_\epsilon^P K_T^V\right|\right],$$

где δT и $\delta \epsilon$ - разрешения по температуре и термической деформации соответственно, δP и δV - среднеквадратичные значения шума, возникающие при изменении мощности по Бриллюэну и изменении сдвига частоты по Бриллюэну соответственно.

3. **Зависимости мощности и сдвига частоты Бриллюэна от изменения модуля Юнга**

Модуль Юнга является одним из фундаментальных критериев, используемых для описания упругих свойств материала. Когда к объекту прикладывается внешняя сила, в зависимости от характеристик материала, объект подвергается продольному и поперечному удлинению, которые создают одноосные напряжения и деформации в материале объекта в соответствии с законом Гука [5]. Модуль Юнга, т.е. модуль упругости, определяется как отношение изменения напряжения в любой точке материала к изменению деформации в этой точке как [5]

$$E = \frac{\sigma}{\epsilon} = \frac{F/S}{\Delta L/L'},$$

где σ обозначает растягивающее напряжение, а ϵ обозначает растягивающую деформацию, возникшую на объекте, F - сила, действующая на объект, S - площадь поперечного сечения, на которую действует сила, ΔL - величина изменения длины, а L - исходная длина объекта.

Модуль Юнга волокна из плавленого кремнезема линейно изменяется в зависимости от температуры окружающей среды и образования термических деформаций в среде. Зависимости модуля Юнга сердцевины из кремнеземного волокна от температуры и термической деформации могут быть представлены соответственно в виде [1]

$$E = 69.68 + 1.126x10^{-2}T,$$

$$E = E_0(1 + 5.75x\ \epsilon),$$

где E - модуль Юнга сердцевины волокна в пересчете на ГПа, E_0 - значение модуля Юнга при нулевой деформации и температуре 293 °K, т.е. E_0 = 72,97918 ГПа, T_k - температура в пересчете на °K, ϵ - деформация.

Изменение мощности по Бриллюэну ΔP_B и изменение частоты по Бриллюэну ΔV_B могут быть записаны соответственно

$$\Delta P_B = K_T^P \Delta T_C + K_\epsilon^P \Delta \epsilon\ ,$$

$$\Delta V_B = K_T^V \Delta T_C + K_\epsilon^V \Delta \epsilon,$$

где ΔT_C и $\Delta \epsilon$ - изменения температуры и деформации, происходящие вдоль чувствительного волокна, соответственно.

Изменение мощности по Бриллюэну и изменение сдвига частоты по Бриллюэну вдоль чувствительного волокна могут быть получены как

$$\Delta P_B(L) = K_T^P T_C(L) + K_\epsilon^P \in (L),$$

$$\Delta V_B(L) = K_T^V T_C(L) + K_\epsilon^V \in (L).$$

Изменение мощности Бриллюэна и изменение сдвига частоты Бриллюэна можно записать как функцию модуля Юнга как

$$\Delta P_B(E) = 29.827xE - 2169.550,$$

$$\Delta V_B(E) = 209.413xE - 15260.766,$$

где E - модуль Юнга сердцевины чувствительного волокна в ГПа. Как очевидно из уравнений, существует линейная зависимость между модулем Юнга и изменением мощности Бриллюэна и изменением частоты бриллюэновского сдвига оптического сигнала обратного рассеяния, направленного по чувствительному волокну.

4. Заключение

Поскольку модуль Юнга сердцевины волокна изменяется в зависимости от температуры окружающей среды и деформационных образований, влияние изменений модуля Юнга на параметры Бриллюэна очень важно с точки зрения производительности сенсорной системы. Следовательно, для различных значений модуля Юнга сердцевины волокна на выходе чувствительной системы могут быть получены различные данные об изменении мощности по Бриллюэну и сдвиге частоты по Бриллюэну. Используя (21) и (22), отношение чувствительности модуля Юнга к изменению частоты Бриллюэна к изменению мощности Бриллюэна для нулевой деформации и температуры 293 ° K может быть вычислено как ~ 2,30. Следовательно, можно сделать вывод, что модуль Юнга оказывает более доминирующее влияние на изменение частоты Бриллюэна по отношению к изменению мощности Бриллюэна

СПИСОК ЛИТЕРАТУРЫ:

1. K. R. C. P. De Souza, Fiber optic distributed sensing based on spontaneous Brillouin scattering, PhD Dissertation, University of Southampton (1999).
2. M. Alahbabi, Distributed optical fiber sensors based on the coherent detection of spontaneous Brillouin scattering, PhD Dissertation, University of Southampton (2005).
3. A. Gunday, S. E. Karlik, G. Yilmaz, International Review of Electrical Engineering (IREE), 8(2), 920 (2013).
4. A. Minardo, R. Bernini, L. Amato, L. Zeni, IEEE Sensors J. 12(1), 145 (2012).
5. S. M. Maughan, H. H. Kee, T. P. Newson, Meas. Sci. Technol. 12(7), 834 (2001)

Д.Д. Ганченко, Е.Е. Ганченко, Н.М. Сеначин

ИМПОРТОЗАМЕЩЕНИЕ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ НА ПРИМЕРЕ КОМПАНИИ ОАО «РЖД»

Научный руководитель: Ю. В. Могильников

Уральский государственный университет путей сообщения в г. Екатеринбурге (УрГУПС), Россия

Ключевые слова: Видеоконференцсвязь, связь совещаний, платформа для общения, импортозамещение, Cisco Jabber, IVA UC.

На сегодняшний день компания ОАО «РЖД» использует программную платформу Cisco Jabber. Данная платформа используется уже долгое время и морально и функционально устаревает, а также является разработкой зарубежной компании. Для решения данной проблемы было принято решение разработать отечественную программную платформу, которая является более современным и функциональным аналогом.

D.D. Ganchenko, E.E. Ganchenko, N.M. Senachin

IMPORT SUBSTITUTION OF VIDEOCONFERENCING SYSTEMS ON THE EXAMPLE OF RUSSIAN RAILWAYS

Scientific supervisor - Y.V. Mogilnikov

Ural State University of Railway Transport in Yekaterinburg (UrGUPS), Russia

Keywords: Video conferencing, meeting link, communication platform, import substitution, Cisco Jabber, IVA UC.

Today, Russian Railways uses the Cisco Jabber software platform. This platform has been used for a long time and is morally and functionally obsolete, and is also a development of a foreign company. To solve this problem, it was decided to develop a domestic software platform, which is a more modern and functional analogue.

Cisco Jabber - это программное обеспечение для мгновенного обмена сообщениями, голосовой и видеосвязи, а также совместной работы внутри организации. Оно разработано компанией Cisco Systems и может быть использовано на различных устройствах, включая персональные компьютеры, ноутбуки, смартфоны и планшеты.

Вот несколько ключевых фактов о Cisco Jabber:

1. Основные функции. Cisco Jabber предоставляет пользователю возможность обмениваться мгновенными сообщениями, делать голосовые и видеозвонки, проводить видеоконференции, делиться рабочими файлами и документами, управлять календарем и контактами.
2. Интеграция с другими продуктами Cisco. Cisco Jabber интегрируется с другими продуктами Cisco, включая Cisco Webex, Cisco TelePresence, Cisco Unified Communications Manager и Cisco Meeting Server.
3. Безопасность. Cisco Jabber обеспечивает высокий уровень безопасности, включая шифрование данных, аутентификацию и авторизацию пользователей, защиту от атак на сеть и системы.
4. Гибкость и мобильность. Cisco Jabber поддерживает работу на различных устройствах и операционных системах, включая Windows, Mac, iOS и Android. Это позволяет пользователям оставаться на связи в любое время и в любом месте.

5. Возможности совместной работы. Cisco Jabber предоставляет пользователю возможность работать с коллегами в режиме реального времени, совместно редактировать документы, проводить веб-конференции и управлять задачами.

6. Администрирование и управление. Cisco Jabber может быть установлен и настроен администраторами с помощью инструментов управления и мониторинга, предоставляемых Cisco.

7. Интеграция с сторонними приложениями. Cisco Jabber поддерживает интеграцию с сторонними приложениями, такими как Salesforce, Microsoft Office и Google Drive.

В целом, Cisco Jabber предоставляет широкий спектр возможностей для совместной работы и обмена информацией внутри организации, что делает его полезным инструментом для бизнеса.

Cisco Jabber имеет ряд преимуществ и недостатков, которые могут влиять на его использование в конкретных ситуациях.

Плюсы:

1. Интеграция с другими продуктами Cisco. Cisco Jabber интегрируется с другими продуктами Cisco, что позволяет пользователям использовать единый интерфейс для управления коммуникациями и совместной работы.

2. Гибкость и мобильность. Cisco Jabber поддерживает работу на различных устройствах и операционных системах, что позволяет пользователям оставаться на связи в любое время и в любом месте.

3. Безопасность. Cisco Jabber обеспечивает высокий уровень безопасности, включая шифрование данных, аутентификацию и авторизацию пользователей, защиту от атак на сеть и системы.

4. Возможности совместной работы. Cisco Jabber предоставляет пользователям возможность обмениваться сообщениями, делать голосовые и видеозвонки, проводить видеоконференции, делиться файлами и документами, управлять календарем и контактами.

5. Интеграция с сторонними приложениями. Cisco Jabber поддерживает интеграцию со многими сторонними приложениями, такими как Salesforce, Microsoft Office и Google Drive, что позволяет пользователям управлять своими задачами и проектами.

Минусы:

1. Сложность использования. Cisco Jabber имеет богатый набор функций, что может сделать его сложным для использования для новых пользователей.

2. Ограниченная поддержка сторонних устройств. Cisco Jabber поддерживает только определенные модели устройств, что может ограничить его использование для пользователей, использующих не поддерживаемые устройства.

3. Высокая стоимость. Использование Cisco Jabber может быть дороже, чем использование более простых мгновенных сообщений или голосовой связи.

4. Необходимость интеграции с другими продуктами Cisco. Чтобы получить максимальную выгоду от Cisco Jabber, может потребоваться интеграция с другими продуктами Cisco, что может быть сложным и затратным.

5. Зависимость от сети. Cisco Jabber требует доступа к сети, чтобы работать, что может создавать проблемы, если сеть недоступна или нестабильна [1].

В целом, Cisco Jabber предоставляет широкий спектр возможностей для совместной работы и коммуникаций, которые могут быть полезны в различных ситуациях, особенно для компаний, использующих другие продукты Cisco. Однако, перед использованием Cisco Jabber необходимо учитывать его сложность, высокую стоимость и зависимость от сети, а также возможные ограничения для сторонних устройств.

Кроме того, для эффективного использования Cisco Jabber, может потребоваться интеграция с другими продуктами Cisco, такими как Cisco Webex или Cisco Unified Communications Manager, что может увеличить затраты на внедрение и поддержку.

В целом, Cisco Jabber может быть полезным инструментом для организации коммуникаций и совместной работы, но его использование должно быть осознанным и приниматься с учетом конкретных потребностей и возможностей организации.

IVA UC - это решение для управления коммуникациями, которое предоставляется компанией Interactive Intelligence. Оно включает в себя широкий набор инструментов для совместной работы и общения внутри компании и за ее пределами.

Некоторые из основных функций IVA UC включают в себя:

1. Голосовую связь. IVA UC позволяет пользователям совершать голосовые звонки внутри и за пределами компании, а также использовать функции конференц-связи и автоответчика.
2. Видеосвязь. IVA UC позволяет пользователям использовать видеоконференции для совместной работы и общения с коллегами и клиентами.
3. Мгновенные сообщения. IVA UC включает в себя функции мгновенного обмена сообщениями, которые позволяют пользователям быстро и удобно общаться внутри компании.
4. Электронную почту и календарь. IVA UC интегрируется с электронной почтой и календарем, что позволяет пользователям легко управлять своими задачами и проектами.
5. Мобильную связь. IVA UC поддерживает работу на различных устройствах, включая мобильные устройства, что позволяет пользователям оставаться на связи в любое время и в любом месте.
6. Аналитику и отчетность. IVA UC предоставляет инструменты для анализа данных и создания отчетов о коммуникациях, что позволяет оценивать эффективность работы и принимать решения на основе данных.

Некоторые из преимуществ IVA UC включают в себя:

1. Гибкость. IVA UC поддерживает работу на различных устройствах и операционных системах, что позволяет пользователям использовать его в любом месте и на любом устройстве.
2. Безопасность. IVA UC обеспечивает высокий уровень безопасности, включая шифрование данных и защиту от атак на сеть и системы.
3. Интеграция с другими продуктами. IVA UC интегрируется с другими продуктами Interactive Intelligence, что позволяет пользователям использовать единый интерфейс для управления коммуникациями и совместной работы.
4. Голосовое и видео качество. IVA UC обеспечивает высокое качество голосовой и видеосвязи благодаря использованию современных технологий.
5. Автоматизация. IVA UC позволяет автоматизировать некоторые процессы, такие как обработка звонков и маршрутизация сообщений, что повышает эффективность работы.
6. Управление. IVA UC предоставляет инструменты для управления коммуникациями и администрирования системы, что позволяет быстро и легко настраивать и управлять настройками.

Однако, некоторые из возможных недостатков IVA UC включают в себя:

1. Сложность. IVA UC может быть сложным в использовании и настройке, особенно для непрофессионалов.
2. Высокая стоимость. IVA UC может быть дорогим решением, особенно для малых и средних компаний.
3. Зависимость от сети. IVA UC требует стабильной и быстрой сети для обеспечения высокого качества коммуникаций.
4. Интеграция с другими системами. IVA UC может требовать интеграции с другими системами и продуктами, что может повысить сложность и затраты на внедрение и поддержку [2].

IVA UC и Cisco Jabber - это два разных продукта, которые предназначены для управления коммуникациями внутри компании и за ее пределами.

Основное сравнение между IVA UC и Cisco Jabber может быть сделано на основе следующих параметров:

1. Функциональность: IVA UC предоставляет более широкий спектр функций, чем Cisco Jabber. IVA UC включает функции, такие как виртуальная АТС, видеоконференции, мультимедийные сообщения и колл-центр. Cisco Jabber, в свою очередь, предоставляет возможность общения по телефону, обмена сообщениями, видеоконференций и общения через социальные сети.

2. Интеграция: IVA UC имеет большую гибкость и возможности для интеграции с другими системами, в то время как Cisco Jabber имеет предустановленные интеграции с другими продуктами Cisco, такими как Cisco WebEx и Cisco TelePresence.

3. Сложность использования: Cisco Jabber является более простым в использовании и понимании, чем IVA UC. Cisco Jabber имеет более простой пользовательский интерфейс и легче настраивается.

4. Стоимость: Оба продукта могут быть дорогими для небольших и средних компаний, но Cisco Jabber является более доступным решением, чем IVA UC [3].

В целом, IVA UC и Cisco Jabber имеют свои преимущества и недостатки, и выбор между ними должен быть сделан на основе конкретных потребностей и возможностей организации. Если вам нужна более широкая функциональность и возможности интеграции, то IVA UC может быть лучшим решением. Если же вы ищете простое и доступное решение для обмена сообщениями и проведения видеоконференций, то Cisco Jabber может быть лучшим выбором.

Более подробное сравнение между IVA UC и Cisco Jabber может быть сделано на основе различных критериев, таких как функциональность, интеграция, сложность использования и стоимость.

Функциональность:

IVA UC предоставляет более широкий спектр функций, чем Cisco Jabber. Он включает в себя функции виртуальной АТС, видеоконференции, мультимедийных сообщений и колл-центра. Эти функции могут быть полезны для больших компаний, которые требуют более расширенных возможностей коммуникаций.

Cisco Jabber, в свою очередь, предоставляет возможность общения по телефону, обмена сообщениями, видеоконференций и общения через социальные сети. Эти функции обеспечивают простоту использования для пользователей, которые ищут только базовые возможности коммуникаций.

Интеграция:

IVA UC имеет большую гибкость и возможности для интеграции с другими системами, в то время как Cisco Jabber имеет предустановленные интеграции с другими продуктами Cisco, такими как Cisco WebEx и Cisco TelePresence.

IVA UC может быть лучшим выбором для компаний, которые хотят интегрировать свои системы коммуникаций с другими системами, такими как CRM, ERP или другими бизнес-приложениями. Он может обеспечить большую гибкость для различных типов систем и интеграций.

С другой стороны, Cisco Jabber может быть более удобным для компаний, которые используют другие продукты Cisco, такие как Cisco WebEx и Cisco TelePresence, поскольку у них уже есть интеграция с этими продуктами.

Сложность использования:

Cisco Jabber является более простым в использовании и понимании, чем IVA UC. Cisco Jabber имеет более простой пользовательский интерфейс и легче настраивается.

IVA UC имеет более сложную структуру, которая может быть сложна для понимания для некоторых пользователей. Он может требовать больше времени на настройку и обучение, что может быть проблемой для некоторых компаний.

Стоимость:

Оба продукта могут быть дорогими для небольших и средних компаний, но Cisco Jabber является более доступным решением, чем IVA UC.

IVA UC может быть более дорогим решением, чем Cisco Jabber, особенно если учитывать расходы на настройку и обучение персонала. IVA UC также может требовать дополнительных инвестиций в оборудование, так как он может работать только на высокоскоростных сетях.

Cisco Jabber, с другой стороны, может быть более доступным и более простым в использовании для небольших и средних компаний. Он может быть использован с существующим оборудованием и требует меньше времени на настройку и обучение персонала [4].

В целом, выбор между IVA UC и Cisco Jabber будет зависеть от потребностей и бюджета компании. IVA UC может быть более подходящим для крупных компаний с более сложными

потребностями коммуникаций, в то время как Cisco Jabber может быть лучшим выбором для небольших и средних компаний, которые ищут простое и доступное решение для своих коммуникационных потребностей.

Список литературы:

1. "Cisco Jabber vs. Skype for Business: Which is the Better Collaboration Tool?", на сайте Business News Daily, [электронный ресурс] URL: https://www.businessnewsdaily.com/8717-cisco-jabber-vs-skype-for-business.html (дата обращения: 09.04.2023);
2. "IVA UC: The Ideal UC&C Solution for Large Enterprises", на сайте Star2Star Communications, [электронный ресурс] URL: https://www.star2star.com/insights/blog/iva-uc-the-ideal-ucc-solution-for-large-enterprises (дата обращения: 09.04.2023);
3. "Cisco Jabber", на сайте Cisco , [электронный ресурс] URL: https://www.cisco.com/c/en/us/products/unified-communications/jabber/index.html (дата обращения: 09.04.2023);
4. "IVA UC: What Is Intelligent Visual Assistance, and How Does It Work?", на сайте Star2Star Communications , [электронный ресурс] URL: https://www.star2star.com/insights/blog/what-is-iva-uc-and-how-does-it-work (дата обращения: 09.04.2023).

А.В. Земсков, И.А. Малкова

3D-ТРЕНАЖЁР ДЛЯ ОБУЧЕНИЯ ПЕРСОНАЛА СЛУЖБЫ СВЯЗИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО
«Сибирский государственный университет телекоммуникаций и информатики»
в г. Екатеринбурге, Россия

Ключевые слова: 3d-моделирование, 3d-тренажер, 3ds Max, Unity3D, информационная система, программные скрипты, Quadralink, Muldex, служба связи.

В настоящей работе описан инструментарий и разработка компьютерного 3d-тренажера для обучения персонала службы связи без отрыва от производства, который предназначен для отработки профессиональных знаний, умений и навыков в процессе работы с реальным оборудованием.

Показано, что по итогам тестирования разработанный тренажер выполняет поставленные задачи.

A.V. Zemskov, I.A. Malkova

3D TRAINING SIMULATOR FOR COMMUNICATIONS STAFF

Federal State Budget Institution of Higher Professional Education «Siberian State University of Telecommunications and Informatics» Ural Technical Institute of Communications and Informatics (Branch), Yekaterinburg, Russia

Keywords: 3d modeling, 3d simulator, 3ds Max, Unity3D, information system, software scripts, Quadralink, Muldex, communication service.

At the presented paper describes the tools and development of a computer 3d simulator for on-the-job training of communications staff, that is intended to training professional knowledge, skills and abilities in the process of working with real equipment.

It was shown that the 3D simulator performs the assigned tasks based on the results of testing.

Дополненная и виртуальная реальность в настоящее время представляет собой наибольший научный и практический интерес. В первом случае AR-технология подразумевает восприятие с помощью специальных устройств, отдельных искусственных элементов виртуальной информации как неотъемлемой части окружающего мира. VR создает новую реалистичную виртуальную среду, с которой пользователь может взаимодействовать с помощью органов чувств. Человек полностью погружается в искусственный мир и ощущает реальность происходящего. Для того чтобы в полной мере имитировать взаимодействие с виртуальной средой используются различные устройства: от смартфонов со специальным функционалом, очков и шлемов до виртуальных ретинальных мониторов, формирующих изображение на сетчатке глаза, и комнат виртуальной реальности, в которых достигается максимальный эффект погружения. Реалистичность усиливается многоканальной акустической системой с локацией источника звука и имитацией тактильных ощущений с помощью датчиков движения и манипуляторов [1, 2].

В настоящий момент уровень подготовки рабочего персонала играет большую роль в деятельности любой компании. Поэтому разрабатываются и внедряются различные технологии и системы обучения персонала как для оценки текущего уровня подготовки сотрудников, так и для его повышения. Во-первых, ощущается потребность качественного улучшения подготовки персонала, которая вызвана постоянным усложнением технологических процессов и появлением новых информационных систем управления. Во-вторых, постоянно движущиеся вперед информационные технологии создают отличную возможность для создания новых систем для

тренировки на компьютерном тренажере, превосходящих по эффективности все известные формы обучения, включая не всегда доступные и потенциально опасные тренировки на реальных объектах [3, 4].

На практике применяются различные виды обучения: инструктажи, мастер-классы, тренинги, обучение с применением компьютерных тренажеров и стендов.

3Д-технологии сегодня – это различные по сложности системы моделирования, симуляции и визуализации, использующие специальные методики для подготовки человека к принятию качественных и быстрых решений [4]. Компьютерные тренажеры и симуляторы представляют собой компьютерные программы в виде виртуальной компьютерной игры или физические модели, которые управляют каким-либо процессом, аппаратом или транспортным средством. Другими словами, компьютерный тренажер - это средство эффективного обучения, с помощью которого можно повысить его качество.

Основными преимуществами 3D-тренажёра являются: наглядность, повышение качества и эффективности обучения, возможность многократной отработки обучаемым различных сценариев и действий, которые необходимы в профессиональной деятельности, а также возможность дистанционного обучения. Обучающиеся применяют знания на практике без использования дорогостоящего оборудования [4, 5].

Области применения тренажеров разнообразны. Данные системы обучения могут использоваться для образовательных учреждений, учебных центров на предприятиях или в качестве визуализации архитектурных сооружений на нулевой стадии строительства. Эффективность усвоения информации в виртуальной реальности значительно выше в сравнении с классическими методами обучения. Компьютерные тренажеры позволяют создать модель реальной обстановки с оборудованием, звуком, производственными задачами [4].

Раньше сотрудники внимательно изучали планы эвакуации, инструкции по технике безопасности и по работе с определёнными приборами, агрегатами и пультами, чтобы, находясь на производстве, не допустить погрешностей, приводящих не только к плохим, но и к необратимым последствиям. Использование 3d-тренажеров позволяет обучать сотрудников с предупреждением дорогостоящих ошибок в реальном процессе и без отрыва от основной работы. Симуляторы также могут использоваться для изучения производственного процесса и итоговой аттестации сотрудников, проведения презентации закрытых или потенциально опасных объектов.

Таким образом, разработка компьютерных тренажеров является *актуальной* задачей.

Целью настоящей работы является создание 3D-тренажера для обучения персонала службы связи. Тренажер представляет собой программное решение, позволяющее выполнять производственные процессы на компьютере без непосредственного контакта с реальными объектами [3]. Поэтому *основными задачами* проектирования 3d-симулятора являются разработка логики и алгоритма программы, логических схем и диаграмм управления программой, моделирование трехмерных моделей реальных объектов, создание текстур для 3d-моделей, написание программных скриптов, а также проведение тестирования симулятора на наличие ошибок.

Аппаратная составляющая тренажера представляет собой персональный компьютер, обладающий достаточной вычислительной мощностью для воспроизведения 3D-графики. Программная составляющая – это математически обоснованная виртуальная модель, которая включает в себя систему графической визуализации, звуковое сопровождение и текстовую информацию. Ввод и вывод информации осуществляется согласно программному коду виртуальной модели [3].

Разработка 3d-тренажера включает в себя несколько этапов.

Проектирование. На данном этапе разработана диаграмма вариантов использования, определяющая границы и контекст моделируемой предметной области. Данная диаграмма отображает общие требования к функциональному поведению программного продукта. На структурной схеме (рис. 1) представлены компоненты программы и их взаимодействия.

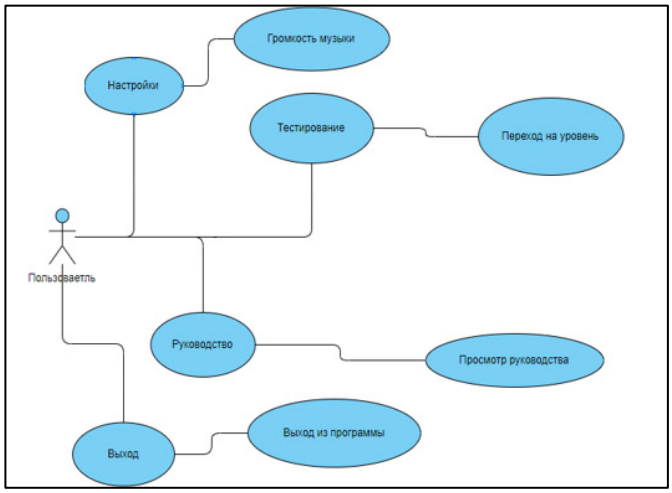


Рис. 1. Диаграмма вариантов использования для пользователя

Второй этап – разработка информационной системы. Интерфейс пользователя состоит из нескольких страниц и функционала для пользователя. На рис.2 показан внешний вид главного меню, где отображены кнопки перехода на другие уровни и модули.

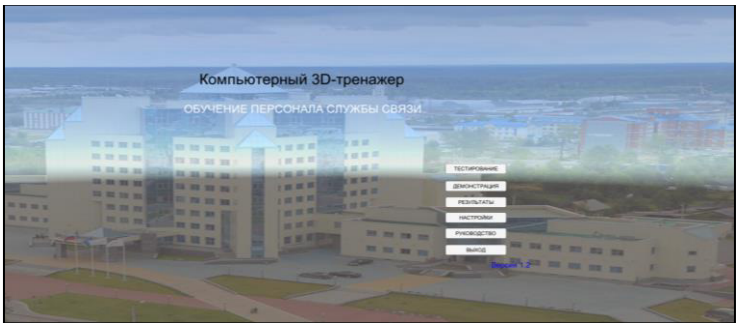


Рис.2. Главное меню

Следующий этап включает в себя разработку программных модулей. Для полноценной работы 3d-тренажера созданы такие программные модули, как уровень тестирования, модуль настроек и руководство пользователя. На рисунке 3 показан внешний вид данных модулей. Для создания программных модулей используются программные скрипты.

Рис. 3. Модуль настроек и руководство пользователя

Визуальное представление. Данный этап предусматривает создание 3d моделей реальных объектов. В таблице 1 приведены сравнительные характеристики рассматриваемого программного обеспечения для трехмерного моделирования. Для трехмерного моделирования объектов выбран Autodesk 3sd Max.

Программа 3ds Max используется во множестве отраслей. Одно из основных достоинств - гибкость программы, позволяющая применять её для моделирования двигателей, сложных схем, спецэффектов для фильмов, мультфильмов и визуализации физических процессов. К недостаткам программы можно отнести требовательность к ресурсам персональных

компьютеров, потребляя огромное количество оперативной памяти при моделировании сложных объектов и сцен. Blender 3D также пользуется большой популярностью среди пользователей. Он отлично подходит для создания качественных моделей и сцен, однако не так хорошо подходит для точных схем и чертежей [2, 6].

Таблица 1. Сравнительные характеристики рассматриваемых программ

Критерий	Blender	Autodesk 3ds MAX
Характеристики	Производственный путь Tracer; Графический процессор; Набор анимационных инструментов; Создание игры; Маскировка; Отслеживание движения камеры; Отслеживание движения объекта; Compositing; Редактирование видео; Моделирование; Может быть интегрирован с конвейерными инструментами; Настраиваемый пользовательский интерфейс	3D анимация и динамика; 3ds Max жидкости; Имитация импорта данных; Контроллеры создания графиков; Voxel и Heatmap скиннинг; Активный рендеринг оттенков; 3D рендеринг; Raytracer Renderer; Настраиваемые рабочие пространства; Сплайн рабочие процессы Сетка и моделирование поверхности; Hair-мех и модификатор канала данных; Назначение текстуры
Поддерживаемые языки	Английский	Английский; Немецкий; Китайский; Индийский; японский; Испанский французский; Русский

Отсюда следует, что инструментарий каждой из описанных программ обширен, однако каждая из них предназначена под определённые задачи. Для разработки 3d-тренажера требуется создание трехмерной модели со сложными математическими данными и физической моделью, поэтому для создания 3d-объектов выбран 3ds Max. На рисунке 4 представлен пример создания трехмерной модели.

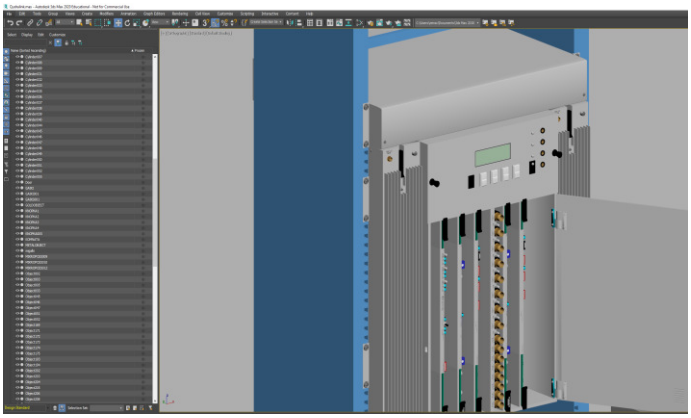


Рис. 4. Создание 3d-модели

Разработка интерактивного модуля. Написание программного кода виртуальной модели является наиболее трудоемкой частью работы. Основными задачами данного этапа являются разработка алгоритма, корректно описывающего физику реального процесса. Программа (программный код) связывает между собой графические элементы, текстовое и звуковое сопровождение, интерактивную составляющую и имитирует динамику протекания процесса [7].

Выбор ядра. Для разработки 3D-тренажёра рассмотрены движки Unity, Unreal Engine и Cry Engine. В таблице 2 представлены основные характеристики данных движков. Для создания тренажера на данном этапе выбрано программное обеспечение Unity.

Unity - это кроссплатформенный игровой движок, позволяющий создавать двухмерные и трехмерные игры и приложения. К основным достоинствам Unity можно отнести простой и понятный интерфейс, а также объекты «GameObject» и компоненты «MonoBehaviour». Редактор можно расширять собственными сценариями. В Unity также оптимизирован рендеринг для множества однотипных объектов. Кроме того, длительность итерации в Unity гораздо меньше (развертывание и компиляция исходного кода происходит быстрее, шейдеры компилируются почти мгновенно) [7].

Таблица 2- Сравнительные характеристики программного обеспечения

Критерии	Unity	Unreal Engine	Cry Engine
Магазина ассетов	+	-	-
Отладка в редакторе	+	-	-
Руководство пользователя	+	-	+
Система Blueprints	+	+	-
Два и более языка программирования	+	-	-
Консоль	+	+	+
Редактирование анимации	+	+	-

Для написания программных скриптов используется язык программирования C#, что позволит достичь поставленных целей. C# простой, современный объектно-ориентированный язык программирования, одним из основных достоинств которого является практичность. Так же C# отлично подходит для создания и применения программных компонентов.

Тестирование – заключительный этап разработки. Данный этап необходим для выявления всех возможных уязвимостей и ошибок работы алгоритма.

Создание специализированных 3d-тренажеров на базе технологий виртуальной реальности позволяет приблизить использующего их человека к реальной действительности. Следовательно, можно сделать следующие выводы по результатам работы. Разработан алгоритм работы 3d-тренажера для обучения персонала службы связи, составлены логические схемы и диаграммы управления программой. Созданы 3d-модели и текстуры плат и оборудования. Написаны необходимые программные скрипты для реализации работы симулятора.

Установлено, что в ходе проведения тестирования работоспособности программы 3d-симулятор выполняет поставленные задачи.

СПИСОК ЛИТЕРАТУРЫ:

1. Новые изобретения и технологии 21 века [Электронный ресурс]. -Режим доступа:https://qwizz.ru/новейшие-технологии-21-века
2. Обзор 3ds max: коротко о главном [Электронный ресурс]. -Режим доступа: https://3ddevice.com.ua/blog/3d-printer-obzory/obzor-3ds-max/
3. Ершов Е. В., Виноградова Л. Н., Челнокова С. В., Мартюгов А. С. Компьютерный тренажер для установки и снятия детали со станка ДИП-400 // Вестник Череповецкого государственного университета. 2019. № 1 (88). с. 20-26
4. Андреев А. А., Солдаткин В. И. Дистанционное обучение: сущность, технология, организация. М.: Московский государственный университет экономики, статистики и информатики, 1999. 196 с.
5. Грибова В.В., Петряева М.В., Федорищев Л.А. Компьютерный обучающий тренажер с виртуальной реальностью для офтальмологии. Открытое образование. 2013, №6(101). с. 45-51.
6. Использование программ 3dsmax, blender в образовательной деятельности [Электронный ресурс]. -Режим доступа:https://cyberleninka.ru/article/n/ispolzovanie-programm-3dsmax-blender-v-obrazovatelnoy-deyatelnosti
7. Unity [Электронный ресурс]. -Режим доступа: https://blog.skillfactory.ru/glossary/unity/

Д. В. Зыскина, И.И. Шестаков, Е.И. Гниломёдов

РАЗРАБОТКА ОСНОВНЫХ РЕШЕНИЙ ПО РАСШИРЕНИЮ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ В УЧЕБНОЙ ЛАБОРАТОРИИ УРТИСИ СИБГУТИ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: транспортная сеть связи, компетентностный подход, практико-ориентированное обучение, учебная лаборатория, технология DWDM.

В работе рассмотрены вопросы организации сегмента транспортной сети связи в учебной лаборатории УрТИСИ СибГУТИ с включением проектируемого сегмента в существующую транспортную сеть. Рассматриваются вопросы разработки схемы организации связи, конфигурации оборудования DWDM, организации подключения к модели линейного тракта ВОЛС.

D.V. Zyskina, I.I. Shestakov, E.I. Gnilomedov

DEVELOPMENT OF MAIN SOLUTIONS TO EXPAND THE TRANSPORT COMMUNICATION NETWORK IN THE TRAINING LABORATORY OF URTISI SIBGUTI

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: transport communication network, competence-based approach, practice-oriented learning, educational laboratory, DWDM technology.

The paper considers the issues of organizing a segment of the transport communication network in the educational laboratory of the UrTISI SibGUTI with the inclusion of the projected segment in the existing transport network. The issues of developing a communication organization scheme, DWDM equipment configuration, organization of connection to the FOCL linear path model are considered.

Согласно действующей в настоящее время национальной программы «Цифровая экономика», основой современного развития цифровой экономики выступает сектор информационно коммуникационных технологий, состоящий из ИТ-отрасли и отрасли связи и телекоммуникаций [1]. Применение практикоориентированного обучения при подготовке специалистов для отраслей экономики и, в частности, для отрасли инфокоммуникаций является приоритетной технологией в сфере образования как на ступени подготовки специалистов среднего звена, так и на ступени подготовки инженерных кадров уровня бакалавриата и магистратуры. Реализация подхода практикоориентированного обучения позволяет уже в учебном заведении сформировать у студентов компетенции, соответствующие требованиям профессиональных стандартов, что отражается в федеральных образовательных стандартах [2,3].

С целью формирования профессиональных компетенций у выпускников направления подготовки бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи, закрепления теоретических знаний у студентов, применение ситуативного подхода на занятиях с моделированием рабочих ситуаций, возникающих в реальных условиях эксплуатации оборудования на сетях связи, в Уральском техническом институте связи и информатики на кафедре многоканальной электрической связи создана учебная лаборатория «Транспортных сетей и систем связи» [4].

Лаборатория включает в себя натурные модели элементов, сегментов и участков сетей связи, связанных между собой в соответствии с принципами, реализуемыми в сетях связи. В частности, сегменты местных сетей связи, внутризоновых сетей и магистральной первичной сети

связи. Участок магистральной сети реализован на основе транспортной технологии DWDM. В качестве оборудования на данном участке применены мультиплексоры компании Huawei Optix BWS 320G. Однако на реальной сети связи часто возникает ситуация, когда отдельные сегменты транспортных сетей используют оборудования различных производителей, реализующих технологию DWDM. Для моделирования данной ситуации было принято решение расширить транспортную сеть в учебной лаборатории, путем создания дополнительного сегмента. В качестве оборудования волнового мультиплексирования на нем будет применено оборудование компании NEC. В частности, несколько мультиплексоров NEC DW4200, смонтированных в четырех шкафах. Каждый коммуникационный шкаф в высоту составляет 2.2 м. Само оборудование размещается в стандартных каркасах, в каждом каркасе по три корзины. Корзины укомплектована платами расширения, определяющими конфигурацию мультиплексного оборудования. Пример конфигурации проектируемых мультиплексоров показана на рис. 1.

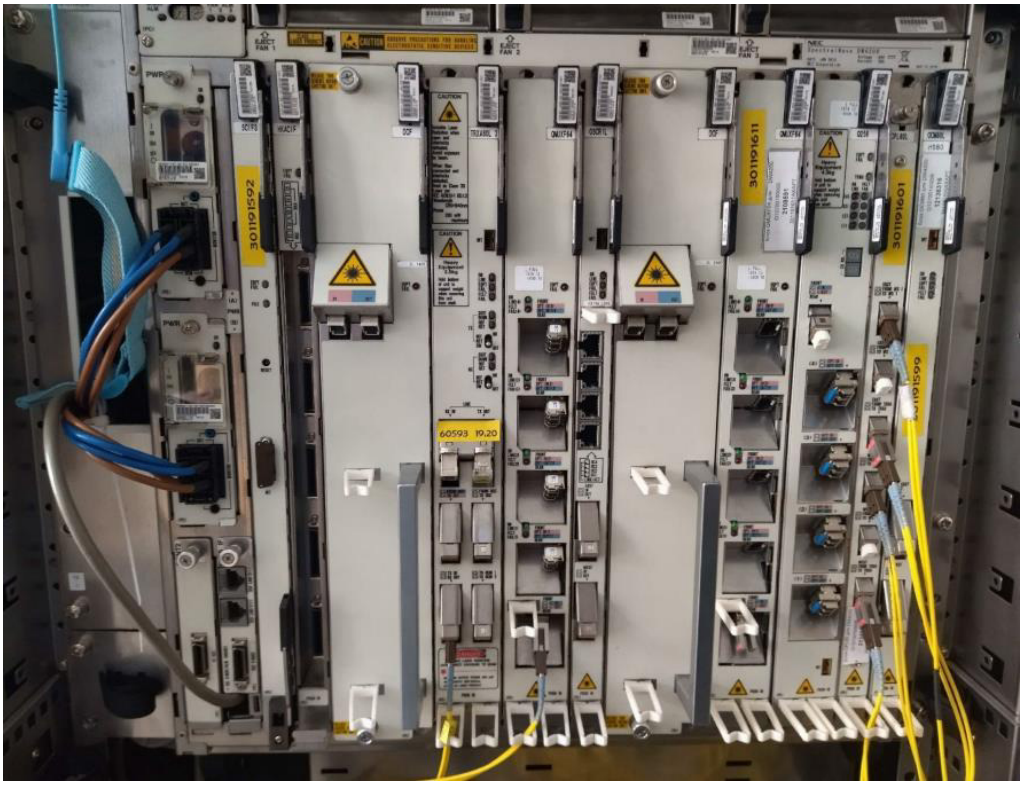


Рисунок 1 – Пример конфигурации мультиплексного оборудования

В состав проектируемого оборудования входят четыре мультиплексора. Два мультиплексора сконфигурированы в качестве мультиплексоров ввода вывода, а два в качестве терминальных мультиплексоров. Загрузку мультиплексоров трафиком предполагается организовать от существующей сети, через организуемый участок волоконно-оптической линии связи, получая нагрузку от гигабитных коммутаторов. Включение нового сегмента в существующую сеть будет осуществляться через оптические кроссы, посредством оптического кабеля, проложенного в кабель-каналах до существующей натурной модели оптического линейного тракта длиной 112 километров с возможностью переключения на отдельные участки длиной от 12 до 40 километров [4]. Такое решение позволяет смоделировать различные производственные ситуации, возникающие н реальных сетях, процессе их эксплуатации. Схема организации связи в лаборатории представлена на рис. 2.

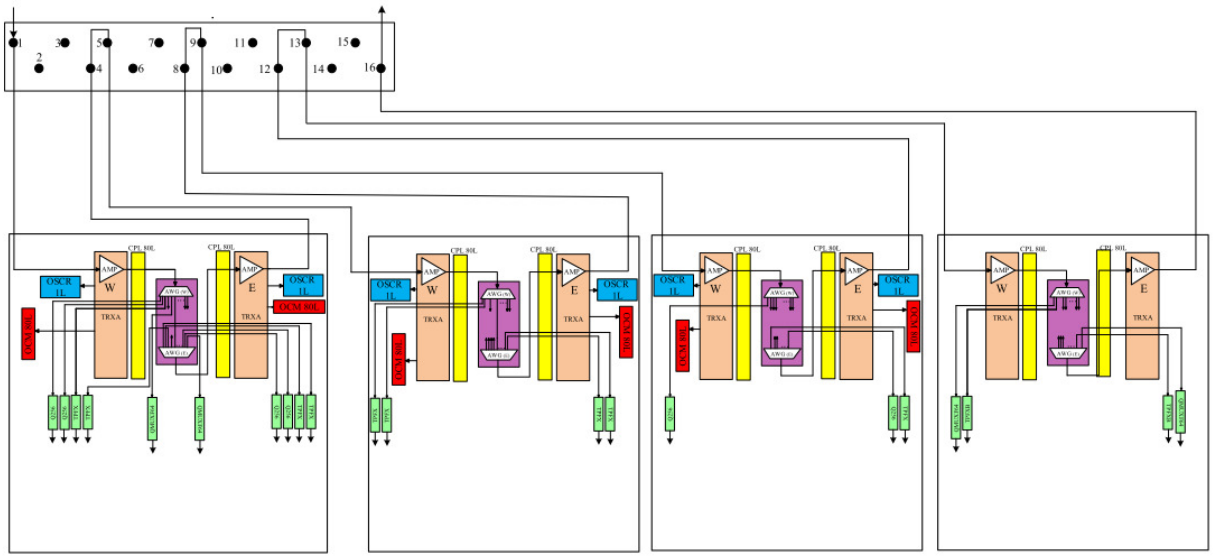


Рисунок 2 – Схема организации связи

В процессе организации лаборатории был произведен монтаж межблочных соединительных шнуров, обеспечивающих оптимальную конфигурацию оборудования, разработаны схемы соединения мультиплексоров. Пример схемы соединения представлен на рис. 3.

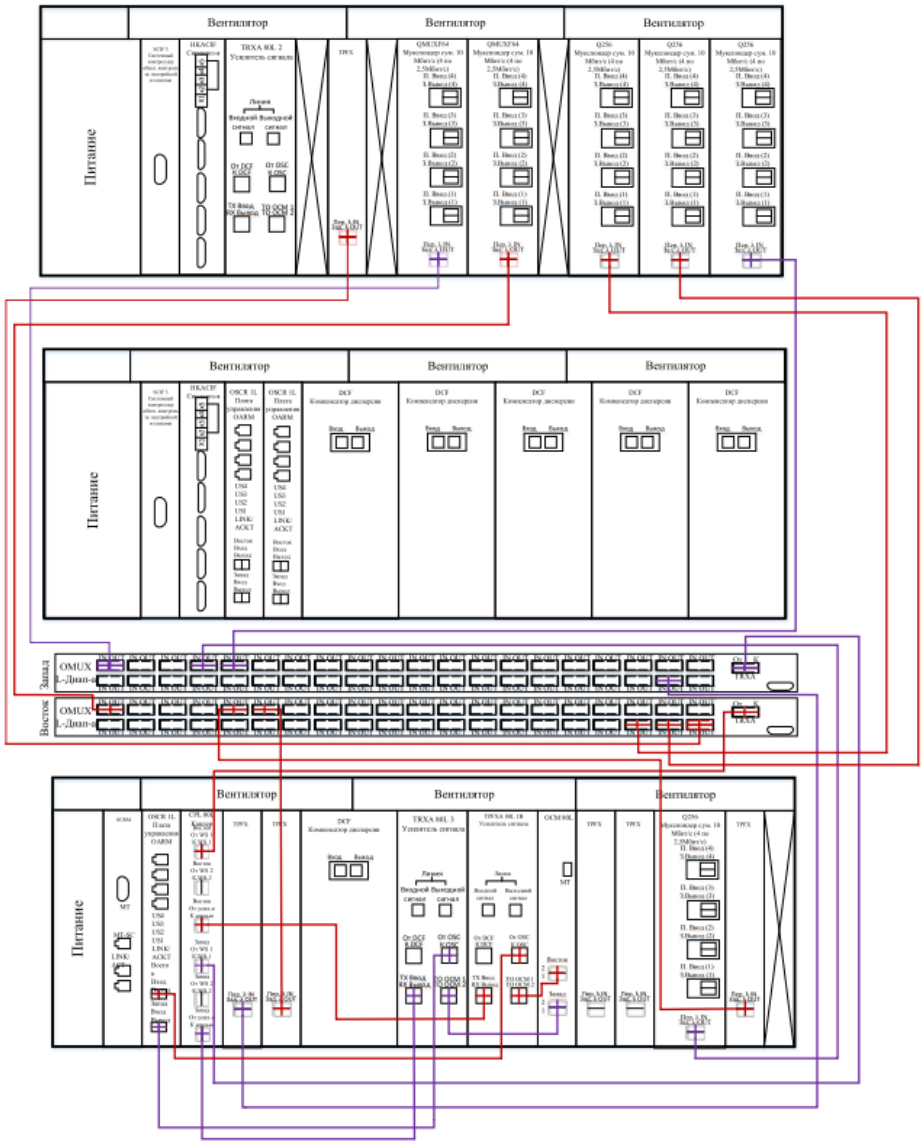


Рисунок 3 – Схема соединения блоков мультиплексора

Особое внимание в лаборатории уделено организации электропитанию, так как проектируемое оборудование имеет большую потребляемую мощность, более 10 ампер на шкаф, в качестве электропитающей установки в лаборатории используется устройство электропитания оборудования связи УЭПС-2 48/120, оснащенный четырьмя блоками выпрямителей ВББВ с выходной мощностью до 1200 ватт каждый [5]. Подключение установки произведено к трехфазной силовой электросети организации, что обеспечивает наиболее эффективную работу выпрямителей.

Таким образом, разрабатываемая в учебной лаборатории модель сети DWDM, будет имитировать основные производственные ситуации, возникающие при эксплуатации и техническом обслуживании элементов сети в реальных условиях. Применение действующего на сетях связи оборудования, позволит сформировать у студентов профессиональные компетенции, отвечающие требованиям профессиональных стандартов отрасли связи. Выполняя лабораторные работы на данном оборудовании, учащиеся получают возможность освоить необходимые методы работы и технологии, используемые в данной профессии, а также приобрести понимание ее структуры и особенностей функционирования.

СПИСОК ЛИТЕРАТУРЫ:

1. Дефицит ИТ-кадров: глобальные тренды, международный опыт развития кадрового потенциала [Электронный ресурс]. – URL: https://files.data-economy.ru/Docs/Deficit_IT_kadrov_globalnye_trendy.pdf (дата обращения 22.03.2023).
2. Приказ Минобрнауки России от 19.09.2017. г. N 930 «Об утверждении федерального государственного образовательного стандарта высшего образования — бакалавриата по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи [Электронный ресурс]. – URL: https://base.garant.ru/71787568 (дата обращения 12.03.2023)
3. Профстандарт: 06.018. Инженер по технической эксплуатации линий связи. [Электронный ресурс]. – URL: https://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/reestr-professionalnykh-standartov/index.php?ELEMENT_ID=110369 (дата обращения 22.03.2023)
4. Применение натурной модели транспортной сети связи в процессе практико-ориентированного обучения студентов инфокоммуникационного вуза/ Гниломёдов Е.И., Бурумбаев Д.И. В сборнике: Проблемы управления качеством образования. сборник избранных статей Международной научно-методической конференции. Санкт-Петербург, 2021. С. 87-90.
5. Официальный сайт ООО «Промсвязьдизайн». [Электронный ресурс]. – https://www.promsd.ru/market/ustrojstva-i-sistemy-elektropitaniya/ueps-9 (дата обращения 25.03.2023)

С.С. Казанцев, И.И. Шестаков

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛГИИ WDM В СЕТИ FSO

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: компьютерное моделирование, пропускная способность, оптика свободного пространства.

В статье сделан обзор на технологии FSO и WDM. Была исследована возможность увеличения пропускной способности FSO с применением технологии WDM. Путем компьютерного моделирования в программе OptiSystem была получена схема внедрения технологии WDM в сети FSO. Был построен график зависимости расстояния между трансиверами FSO и Q-фактором.

S.S. Kazancev, I.I. Shestakov

INVESTIGATION OF THE POSSIBILITY OF USING WDM TECHNOLOGY IN THE FSO NETWORK

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: computer modeling, bandwidth, free-space optics.

The article provides an overview of the FSO and WDM technologies. The possibility of increasing the bandwidth of the FSO with the use of WDM technology was investigated. By computer modeling in the OptiSystem program, a scheme for implementing WDM technology in the FSO network was obtained. A graph of the dependence of the distance between the FSO transceivers and the Q factor was constructed.

Оптическая связь в свободном пространстве (FSO) становится многообещающим решением для передачи данных в сетях доступа. Однако сети FSO ограничены их узкой пропускной способностью и дальностью связи. [1]

Оптика свободного пространства FSO — это технология беспроводной связи, которая использует модулированные лучи света для передачи данных по воздуху. Системы FSO состоят из передатчика, который использует лазер для передачи оптического сигнала, и приемника, который принимает оптический сигнал с помощью фотодиода.

Сеть FSO работает в инфракрасном спектре света и использует узкий луч света для передачи данных. Луч обычно направляется на приемник по воздуху на расстоянии от нескольких сотен метров до нескольких километров, в зависимости от мощности лазера, чувствительности приемника, и состояния атмосферы.

Технология FSO используется в различных сферах связи, таких как телекоммуникационная транспортная сеть, подключение к корпоративным сетям и военная связь. Она также используется в городских условиях, где традиционные проводные или беспроводные технологии связи нецелесообразны или экономически неэффективны. На рисунке 1 изображена схема работы технологии FSO.

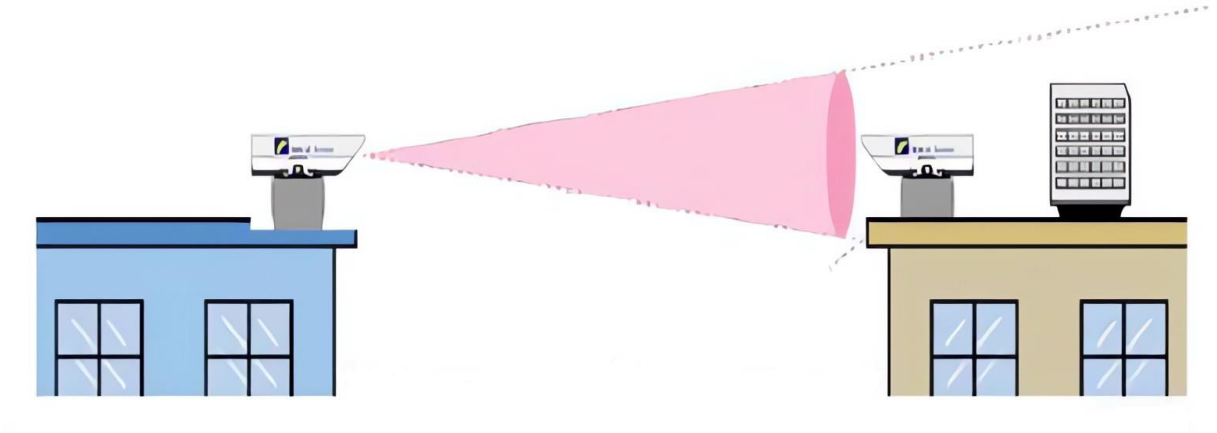


Рис. 1. Схема работы технологии FSO

FSO обладает высокой степенью защиты и невосприимчив к электромагнитным помехам, поскольку работает в оптическом спектре. Скорость передачи данных в технологии FSO, которая может достигать 1 Гбит/с, ограничивается прямой видимостью между передатчиком и приемником, и погодными условиями, такими как дождь, туман и снег. Для увеличения пропускной способности можно интегрировать технологию DWDM в атмосферные оптические линии связи.

DWDM (плотное мультиплексирование с разделением по длине волны) применяется в сетях оптической связи и позволяет одновременно передавать несколько оптических сигналов на разных длинах волн в оптоволокне с шагом 0,4/0,8 нм.[2]

В системах DWDM обычно используются лазеры для генерации оптических сигналов и оптические усилители для повышения мощности сигнала при его передаче на большие расстояния. Затем сигналы разделяются на принимающей стороне с помощью демультиплексора, который разделяет разные длины волн на отдельные каналы.

Одним из ключевых преимуществ технологии DWDM является скорость передачи данных до 400 Гбит/с на канал. Количество каналов в системе DWDM может достигать 46. [4]

Исследование возможности увеличения пропускной способности сети FSO посредством интеграции технологии DWDM было проведено в программе OptiSystem. Назработана схема сети DWDM, в которой вместо оптоволоконного кабеля применена атмосферная оптическая линия связи, схема изображена на рисунке 2.

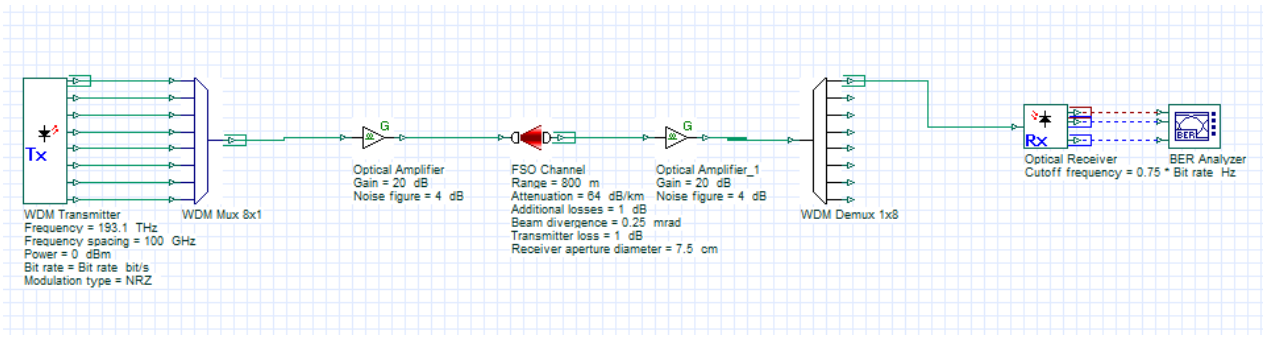


Рис. 2. Схема интеграции DWDM системы в FSO

Схема включает в себя следующие компоненты: WDM источник на восемь длин волн, идеальный WDM мультиплексор, атмосферно-оптический канал связи, идеальный WDM демультиплексор, приемник с анализатором ошибок и оптические усилители. Данная схема позволяет оценить возможности применения DWDM технологии с шагом мультиплексирования 100 ГГц в сети FSO в окне прозрачности атмосферы 1550 нм. Километрическое затухание в атмосферной оптической линии связи задано 60 дБ/км, мощность передатчика 0 дБ, затухание в

мультиплексоре 0 дБ, коэффициент усиления CDFA усилителей 20 дБ.

Возможность применения технологии DWDM в сети FSO оценивалась зависимостью величины Q-фактора от длины атмосферной оптической линии связи. Результаты графиков зависимости представлены на рисунке 3.

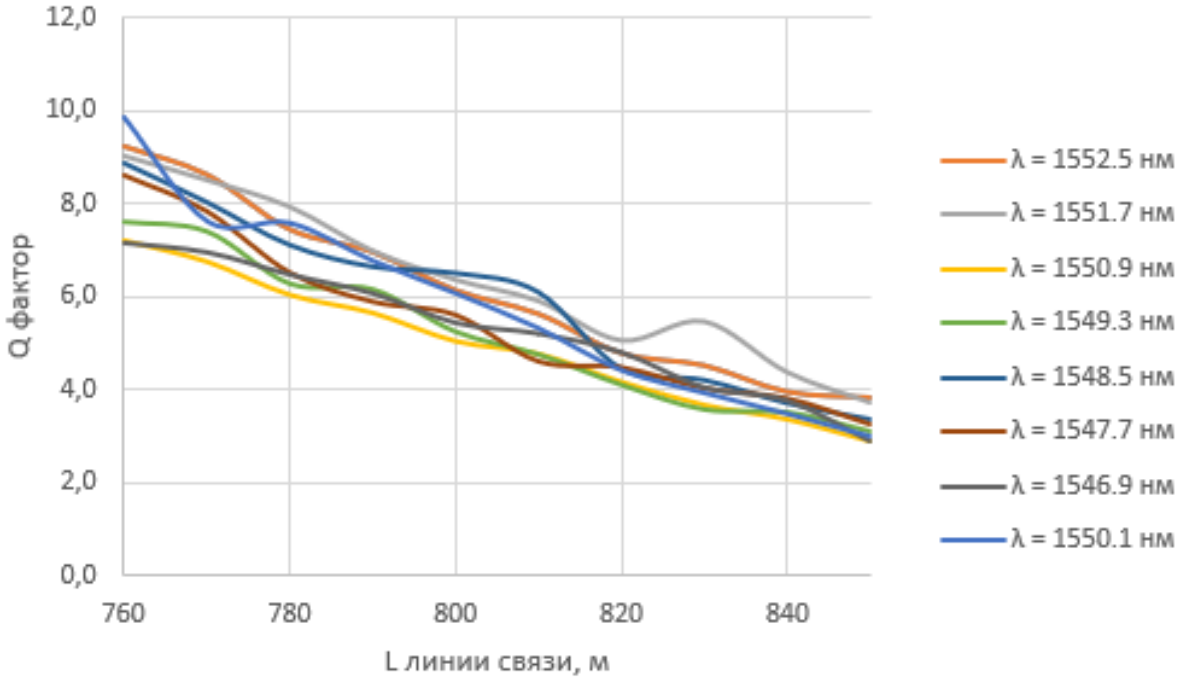


Рис. 3. График зависимости Q-фактора от длины линии

Из анализа графика зависимости видно, что дальность связи в сети WDM-FSO составляет 840 м, при которой значение Q-фактора равно 4 (BER ≈ 10^{-6}). Такая дальность связи характерна для традиционных атмосферных оптических линий связи, что говорит о реальных возможностях интегрирования DWDM технологии в существующие FSO сети.

СПИСОК ЛИТЕРАТУРЫ:

1. Вишневский В.М. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. 592 с.
2. Павлов Н.М. Аппаратура атмосферных оптических линий передачи и методы ее классификации. Фотон – экспресс, № 4, 2006, с. 91 - 105. Режим доступа: http://www.fotonexpress.ru/pdf/PE_6%2854%29.pdf.
3. Воронов В. И., Филиппов В. Л. Атмосферные оптические линии связи: расчет и моделирование устройств, систем и процессов: учебное пособие. - Казань: Новое знание, 2015. 187 с.
4. Листвин В.Н., Трещиков В.Н. DWDM системы: научное издание. – М.: Издательский Дом «Наука», 2013. – 300 с.

А.Е. Кайгородов, И.А. Осипова

ПРИМЕНЕНИЕ БАЙЕСОВСКИХ СЕТЕЙ В МЕДИЦИНЕ: ОБЗОР ЛИТЕРАТУРЫ И ПЕРСПЕКТИВЫ ИХ ИСПОЛЬЗОВАНИЯ

Уральский технический институт связи и информатики (филиал) (УрТИСИ СибГУТИ), Россия

Ключевые слова: Байесовская сеть, данные с неопределённостью, принятие решений.

В данной статье проводится обзор применения Байесовских сетей в медицинской диагностике. Байесовские сети - это статистические модели, которые могут использоваться для моделирования и анализа различных медицинских данных, таких как результаты обследований пациентов, лабораторные показатели, истории болезней и другие. В статье рассматривается применение Байесовских сетей для диагностики различных заболеваний. Преимущества использования Байесовских сетей в медицинской диагностике заключаются в возможности учитывать неопределенность и неполноту информации, а также в автоматизации процесса принятия решений. В статье также производится анализ существующих исследований по данной теме, с целью выявления перспектив использования Байесовских сетей в будущих медицинских исследованиях и практике. В результате обзора и анализа литературы, делается вывод о том, что Байесовские сети могут быть эффективным инструментом для повышения точности и эффективности медицинской диагностики. В целом, данная статья представляет интерес для медицинских специалистов, исследователей и разработчиков медицинского программного обеспечения, которые заинтересованы в использовании новых методов и технологий для улучшения качества медицинской диагностики и лечения.

A.E. Kaigorodov, I.A. Osipova

APPLICATION OF BAYESIAN NETWORKS IN MEDICAL DIAGNOSTICS: A LITERATURE REVIEW AND PROSPECTS FOR THEIR USE

Ural Technical Institute of Communications and Informatics (branch) (UrTISI SibGUTI), Russia

Keywords: Bayesian network, data with uncertainty, decision making.

This article reviews the application of Bayesian networks in medical diagnostics. Bayesian networks are statistical models that can be used to model and analyze a variety of medical data, such as patient examinations, laboratory values, case histories, and others. This article discusses the use of Bayesian networks for diagnosing various diseases. The advantages of using Bayesian networks in medical diagnostics lie in the ability to take into account uncertainty and incompleteness of information, as well as in the automation of the decision-making process. The article also analyzes existing research on this topic in order to identify prospects for the use of Bayesian networks in future medical research and practice. As a result of the literature review and analysis, it is concluded that Bayesian networks can be an effective tool for improving the accuracy and efficiency of medical diagnostics. Overall, this article is of interest to medical professionals, researchers, and medical software developers who are interested in using new methods and technologies to improve the quality of medical diagnosis and treatment.

Современная медицина сталкивается с растущей необходимостью использовать новые технологии и методы для более точной диагностики и лечения различных заболеваний. В последние годы Байесовские сети привлекли внимание медицинской общественности в качестве перспективного инструмента для анализа и моделирования медицинских данных. Байесовские сети являются статистическими моделями, которые могут использоваться для решения различных задач, связанных с медицинской диагностикой, таких как прогнозирование рисков

заболеваний, выявление факторов риска, постановка диагнозов и определение оптимального лечения.

Цель данной статьи - обзор применения Байесовских сетей в медицинской диагностике и анализ существующих исследований в этой области. В статье будет рассмотрено применение Байесовских сетей для диагностики различных заболеваний, а также выявлены преимущества и недостатки использования этих сетей в медицинской практике. Будут проанализированы результаты исследований, проведенных в этой области, с целью выявления перспектив использования Байесовских сетей для более эффективной медицинской диагностики.

Данная научная статья может представлять интерес для медицинских специалистов, исследователей и разработчиков медицинского программного обеспечения, которые заинтересованы в использовании новых методов и технологий для улучшения качества медицинской диагностики и лечения.

Байесовские сети (БС) — это графические структуры для представления вероятностных отношений между большим количеством переменных и для осуществления вероятностного вывода на основе этих переменных» [1].

БС обычно используются в случае, когда имеется ряд связанных друг с другом событий (пропозиций), вероятности истинности которых могут быть получены от специалистов предметной области. БС должна сопоставить информацию (знания) от экспертов так, чтобы отдельные факты не противоречили друг другу. Затем принимаются во внимание фактические данные (свидетельства) о произошедших событиях или возможные вариации априорных вероятностей.

Байесовские сети доверия. Байесовские сети доверия (БСД, причинно следственные сети) предназначены для создания вероятностных экспертных систем с использованием байесовского вывода и применяются при решении задач с неопределённостью, связанной с [2, 3]:

а) многообразием причинно-следственных связей в исследуемой предметной области;

б) наличием неполных знаний о параметрах;

в) случайными факторами, влияющими на осуществление событий.

БСД применяются в задачах описания взаимосвязей — различных переменных и могут быть изображены, как направленный граф причинноследственных связей, являющийся ациклическим (направленные циклы недопустимы). События являются вершинами графа, а причинноследственные связи между ними обозначены ребрами. Такой подход позволяет производить оценку вероятностей событий, зависящих от других событий [2].

БСД может быть использована для вычисления вероятности того, в чем причина не исправности устройства, основываясь на данных, полученных из датчиков и поведением устройства в целом. Таким образом, строятся зависимости между сигналами и неисправности устройства. Графическое представление примера БСД представлен на изображении 1. На изображение 1 показано, что B и C зависит от A.

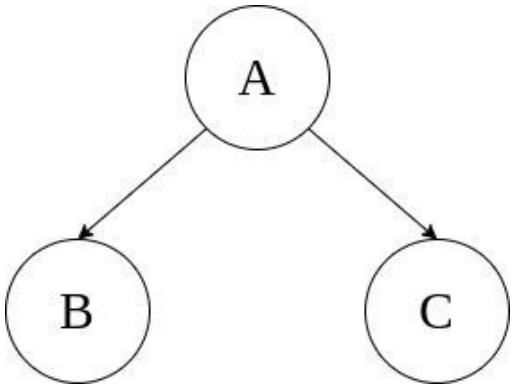


Рисунок 1 – Пример байесовской сети доверия

В основе модели лежит формула, представлена Байесом (1):

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)} \quad (1)$$

где, $P(A|B)$ – вероятность наступления события A при условии, что событие B уже случилось,

$P(B|A)$ – вероятность наступления события B, при условии, что событие A уже случилось,

$P(A)$ – полная (априорная) вероятность исследуемого события A,
$P(B)$ – полная (априорная) вероятность исследуемого события B.

Пусть $A_1, A_2, A_3 \dots A_n$ полная группа несовместных взаимоисключающих событий. Тогда апостериорная вероятность $P(A_i \vee B)$ каждого из событий $A_i, i = 1..n$ при условии, что произошло события B выражается априорной вероятностью A_i (2):

$$P(A_i \vee B) = \frac{P(B \vee A_i) * P(A_i)}{P(B)} = \frac{P(B \vee A_i) * P(A_i)}{\sum_{i=1}^{n} P(B \vee A_i) * P(A_i)} \quad (2)$$

Преимущества использования Байесовских сетей в диагностике различных заболеваний заключаются в их способности учитывать неопределенность и неполноту информации. В случаях, когда информация о заболевании неполная или неоднозначная, Байесовские сети могут помочь определить вероятность наличия заболевания на основе имеющихся данных. Это может ускорить процесс постановки диагноза и предотвратить возможные ошибки.

Кроме того, использование Байесовских сетей в медицинской диагностике может привести к автоматизации процесса принятия решений, что может улучшить точность и эффективность диагностики. Байесовские сети также могут быть использованы для прогнозирования прогрессирования заболевания, определения прогноза и выбора оптимальной стратегии лечения.

Существуют множество исследований, демонстрирующих применение Байесовских сетей в диагностике различных заболеваний, включая онкологические, инфекционные и неврологические заболевания. Например, Байесовские сети могут быть использованы для диагностики рака молочной железы на основе результатов маммографии и других лабораторных показателей. В случаях инфекционных заболеваний, Байесовские сети могут использоваться для определения вероятности наличия инфекции на основе симптомов и результатов лабораторных исследований. В неврологической диагностике, Байесовские сети могут помочь в дифференциальной диагностике между различными видами неврологических заболеваний.

Несмотря на множество преимуществ использования Байесовских сетей в диагностике различных заболеваний, существуют и некоторые недостатки, которые нужно учитывать при их применении.

Один из недостатков заключается в том, что Байесовские сети могут оказаться сложными для построения и обучения. Необходимость обработки большого количества информации, а также учет различных факторов, может требовать высокой вычислительной мощности и специализированных знаний в области статистики и машинного обучения.

Также существуют ограничения в использовании Байесовских сетей для диагностики некоторых заболеваний, например, если важными факторами являются временные зависимости или динамические процессы, такие как прогрессирование заболевания.

Кроме того, Байесовские сети могут быть неприменимы для диагностики редких или малоизученных заболеваний, когда данных недостаточно для обучения модели.

Несмотря на эти ограничения, преимущества использования Байесовских сетей в диагностике различных заболеваний все же значительны, и правильное применение этих моделей может помочь улучшить точность и эффективность диагностики, что в конечном итоге может привести к лучшему лечению и результатам для пациентов.

В целом, использование Байесовских сетей в медицинской диагностике представляет значительный потенциал для улучшения точности, эффективности и автоматизации процесса диагностики различных заболеваний.

В работе "Bayesian Networks in Healthcare: Distribution by Medical Condition" [4] авторы Scott McLachlan, Kudakwashe Dube, Graham A Hitman, Norman Fenton и Evangelia Kyrimi исследуют типы медицинских состояний, которые моделируются с помощью БС, и различия в том, как и почему они применяются к разным состояниям. Авторы обнаружили, что почти две трети всех БС в области здравоохранения сосредоточены на четырех состояниях: сердечно-сосудистых, онкологических, психологических и легочных заболеваниях. Авторы считают, что существует недостаток понимания того, как работают BNs и что они способны делать, и что только при большем понимании и продвижении мы можем реализовать полный потенциал БС для достижения положительных изменений в повседневной практике здравоохранения.

В статье "From heterogeneous healthcare data to disease-specific biomarker networks: A hierarchical Bayesian network approach" [5] авторы Ann-Kristin Becker, Marcus Dörr, Stephan B. Felix, Fabian Frost, Hans J. Grabe, Markus M. Lerch, Matthias Nauck, Uwe Völker, Henry Völzke и Lars Kaderali представляют полностью автоматизированный подход к выявлению биомаркеров, связанных с заболеваниями и факторов риска из гетерогенных и высокоразмерных данных о здравоохранении. Их рабочий процесс основан на БС, которые являются популярным инструментом для анализа взаимодействия биомаркеров. Обычно данные требуют обширной ручной предварительной обработки и сокращения размерности, чтобы обеспечить эффективное обучение БС. Для гетерогенных данных такая предварительная обработка трудно автоматизировать и обычно требует специфических знаний в области. Авторы здесь объединяют обучение БС с иерархической кластеризацией переменных, чтобы обнаруживать группы похожих признаков и изучать взаимодействия между ними полностью автоматически. Они представляют алгоритм оптимизации для адаптивного уточнения таких групп БС для учета конкретной целевой переменной, такой как заболевание. Комбинация БС, кластеризации и уточнения дает низкоразмерные, но специфичные для заболевания сети взаимодействий. Эти сети предоставляют легко интерпретируемые, но точные модели взаимосвязей между биомаркерами.

Вывод. В данной статье было рассмотрено применении Байесовских сетей в медицинской диагностике. В частности, были рассмотрены преимущества использования Байесовских сетей в диагностике. В статье проанализировали некоторые исследования в этой области и вывод таков, что Байесовские сети могут быть эффективным инструментом для повышения точности и эффективности медицинской диагностики. Байесовские сети позволяют учитывать неопределенность и неполноту информации, что является важным преимуществом в медицинской диагностике, где часто бывает необходимо принимать решения на основе ограниченной информации. Таким образом, данная статья может быть полезна для медицинских специалистов и исследователей, которые заинтересованы в использовании новых методов и технологий для улучшения качества медицинской диагностики и лечения.

Список литературы:

1. Управление знаниями. Технологии управления знаниями. Data Mining – Режим доступа: https://www.sites.google.com/site/upravlenieznaniami/tehnologii-upravlenia-znaniami/data-mining (Дата обращения: 19.11.2022).
2. Jensen, F. V. Bayesian Networks and Decision Graphs / F. V. Jensen //NY: Springer Verlag, 2001. - 268p.
3. Probabilistic Networks and Expert Systems: tutorial / R. G. Cowell, P. Dawid, S. L. Lauritzen, D. J. Spiegelhalter.//New York: Springer-Verlag, 1999. - 205p.
4. Scott McLachlan, Kudakwashe Dube, Graham A Hitman, Norman E Fenton, Evangelia Kyrimi. Bayesian networks in healthcare: Distribution by medical condition / Scott McLachlan, Kudakwashe Dube, Graham A Hitman, Norman E Fenton, Evangelia Kyrimi // Artificial Intelligence in Medicine – 2020, January
5. Becker, A. K. "Dö rr M, Felix SB, Frost F, Grabe HJ, Lerch MM. From heterogeneous healthcare data to disease-specific biomarker networks: A hierarchical Bayesian network approach." / Becker, A. K. "Dö rr M, Felix SB, Frost F, Grabe HJ, Lerch MM // PLoS Comput Biol — 2021, February

А.Е. Каменсков, Д.В. Кусайкин, Д.В. Денисов

ПРОГНОЗИРОВАНИЕ ХАРАКТЕРИСТИК МНОГОЛУЧЕВОЙ ЛИНЗОВОЙ АНТЕННЫ С ПОМОЩЬЮ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: нейронная сеть, линзовая антенна, диаграмма направленности.

Сегодня нейронные сети являются очень популярной концепцией и множество исследователей изучают их возможности в различных задачах, в том числе в качестве инструмента для проектирования антенн, прогнозирования их электродинамических и конструктивных параметров. В работе приведены результаты исследования эффективности прогнозирования значений диаграммы направленности линзовой антенны Люнеберга, работающей в многолучевом режиме, с помощью метода нейронных сетей.

A.E. Kamenskov, D.V. Kusaykin, D.V. Denisov

PREDICTION OF THE CHARACTERISTICS OF A MULTIBEAM LENS ANTENNA USING ARTIFICIAL NEURAL NETWORKS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: neural network, lens antenna, radiation pattern.

Today neural networks are a very popular concept and many researchers are studying their capabilities in various tasks, including as a tool for designing antennas, predicting their electrodynamic and design parameters. The paper presents the results of a study of the effectiveness of predicting the values of the radiation pattern of a Luneberg lens antenna operating in multipath mode using the neural network method.

Сегодня НС являются очень популярной концепцией и множество исследователей изучают их возможности в различных задачах и в самых разных областях. Одной из сфер применения НС является их использование в качестве инструмента для проектирования антенн и прогнозирования их электродинамических и конструктивных параметров. Основная роль применения НС в данной области заключается в сокращении трудоемких и затратных по времени стадий анализа и проектирования антенн. При рассмотрении процессов и задач нетривиальных антенн можно заметить весьма сложные нелинейные зависимости между входными и выходными параметрами. Например, синтез сферической линзовой антенны Люнеберга является довольно непростой задачей, долгое время широкое распространение этой антенны сдерживал фактор сложности ее изготовления и соответственно стоимости. Сегодня же для определения оптимальных параметров линзы можно воспользоваться вычислительными ресурсами искусственных НС. За счет своей структуры с множеством слоев НС хорошо справляются с аппроксимацией разного рода многопараметрических нелинейных зависимостей. В связи с этим можно отметить целесообразность применения такого инструментария как НС для решения задач прогнозирования характеристик линзовых антенн.

Обзор научных публикаций показал, что на сегодняшний день проведен ряд исследований в области оптимизации [1] и синтеза с помощью НС таких видов антенн, как патч-антенна [2], антенна Вивальди [3], метаповерхностная антенна [4]. Однако в литературе не встречаются подобные исследования касательно линзовых антенн Люнеберга [5].

В данной работе приведены результаты прогнозирования значений диаграммы направленности линзовой антенны, работающей в многолучевом режиме, с использованием НС вида многослойного персептрона.

Приведем сначала описание модели нейронной сети. Входными параметрами НС являлись мощности облучателей многолучевой сферической линзовой антенны, размещенных на ее теле. Выходными параметрами НС являются значения диаграммы направленности антенны. При обучении НС было сгенерирован набор данных, содержащий 6560 реализаций диаграмм направленностей линзовой антенны, сформированных при разных комбинациях значений мощности (0 Вт, 0.5 Вт; 1 Вт) восьми облучателей многолучевой линзовой антенны. Входной слой НС содержал 8 нормализованных искусственных нейронов, определяющих значения мощности восьми облучателей. Первый скрытый слой состоял из 512 искусственных нейронов, второй и третий слои из 1024 нейронов каждый. Выходной слой содержал 721 нейрон, которые формировали значения графика диаграммы направленности антенны (рисунок 1). В качестве функции потерь НС использовалась среднеквадратичная ошибка:

$$MSE = \frac{1}{N} * \sum_{j=1}^{N} (y_j - \tilde{y}_j)^2 , \tag{1}$$

где N – количество реализаций, y_j – ожидаемые значения, $\tilde{y}_j$ – прогнозированные значение.

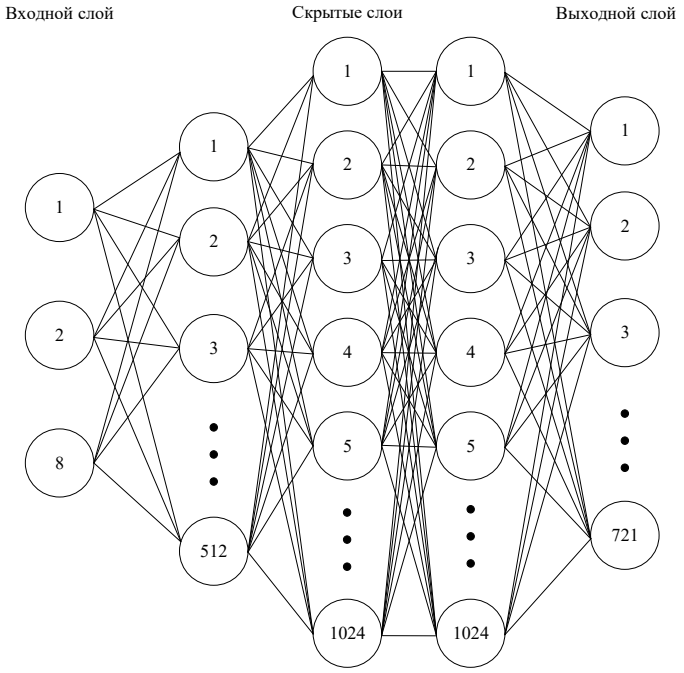


Рисунок 1 – Многослойный персептрон

В качестве функции активации нейронов использовалась нелинейная функция ReLU (Rectified Linear Unit), которая по сравнению со сигмоидной функцией активации более простая в вычислительном плане и не вызывает затухания градиента при обратном распространении ошибки

$$\mathrm{ReLU}(x) = \begin{cases} x, & x > 0 \\ 0, & x \le 0 \end{cases} \tag{2}$$

Функция ReLU представляет собой линейную функцию, выходящую из центра соей координат и принимающую нулевые значения на всей отрицательной области оси абсцисс. График функции показан на рисунке 2.

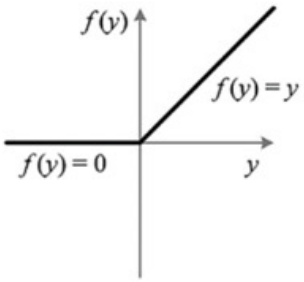


Рисунок 2 – Функция активации ReLU

Преимущество ReLU – это разреженность активации, что позволяет активировать только часть нейронов (разреженная активация). Сама сеть становится легче и меньше нагружается.

На рисунке 3б показано, что в случае сигмоидной функции активации первые 25 эпох нейронная сеть не могла обучаться корректно, выдавая низкие показатели точности. Под конец обучения происходит затухание градиента, что приводит к тому, что НС перестает обучаться или делает это крайне медленно. В случае функции активации ReLU (рисунок 3а) данный недостаток не наблюдается, и точность повышается с первой эпохи. На конечном этапе обучения затухание градиента происходит меньше, поэтому нейронная сеть способна обучаться дальше.

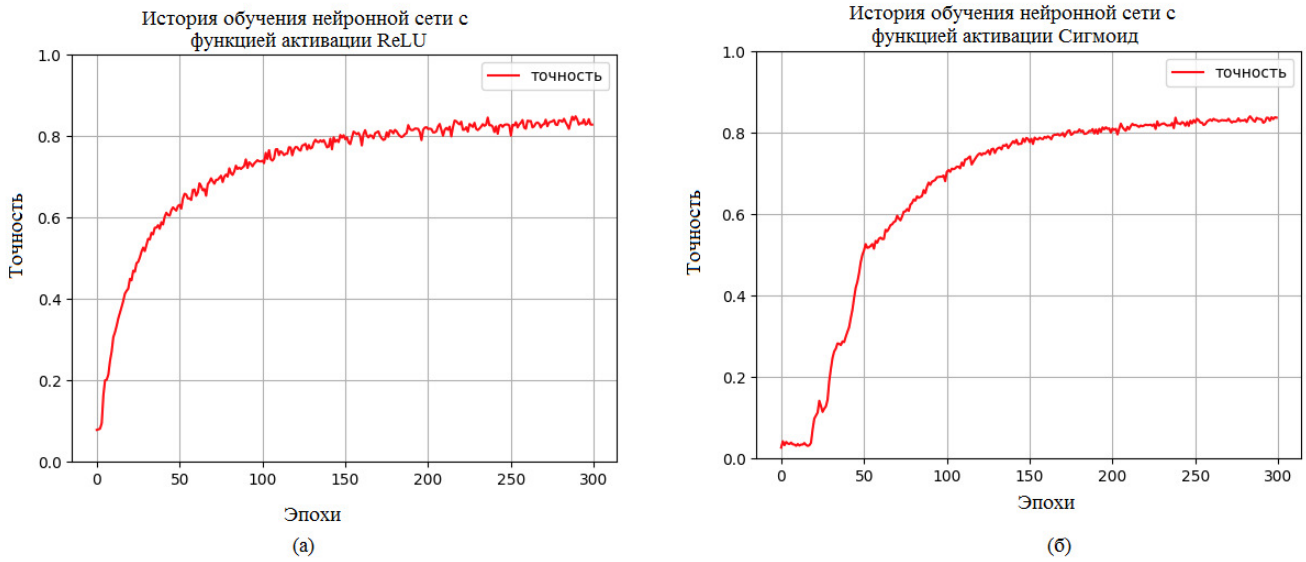


Рисунок 3 – История обучения нейронной сети: (а) с функцией активации ReLU, (б) с функцией активации сигмоид

Набор данных для обучения НС был сгенерирован на основе модели шестислойной сферической линзы Люнеберга радиусом три длины волны с восемью облучателями в программном пакете Ansys Electronics Desktop (HFSS Design).

В результате обучения НС средняя квадратичная ошибка после 300 эпох равнялась 0.208, финальная точность НС составила 88.1%. На рисунке 4 приведен график исходной и спрогнозированной нейросетью функции диаграммы направленности линзовой антенны при входных значениях [1, 1, 0.5, 0.5, 0.5, 0.5, 1, 1].

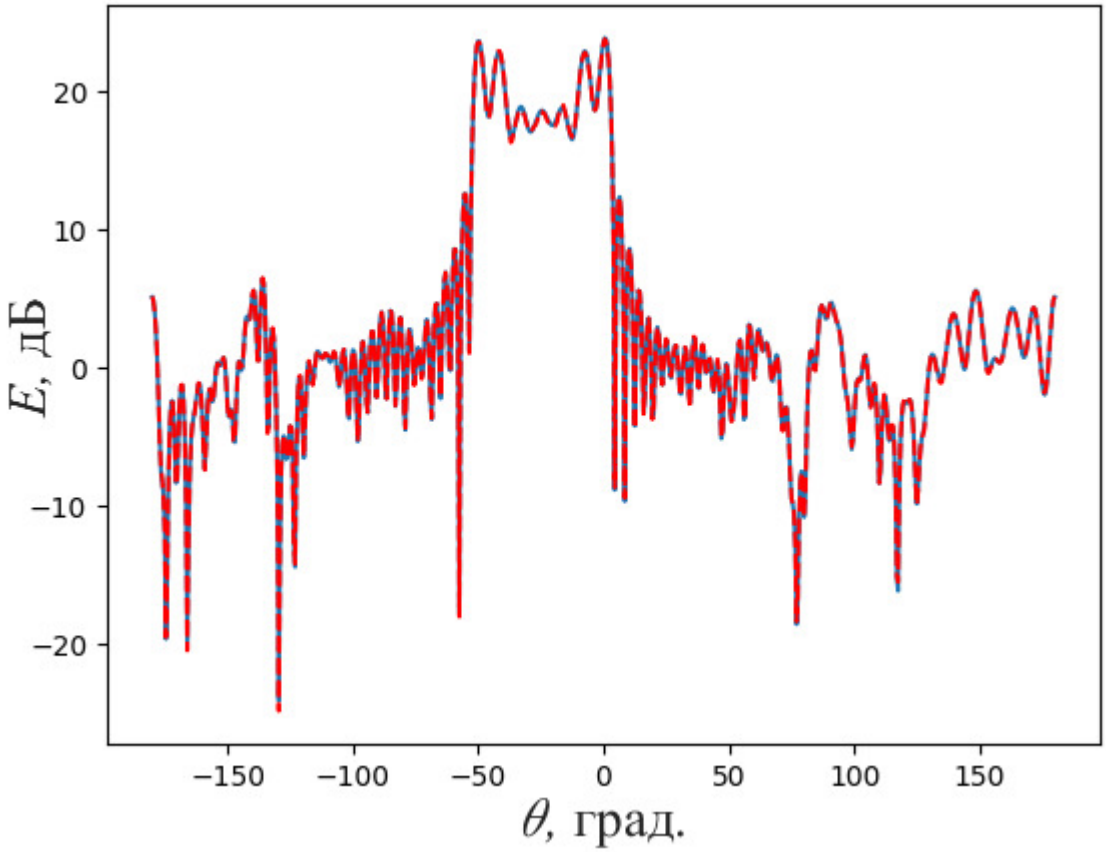


Рисунок 4 – График диаграммы направленности сферической линзовой антенны (синяя кривая – исходный график, красная – результат прогнозирования НС)

Как видно из рисунка 4, диаграмма направленности, полученная в результате прогнозирования НС, совпадает с исходной диаграммой направленности, рассчитанной в среде Ansys HFSS.

Таким образом, можно сделать вывод, что с помощью НС возможно осуществлять прогнозирование диаграммы направленности сферической линзовой антенны Люнеберга с приемлемой точностью.

Работа выполнена в рамках Государственного задания № 071–03-2023-001.

СПИСОК ЛИТЕРАТУРЫ:

1. Степанчук А.П. О решении задачи оптимизации антенны // Сборник научных статей 2-й Всероссийской научной конференции перспективных разработок молодых ученых, Курск. – 2018. – С. 340-343.
2. Abbassi P.K., Badra N. M., Allam A., El-Rafei A. WiFi Antenna Design and Modeling using Artificial Neural Networks // 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). – 2019. – P. 270-274.
3. Elsherbini A., Kamel A. H., Elhennawy H. Optimization of an Antipodal Vivaldi Antenna using Synthesis Neural Networks and a Novel Genetic Algorithms Approach // National Radio Science Conference, Egypt. – 2007. – P. 1-7.
4. Noh J., Nam Y., So S., Lee C., Lee S., Kim Y., T. Kim, Lee J., Rho J. Design of a transmissive metasurface antenna using deep neural networks // 2021 Optical Materials Express, Vol. 11, no 7, P. 2310–2317.
5. Кусайкин Д.В., Каменсков А.Е. Анализ подходов проектирования антенн с помощью нейронных сетей // Информационные технологии и когнитивная электросвязь, Екатеринбург. – 2022. – С. 164-168.

А.Т. Козловский

МЕТОДИКА ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ БАЗОВЫХ СТАНЦИЙ СЕТЕЙ ПОДВИЖНОЙ РАДИОСВЯЗИ И ЗОН ПОКРЫТИЯ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: поиск, обнаружение, подвижная радиосвязь, мероприятия подразделений главного радиочастотного центра (ФГУП «ГРЧЦ»).

В статье рассматриваются способы определения местоположения базовых станций (БС) сетей подвижной радиосвязи и зон их покрытия на основе обратного метода Монте-Карло. Применение в методике статистических методов анализа позволяет повысить достоверность реальной зоны покрытия операторов связи в субъектах Российской Федерации. Рассматриваемая методика включает получение статистических данных по качеству подвижной радиотелефонной связи; построение на основе открытых источников зон покрытия БС в локальном районе; моделирование плотности покрытия БС сетей подвижной радиосвязи в конкретном субъекте России.

A.T. Kozlovskiy

METHODOLOGY OF DETECTION OF MOBILE RADIO BASE STATIONS LOCATIONS AND THEIR COVERAGE AREAS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: search, detection, обнаружение, mobile radio communication, activities of divisions of Federal State Unitary Enterprise «State Radio Frequency Center».

In this article, we analyze technique of detection of mobile radio base station locations and their coverage areas by the reverse method of Monte-Carlo. Due to application of statistical analytical methods, our methodology makes it possible to improve the reliability of real coverage areas for telecommunications operator in Russian Federation regions. This methodology includes receiving statistical data about mobile radio communication quality; creating the base station coverage areas in the local district based on open data sources; modeling the coating density of mobile radio base station in a specific subject of Russia.

Обнаружение, идентификация параметров БС сотовых сетей, а также определение их местоположения и зон радиопокрытия в городах и на автомагистралях является одной из приоритетных задач территориальных подразделений ФГУП «ГРЧЦ» при проведении мероприятий по оценке качества услуг подвижной радиотелефонной связи на территории России [1].

Сложность проведения таких мероприятий обусловлена большим количеством БС операторов сотовых сетей подвижной радиосвязи (операторов связи) и их высокой плотностью расположения, особенно в городских условиях. Это вызывает трудности в выборе маршрутов движения возимых аппаратно-программных комплексов (АПК), которые должны охватывать магистральные дороги, улицы общегородского и местного значения, а также предусматривать заезды внутрь микрорайонов и дворовых территорий, что требует более детального распределения сил и средств подразделений ФГУП «ГРЧЦ».

Знание точного местоположения и зон покрытия БС на участке местности позволяет также выявлять несанкционированно работающие БС, проверять отклонение их местоположения от условий выданных разрешений, осуществлять проверку соблюдения частотно-территориального

плана [2]. Вопросы определения местоположения БС сетей подвижной радиосвязи приобрели особую актуальность после вхождения в состав Российской Федерации новых административно-территориальных субъектов. Особую важность при этом приобретают сбор информации о антенно-мачтовых сооружениях (в том числе ранее построенных) и о расширении зон покрытия сотовых операторов связи, оценка зоны электромагнитной доступности и анализ решений по вводу новых технологий и стандартов подвижной связи.

Для определения местоположения БС сотовых операторов связи целесообразно воспользоваться следующими способами:

1. Пеленгование и местоопределение БС с задействованием АПК мониторинга типа «Барс», «Артикул», Rohde&Schwarz ESMD и др. При этом осуществляется настройка аппаратуры пеленгования на частоту вещательного канала управления БС (BCCH) и определяется направление на источник излучения. В разных точках траектории маршрута движения выполняется обнаружение некоторого количества БС, их идентификация и формирование пеленга (адресное пеленгование). По совокупности пеленгов каждой из обнаруженных БС, характеризуемых своими идентификационными параметрами, выполняется расчет их местоположения [2]. Недостатком способа является большая трудоемкость обработки пеленгов, т.к. в крупных городах имеется множество БС, частоты которых (в т.ч. для стандарта GSM) используются операторами связи многократно.

2. Сбор и сопоставление данных от операторов связи и открытых интернет-сервисов, формируемых самими абонентами. Например, могут быть использованы различные информационные ресурсы сети «Интернет»: Geolocation от Google, OpenCelliD, Ultrastar, mobile.maps.yandex.net от Яндекса, cellmapper.net, mylnikov.org (через api-запросы), xinit.ru (перестал существовать после 2020 г.) и т.п. Данные сервисы содержат информацию об усредненном местоположении абонентов обслуживаемых БС мобильных операторов по всему миру. Так, базы данных сервисов Яндекса, Google, Mozilla Location Service (MLS) формируются путем сбора и сопоставления координат со встроенных GPS-приемников от мобильных станций абонентов сотовой сети (абонентских терминалов) и параметров обслуживающей БС (MCC, MNC, LAC, CellID). Основным недостатком данного способа является то, что точность позиционирования находится в прямопропорциональной зависимости от количества абонентских терминалов, находящихся в исследуемом районе, и обратно пропорционально дальности действия БС (радиусу зоны обслуживания). Однако, имея актуальные данные LAC и CellID по БС сотовой связи, с помощью указанных интернет-сервисов можно легко уточнить информацию о приблизительном местоположении БС различных операторов.

3. Получение и анализ информации от тестовых терминалов с установленными Android-приложениями (программ анализа) типа NetMonitor, Network Cell Info, OpenSignal App, Cellmapper, Cellumap, Cell Signal Monitor, «Сотовые вышки» и т.п. Данный способ заключается в определении местоположения БС путем накопления и сопоставления статистических данных о местонахождении абонентского терминала с программой анализа и служебной информации, получаемой от БС. Точность позиционирования при этом зависит от количества измерений расстояний от абонента до БС на основе значения Timing Advance, характеризующего временную задержку GSM (всего 63, по 550 м. каждое [3]). Местоположение БС уточняется путем обеспечения работы с нескольких позиций, оптимально 4-5 шт. В отдельных программах анализа сетей возможен экспорт полученной информации в файлы разных форматов. Недостатком данного способа является возможность определения местоположения только тех БС оператора, на которых с выбранных позиций производится регистрация терминала с заранее предустановленной программой типа NetMonitor, OpenSignal App и т.п.

Последний способ был использован в проекте Роскомнадзора «качествосвязи.рф», который описан в [4], и предназначен для инструментальной оценки показателей качества услуг в сетях подвижной радиотелефонной связи. Часто, радиоизмерения осуществляются с помощью программного обеспечения TEMS Automatic независимо в сотовых сетях стандартов GSM 900/1800, UMTS 1900/2100, LTE и по различным операторам связи с сохранением результатов в виде log-файлов, которые в последующем конвертируются в общедоступные форматы txt, csv и пр. Радиоизмерения проводятся с привязкой к местности с применением электронных топографических планов и карт конкретного субъекта России [1].

Стоит отметить, что получение и обработки информации по радиопокрытию подвижной радиотелефонной связью в субъектах Российской Федерации, а также на автомобильных дорогах федерального, регионального и местного значения осуществляется с помощью специально созданной автоматизированной системы контроля [4]. Однако массив анализируемых данных зависит от количества составленных маршрутов и, в настоящее время, охватывает территорию отдельных субъектов только по автомобильным дорогам, на которых, без указания зон покрытия и «секторов» БС операторов, отображено качество связи в стандартах GSM/ UMTS/ LTE.

В свою очередь, для определения зон покрытия БС сотовых операторов связи и границ их «секторов» на территории анализируемого субъекта Российской Федерации можно использовать моделирование медиаданных потерь на трассах наземной подвижной радиосвязи методом Окамура-Хата, рекомендованным МСЭ [5]. Проведенные исследования свидетельствуют о совпадении практически измеренных значений и рассчитанных с использованием данной модели. Однако ввиду большого количества измерений и невозможности автоматизации расчетов с использованием ПЭВМ, данный метод подразделениями применяется слабо.

Автор предлагает определять зоны покрытия, используя данные полученные с помощью комплексов мониторинга, программ анализа типа NetMonitor и Cellmapper, а также из проектов «качествосвязи.рф» [4], OpenCelliD [6]. При этом примерный радиус действия «сектора» БС можно вычислить путем анализа данных об измерениях и геоданных абонентов, находящихся на максимальном удалении от интересующей БС. Границы «сектора» БС могут также вычисляться на терминале абонента путем отслеживания процедуры Handover[1] на соседние БС. Точность определения зон покрытия зависит от количества исследуемых данных.

Определение границ «секторов» БС производится путем фиксации значений геоданных места и параметров БС в момент Handovera, которые отображаются в списке соседних БС. В любой программе анализа построение списка осуществляется путем ранжирования БС по уровню принимаемого сигнала на конкретной местности. Зная параметры БС, включая ее точное местоположение и направления перехода на соседние БС, можно установить границу «сектора». Далее посредством анализа индивидуальных log-файлов и графического моделирования данных на карте выявляются места и идентификаторы БС, на которых происходила передача абонента (терминала с программой анализа) в процессе его перемещения или нахождения на границе действия нескольких «секторов», и в результате рассчитывается зона покрытия конкретной БС. Полученные таким образом границы БС на местности в сочетании с имеющимися сведениями проектов [4] и [6] будут способствовать более точному определению зон радиопокрытия сети в локальных районах субъекта Российской Федерации.

Имея статистические данные о качестве связи на конкретной местности (районе) можно методом Монте-Карло рассчитать обоснованную долю покрытия БС оператора в заданном субъекте России. Указанный метод основан на применении теории вероятности к алгоритмическим процессам нахождения приближенных значений требуемых параметров. Значение отыскивается путем сравнения результатов равновероятных событий в двух множествах, одно из которых полностью включает другое. Так применив обратный метод Монте-Карло, можно более крупное множество задать как неизвестное (требуемое к отысканию), а полностью включенное множество (входящее в крупное) должно быть заведомо с известными значениями.

Например, пусть требуется изучить зону покрытия в заданном субъекте Российской Федерации N (неизвестное крупное множество) конкретного стандарта и оператора связи. При этом, имеются случайно выбранные локальные районы субъекта России известной площадью $S_{\text{района}}$ (например, маршрут, по которым заранее получены статистические данные о качестве связи), площадь субъекта России $S_{\text{субъекта}}$ также определена. В свою очередь, зоны покрытия БС на выбранных участках местности зависят от рельефа местности, мощности БС, стандарта связи и прочих характеристик, и проявляются через уровни приема сигналов, обозначенные на карте разными цветами: зеленым, желтым, красным и черным. В выбранном районе выполнены

[1] Процедура Handover — эстафетная передача терминала из зоны действия одного «сектора» БС в зону другого. Процедура отслеживается путем анализа информации, проходящей в вещательном канале управления *BCCH*.

измерения с конечным общим числом $Y_{\text{общ.}}$, которое для стандарта GSM включает число зон с параметрами: $Y_{\text{зел.}}$ — с хороших (>-80 dB) уровнем сигнала, $Y_{\text{жел.}}$ — нормальным (-80-90 dB), $Y_{\text{кр.}}$ — неуверенных (-90-100 dB) и $Y_{\text{чр.}}$ — неудовлетворительных (<-100 dB).

В результате для вычисления зоны покрытия с хорошим приемом (>-80 dB) следует:

$$\frac{S_{\text{района}}}{S_{\text{субъекта}}} = \frac{Y_{\text{зел.}}}{N_{\text{зел.}}}, \quad (1)$$

что приводит к следующему равенству:

$$N_{\text{зел.}} = \frac{S_{\text{субъекта}} \times Y_{\text{зел.}}}{S_{\text{района}}} \quad (2)$$

Также справедливо будет, что $Y = \frac{Y_{\text{зел.}}}{Y_{\text{общ.}}} \times \frac{Y_{\text{жел.}}}{Y_{\text{общ.}}} \times \frac{Y_{\text{кр.}}}{Y_{\text{общ.}}} \times \frac{Y_{\text{чр.}}}{Y_{\text{общ.}}}$

Вычисление доли происходит следующим образом:

$$N = \frac{S_{\text{субъекта}} \times \text{Y}}{S_{\text{района 1}} + S_{\text{района 2}} + \cdots + S_{\text{района } m}} \quad (3)$$

Аналогично, используя (2), через значения уровней в случайных районах (включая маршруты движения) можно (3) рассчитать долю покрытия подвижной радиотелефонной связи в субъекте Российской Федерации для различных стандартов конкретного оператора связи. Это также можно применить и для расчета других показателей качества связи в субъекте России.

Достоинство предлагаемой методики заключается в том, что любой абонент с вышеуказанными программами анализа на базе Android-приложений сам в состоянии на местности определить местоположение требуемой БС и зону ее покрытия без применения дополнительных комплексов и средств мониторинга. Использование в методике метода Монте-Карло позволяет за короткое время анализа получить достаточно точные решения о долях покрытия операторов в регионе, не прибегая к прямым вычислениям их значений.

Комплексное использование представленных способов позволит с высокой достоверностью выявлять зону покрытия БС сотовых операторов связи и границы их «секторов», что особенно актуально для новых административно-территориальных субъектов России. Рассматриваемая методика при организации мероприятий по оценке качества услуг подвижной радиотелефонной связи позволит за счет случайно выбранных районов на участке местности, и изучения, с помощью программ типа NetMonitor, OpenSignal App, уровня сигнала БС сотовой сети оператора связи оптимально распределять силы и средства подразделений ФГУП «ГРЧЦ».

СПИСОК ЛИТЕРАТУРЫ:

1. Методика оценки качества услуг подвижной радиотелефонной связи // утв. Минкомсвязь России от 08.06.2017 № НН-П19-12345, 2017, с. 31.
2. Манелис В.Б., Сладких В.А., Козьмин В.А., Бизюков П.Е. Адресное пеленгование базовых станций GSM, UMTS, LTE сетей сотовой связи // Системы управления, связи и безопасности. 2021. № 2. С. 142-158. DOI: 10.24412/2410-9916-2021-2-142-158.
3. Сервисные коды для различных телефонов, инженерное меню [Электронный ресурс]. Режим доступа: http://forum.netmonitor.ru, свободный. — Загл. с экрана. — Яз. рус.
4. Качество связи — информация о проекте [Электронный ресурс]. Режим доступа: http://качествосвязи.рф, свободный. — Загл. с экрана. — Яз. рус.
5. Рекомендации МСЭ – R 1546-4. Метод прогнозирования для трасс связи «пункта с зоной» для наземных служб в диапазоне частот от 30 до 3000 МГц. — Женева: МСЭ, 2010.
6. OpenCelliD — сервис о размещении БС [Электронный ресурс]. Режим доступа: http://opencellid.org, свободный. — Загл. с экрана. — Яз. англ.

И.В. Коробицын, Н.В. Будылдина

РАЗРАБОТКА СИСТЕМЫ МИКРОКЛИМАТА В ЛАБОРАТОРИИ «ИНТЕРНЕТ ВЕЩЕЙ И САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ»

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ) в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: IoT, умный дом, устройство, микроконтроллер.

В статье рассматриваются умные устройства системы микроклимата. Их функционал, реализация, взаимодействия этих устройств между собой, а также зачем такие устройства нужны.

I.V. Korobitsyn, N.V. Budyldina

DEVELOPMENT OF A MICROCLIMATE SYSTEM IN THE LABORATORY «INTERNET OF THINGS AND SELF-ORGANIZING NETWORKS»

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Key words: IoT, smart home, device, microcontroller.

The article discusses smart devices of the microclimate system. Their functionality, implementation, interactions of these devices with each other, as well as why such devices are needed.

На сегодняшний день система IoT (Internet of Things) является распространённой как в жилых домах, так и на предприятиях. Система умного дома служит для упрощения ежедневных рутинных работ и автоматизации процессов управления.

Система микроклимата является одной из ключевых систем элементов умного дома, так как включает в себя: отслеживание состояние воздуха, солнечного света, влажность воздуха, температуры помещения, и прочие факторы, связанные с человеком или окружающей его средой.

В качестве примера, будет рассматриваться такие устройства как: «умная розетка», «умная лампа» и «умные шторы». Все системы связаны между собой.

Начать стоит с устройства умных штор. Ключевой задачей данной системы является поднятие и опускание штор в зависимости от показателя освещённости в помещение. Схема данного устройства представлена на рисунке 1.

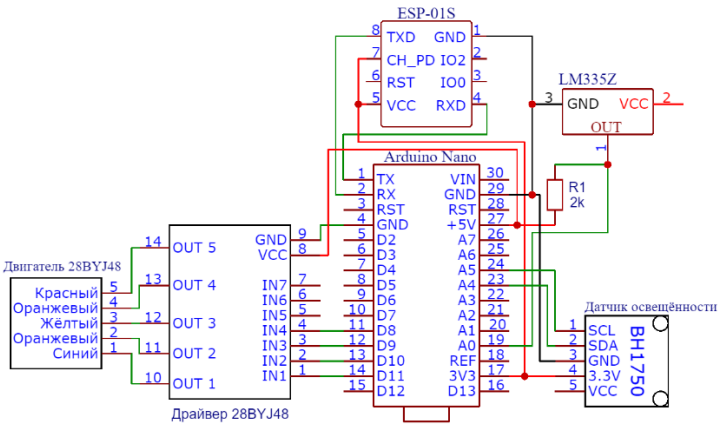


Рисунок 1 – Устройство «умные шторы»

В качестве микроконтроллера, выступает плата семейства Arduino. Датчик освещённости считывается спустя заданное количество времени и отправляет данные на микроконтроллер. Тот

в свою очередь отправляет эти данные с помощью Wi-Fi модуля (ESP-01S) на сервер. Из литературы [1] выберем архитектуру подключения устройств через маршрутизатор. Сервер принимает решения по текущим показателям освещённости, следует открывать или опускать шторы. После этого, решение поступает на микроконтроллер, который в свою очередь начинает выполнять один из двух сценариев: поднятие или опускание шторы, либо же оставить в текущем положение и ничего не изменять. Также данные показатели освещённости поступают уже на другое устройство, под названием «умная лампа». Устройство «умная лампа» представлено на рисунке 2.

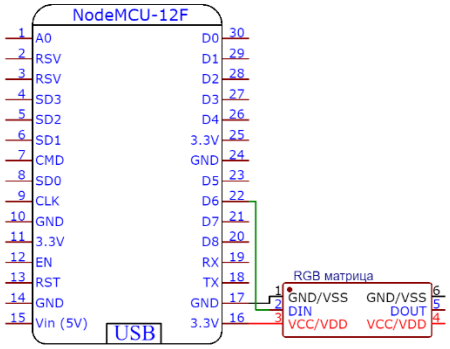


Рисунок 2 – Устройство «умная лампа»

В качестве микроконтроллера, выступает плата NodeMCU, которая включает в себя Wi-Fi модуль. В качестве RGB матрицы, используется матрица размером 8 на 8, но её можно поменять как на матрицу меньших размеров, так и на матрицу больших размеров. Главное учесть, что при подключении достаточно большой матрицы, потребуется внешний источник питания (блок питания).

Главное задачей лампы, является включение или отключение при определённых показателях освещённости. Данные показатели приходят от устройства «умные шторы». Также, датчик освещённости можно подключить и к другим устройствам, собрать суммарно данные, и выполнить сценарий включение или отключение от средних показателей датчика освещённости. Так как лампа является RGB, её можно использовать в качестве источника однотонного света, либо включить переливающиеся цвета. Это положительно скажется на самом человеке, так как источник света уменьшит нагрузку на глаза. Также данное устройство можно использовать в различных теплицах, что положительно скажется на растительности.

Помимо этого, устройство «умная розетка» работает в связке с предыдущими устройствами. Самое устройство представлено на рисунке 3.

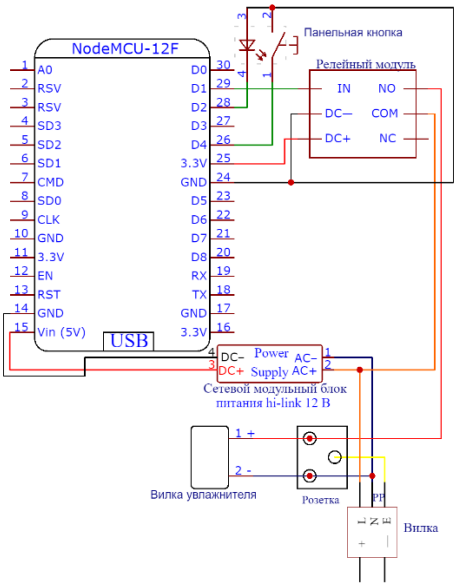


Рисунок 3 – Устройство «умная розетка»

Главной задачей устройства, включать или отключать дистанционно устройство, подключенное к нему. В качестве примера используется увлажнитель воздуха. Данное устройство, как и устройство «умная лампа», использует микроконтроллер NodeMCU. В зависимости от определённых показателей различных датчиков и самого устройства, которое подключается к розетке, решается включение или отключение розетки. В качестве примера датчика, будет использовать датчик влажности. При достижение порогового значения влажности в помещении, данные отправляются на сервер, который в свою очередь решает включить или отключить розетку. При получении ответа от сервера, устройство либо замыкает реле и включает устройство, либо размыкает и отключает устройство.

Таким образом необходимо отметить, что каждое из перечисленных устройств можно собрать в домашних условиях, при этом в разумных ценовых категориях. Все устройства при этом ограничиваются лишь возможностью самого пользователя, что позволяет открыть всех спектр возможностей данного устройства.

СПИСОК ЛИТЕРАТУРЫ:

1. Исследование взаимодействия умных устройств при разной архитектуре подключения к умному зеркалу. Авторы: Коробицын И.В., Будылдина Н.В., Юрченко Е.В. В сборнике: Инфокоммуникационные технологии: актуальные вопросы цифровой экономики. Сборник научных трудов III Международной научно-практической конференции. Под редакцией В.П. Шувалова, сост. М.П. Карачарова. Екатеринбург, 2023. С. 121-125.

И.В. Коробицын, А.А. Левиков, Е.В. Юрченко

СРАВНЕНИЕ ОБОРУДОВАНИЯ IoT ЗАРУБЕЖНОГО И РОССИЙСКОГО ПРОИЗВОДСТВА

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ) в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: Raspberry Pi, Arduino, IoT, Iskra, Repka Pi 3.

Согласно указу Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ», рассматриваются решения IoT, построенных базе зарубежного и отечественного производства. Сравнение показано по нескольким характеристикам: стоимость, тактовая частота, память и визуальное сравнение.

I.V. Korobitsyn, A.A. Levikov, E.V. Yurchenko

COMPARISON OF FOREIGN AND RUSSIAN IOT EQUIPMENT

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: Raspberry Pi, Arduino, IoT, Iskra, Repka Pi 3.

According to the decree of the President of the Russian Federation "On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation", IoT solutions built on the basis of foreign and domestic production are being considered. The comparison is shown by several characteristics: cost, clock frequency, memory and visual comparison.

Интернет вещей (IoT) – это сеть физических устройств, которые подключены к другим устройствам и службам через Интернет или другую сеть и обмениваются с ними данными. В настоящее время в мире более миллиарда подключенных устройств, и с каждым годом их становится больше. Все, что можно оснастить датчиками и программным обеспечением, можно подключить через Интернет. Сети IoT могут включать в себя множество элементов. Основные решения строятся на микроконтроллерах и микрокомпьютерах. Данные элементы выпускаются зарубежными и отечественными производителями. На сегодняшний день используются решения IoT, построенные на базе популярных плат семейства Arduino, Iskra, Vostok, Raspberry Pi, Repka Pi, Rock Pi. Платы семейства Arduino и Raspberry Pi производятся за рубежом, из-за чего цена на российском рынке выше оригинальной, что следует исходя из базовых затрат любого продавца: транспортировка, продажа и, конечно, извлечение прибыли.

Рассмотрим каждый элемент решения IoT по отдельности. Начнём сравнение характеристик плат микроконтроллера. Микроконтроллеры – это микрочип или плата с микрочипом для решения клиентских частей IoT-проектов. К ним относятся линейки плат Arduino, Iskra и Vostok.

Оригинальная стоимость платы Arduino, произведённой в Италии, значительно отличается от стоимости российского рынка. Если брать оригинальную плату, её средняя стоимость составляет около 28 $ (~2280 рублей на момент написание статьи), когда аналог стоит около 600-1000 рублей. В дальнейшем, будем использовать пример аналога.

В соответствие с этим, стоит разобрать российские аналоги данных устройств, и сравнить их по нескольким характеристикам, таких как: стоимость, рабочее напряжение, количество портов, ППЗУ, ОЗУ, ПЗУ, тактовая частота, кроссплатформенность и размер. Характеристики элементов разных производителей сведены в таблицу 1. [1,2]

Таблица 1 – Характеристики микроконтроллеров

Характеристики	Arduino Uno	Iskra Uno	Iskra JS	Vostok Uno
Средняя цена на рынке, руб.	1000	1100	2400	4800
Рабочее напряжение, В.	5	5	3,3	5
Количество портов	20 (14 цифровых, 6 аналоговых)	20 (14 цифровых, 6 аналоговых)	26 (14 аналоговых, 22 цифровых)	27
ППЗУ (Flash)	16 Кб	32 Кб	1024 Кб	16 Кб
ОЗУ (SRAM)	1 Кб	2 Кб	192 Кб	512 байт
ПЗУ (EEPROM)	512 байт	1 Кб	1 Кб	64 Кб
Тактовая частота	16 МГц	16 МГц	168 МГц	4 МГц
Кроссплатформенность	Windows, Linux, MacOS	Windows, Linux, MacOS	Windows, Linux, MacOS	Windows, Linux, MacOS
Размер	69x53	69x53	69x53	68x54

Проанализировав характеристики микроконтроллеров, можно сделать вывод, что рассматриваемые решения обладают примерно одинаковыми размерами, а главное их различие - тактовая частота и память. При визуальном сравнении Arduino Uno и Iskra Uno, можно увидеть, что платы похожи друг на друга, но имеют некоторые различия. Самое главное отличие плат в том, что Iskra Uno имеет в 2 раза больше памяти (ППЗУ, ОЗУ и ПЗУ). По количеству портов, размерам, рабочему напряжению и тактовой частоте - платы одинаковые. Также, платы приблизительно одинаковы по ценовой категории. Из чего можно сделать вывод, что плата Iskra Uno является прямым аналогом Arduino Uno, что положительно сказывается на внутреннем производстве в России. Так как большинство параметров одинаковые, обычному пользователю будет легче привыкнуть к новой плате, ведь она похожа на то, с чем он работал раньше. Внешний вид плат показан на рисунке 1.

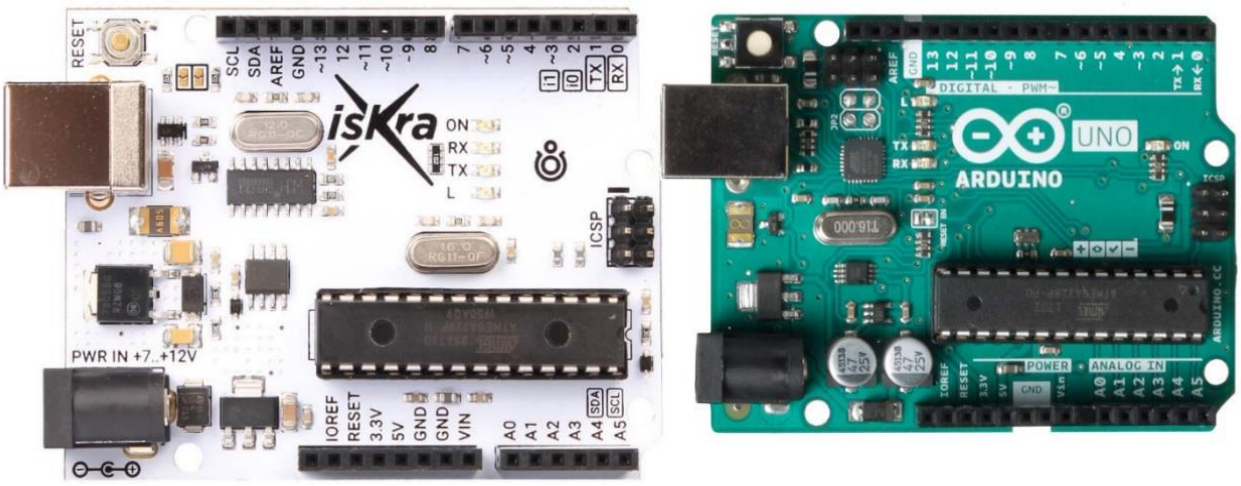


Рисунок 1 – Сравнение плат Iskra Uno и Arduino Uno

Также, у Iskra есть модель с более мощной комплектацией, нежели рассмотренные ранее. Модель платы Iskra JS гораздо мощнее своего аналога Iskra Uno, так как язык программирования этой платы - JavaScript. Плата представлена на рисунке 2.

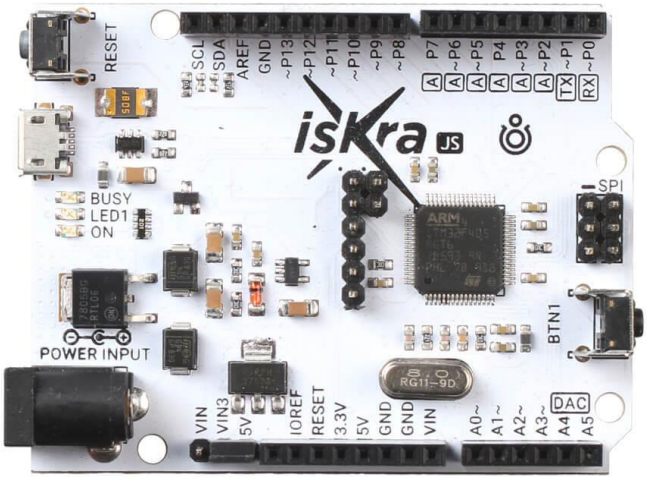


Рисунок 2 – Плата Iskra JS

Так как язык программирования платы JavaScript, можно собрать множество проектов, которые требуют большой вычислительной мощности. Пример такого проекта — это «промышленная автоматика». Из достоинств в использовании JavaScript можно отметить простоту и удобство. Программирование платы Iskra JS, в сравнении с C++, значительно упрощено.

Модель платы производителя Vostok Uno, имеет более весомые отличия от плат, рассмотренных ранее. Плата представлена на рисунке 3.

Рисунок 3 – Плата Vostok Uno

Визуально можно заметить, что платы внешне похожи, но самое главное их отличие — это используемый микроконтроллер. Тактовая частота здесь в 4 раза меньше, чем у микроконтроллера у Arduino Uno и Iskra Uno (ATMEGA328p). Также, ППЗУ больше, чем у Arduino Uno в 128 раз, но при этом ОЗУ меньше в 2 раза. Высокий ценник, почти в 5000 рублей, обусловлен малой партией товара, и в будущем цена может опуститься до цены Arduino Uno.

Помимо микроконтроллеров, рассмотрим микрокомпьютеры. Микрокомпьютеры – это компьютеры, в которых центральный процессор размещён на одной микросхеме, микропроцессоре, устройстве ввода-вывода и блоке хранения памяти. Есть множество вариаций, но самым предпочтительным решением для IoT является зарубежный Raspberry Pi. Оригинальная цена Raspberry Pi в Великобритании (стране-производителя) составляет около 65 $ (~5300 рублей на 2023 год). В это же время, в России цена на плату Raspberry Pi составляет от 15000 рублей (при этом, в магазине данного товара может не быть в наличии). Российским аналогом для

Raspberry Pi являются Repka Pi и Rock Pi. Сравнительные характеристики данных плат сведены в таблицу 2. [3,4]

Таблица 2 – Характеристики микрокомпьютеров

Характеристика		Raspberry Pi 3 Model B+	Repka Pi 3	Rock Pi 4 Plus v1.73
Процессор	Наименование	ARM Cortex-A53(BCM2837)	Allwinner H5 Ядра ARMv8 Cortex-A53	Rockchip RK3399 (OP1): два ядра Cortex-A72, 1,8 ГГц + четыре ядра Cortex-A53, 1,4 ГГц;
	Архитектура	64 бит	64 бит	64 бит
	Тактовая частота	1,2 ГГц	1,0-1,4 ГГц	1,4 и 1,8 ГГц
	Количество ядер	4	4	4
Графический процессор		VideoCore IV	ARM Mali-450MP	Mali T860MP4
Память	ОЗУ	1 Гб (LPDDR2 SDRAM);	1 Гб SDRAM LPDDR3	4ГБ LPDDR4 SDRAM
	ПЗУ	———	———	До 128 Гб eMMC
	Поддержка SD-карты	Поддерживается	Поддерживается	До 128 Гб
	Поддержка NVME	Внешним модулем	Внешним модулем	До 2 Тб
Сеть	Ethernet	300 Мбит/с RJ-45	100 Мбит/с RJ-45	1 Гбит/с RJ-45
	Поддержка PoE	Внешним модулем	Внешним модулем	Да
	Wi-Fi	Wi-Fi 5	Wi-Fi 5	Wi-Fi 5
	Bluetooth	Bluetooth 4.1 с BLE	Bluetooth 5	Bluetooth 5
Питание	Напряжение	5 В	5 В	5 В
	Ток	2,5 А	2-2,5 А	2,5 А
	Интерфейс подключения	Micro-USB GPIO	Micro-USB GPIO	Type-C GPIO
Потребляемая мощность		300 мА (1,5 Вт) – режим ожидания ——— ——— –	350 мА (1,75 Вт) – режим ожидания 1,65 А (8,25 Вт) – максимум	——— ———
Интерфейсы		USB 2.0 x 4 HDMI 1.3a 3,5 мм jack CSI	USB 2.0 x 4 HDMI 3,5 мм jack CSI	USB 2.0 x 2 USB 3.0 x 2 HDMI 2.0 3,5 мм jack CSI
Производитель		Великобритания	Россия	Китай
Размеры	ШхД	85x56	86x58	85x54
Цена		~ 3890 рублей и более СНЯТ С ПРОДАЖИ	13000 рублей	11050 рублей

Проанализировав характеристики микрокомпьютеров, можно сделать вывод, что рассматриваемые платы имеют одинаковую архитектуру, количество ядер процессора, имеют поддержку PoE, Wi-Fi 5, идентичны по электропитанию и интерфейсам. К отличиям можно отнести память, стандарты Ethernet и Bluetooth, а также ценовая категория, в которой наименьшую стоимость на сегодняшний день является китайский производитель.

Рассмотрим визуальные различия данных плат. Сразу стоит отметить, что платы линейки Rock Pi идут сразу от 4-го поколения, что сопоставимо с Raspberry Pi 4. Платы представлены на рисунке 4.

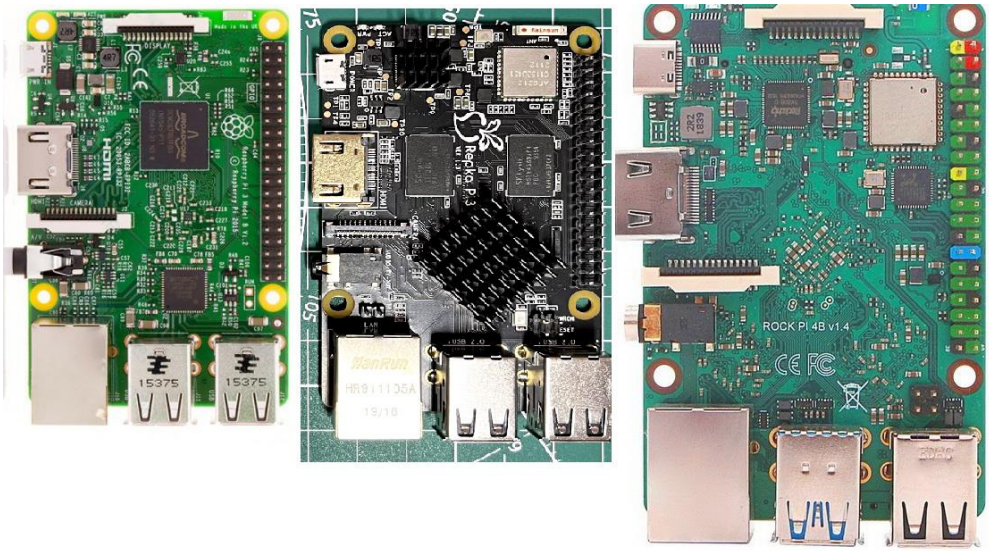


Рисунок 4 – Микрокомпьютеры Raspberry Pi 3, Repka Pi 3, Rock Pi 4

Микрокомпьютеры похожи по размерам и внешне, но различия имеются. Первым ключевым отличием трёх плат, является их оперативная память. В случае Raspberry Pi, используется старый стандарт LPDRR2 на 1 Гб ОЗУ. У платы Repka Pi также 1 Гб ОЗУ, но с уже более новым стандартом LPDDR3. В свою очередь, так как плата Rock Pi является более позднего выпуска сравниваемых плат, микрокомпьютер использует современный стандарт LPDDR4 на 4 Гб ОЗУ. Объём оперативной памяти может варьироваться в зависимости от модели платы.

Следующим отличием является наличие ППЗУ и подключение NVMe напрямую к плате Rock Pi, в то время как платы Raspberry Pi и Repka Pi отсутствует ППЗУ и для подключения NVMe используется дополнительные аксессуары.

Далее, следует сравнить стандарты связи, используемые данными платами. Raspberry Pi использует старый стандарт Bluetooth, но с поддержкой BLE (Bluetooth Low Energy). В то время как Repka Pi и Rock Pi стандарт 5-го поколения. Wi-Fi все три платы используют 5-го поколения. Проводное соединение через RJ-45 передаётся со скоростью 300, 100 и 1000 Мбит/с соответственно для Raspberry Pi, Repka Pi и Rock Pi.

Для электропитания всех трёх плат достаточно 5 В и 2-2,5 А, но в случае Rock Pi, используется в качестве разъёма Type C.

Таким образом отметим, что характеристики рассмотренных плат микроконтроллеров и микрокомпьютеров относительно похожи друг на друга. Стоимость рассмотренных производителей может варьироваться от ситуации на рынке. В связи с указом Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ», на сегодняшний день можно приобрести российские аналоги, которые не уступают зарубежным аналогам по характеристикам, и при этом получить похожий функционал, а в некоторых случаях и гораздо больше.

СПИСОК ЛИТЕРАТУРЫ:

1. Макаров С.Л. ARDUINO UNO И RASPBERRY PI 3: от схемотехники к интернету вещей // ДМК Пресс, 2019, с. 25-37.
2. Iskra UNO и Iskra JS: инструкция, примеры использования и документация [Электронный ресурс] Режим доступа URL: http://wiki.amperka.ru/products:iskra-uno Дата обращения: 09.04.2023
3. Repka Pi 3: руководство [Электронный ресурс] Режим доступа URL: https://rbs-computers.ru/repkapi3 Дата обращения: 10.04.2023
4. Rock Pi: официальный сайт [Электронный ресурс] Режим доступа URL: https://rockpi.eu/Rockpi4/hardware Дата обращения 10.04.2023

Д.Л. Кумачев, В.В. Гладнев, О.Л. Михайленко
Научный руководитель: директор учебно-научного центра «Информационная безопасность», доктор технических наук, профессор Поршнев С.В.

АВТОМАТИЗАЦИЯ ПРОЦЕССА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТ - МАГАЗИНА

Уральский федеральный университет, Институт радиоэлектроники и информационных технологий-РТФ в г. Екатеринбурге, Россия

Ключевые слова: Интернет, система защиты информации, информационная безопасность, аудита безопасности.

Автоматизация процесса аудита информационной безопасности интернет-магазина может быть достигнута с помощью специализированного программного обеспечения, которое позволяет автоматически сканировать веб-сайт на наличие уязвимостей и других проблем, связанных с безопасностью. Кроме того, автоматические инструменты могут проводить анализ журналов доступа и системных журналов для обнаружения необычной активности, которая может указывать на наличие взлома или других нарушений безопасности.

D.L Kumachev, V.V. Gladnev, O.L. Mikhailenko
Scientific supervisor: Director of the educational and Scientific center "Information Security", Doctor of Technical Sciences, Professor Porshnev S.V.

AUTOMATION OF THE ONLINE STORE INFORMATION SECURITY AUDIT PROCESS

Ural Federal University, Institute of Radio Electronics and Information Technologies-RTF in Yekaterinburg, Russia
Keywords: Internet, information security system, information security, security audit.

Automation of the online store information security audit process can be achieved with the help of specialized software that allows you to automatically scan a website for vulnerabilities and other security-related problems. In addition, automated tools can analyze access logs and system logs to detect unusual activity that may indicate the presence of hacking or other security breaches.

Интернет торговля сегодня – популярный способ совершения покупок, которому отдает предпочтение множество покупателей. Вместе с активным ростом и развитием таких площадок, растет интерес к интернет-магазинам со стороны киберпреступников. Интернет-магазины привлекательная мишень для кражи информации и получения незаконной прибыли от выполнения заказов недобросовестных конкурентов ресурса. Это могут быть DDOS-атаки, взлом, заражение вирусным ПО.[3] В рамках настоящего исследования ставится цель – создание и получение практического опыта эксплуатации сканера уязвимостей, выполненного на базе общедоступных сервисов на примере малого предприятия, такого, как интернет-магазин.

Среди угроз безопасности информации такого предприятия, как интернет-магазин можно выделитm несколько наиболее актуальных. Первой из них можно считать утечку данных пользователей. Совершая покупки в интернет-магазинах, пользователи передают большой объем персональных и финансовых данных, хищение которых представляет интерес для злоумышленников. Для завладения такими данными используется заражение вирусным кодом интернет-магазина или перенаправление на поддельные фишинговые сайты. Второй по количеству реализации угрозой является заражение программного кода. Внедрение вредоносного кода в программную платформу интернет-магазина отрицательно влияет на его работоспособность и рейтинг в поисковых системах. В результате заражения замедляется работа,

появляются ошибки, пустые окна, посторонний текст и реклама. Поисковые системы самостоятельно обнаруживают угрозы внутри сайта, после чего относят его к потенциально опасным, вносят в свой «черные списки» и не отображают при запросах пользователей. Не менее популярными являются атаки, направленные на возникновение отказа в обслуживании или DDOS атаки (Distributed Denial of Service), направленной на отказ в обслуживании. При DDOS атаке интернет-магазину направляется большой поток ложных запросов из разных точек. Ресурс не может справиться с таким лавинообразным потоком обращений, в результате это приводит к остановке его работы и как следствие простоям в бизнесе. Также актуальной является атака, направленная на воровство трафика. В результате внедрения в программный код сторонних включений и ссылок, злоумышленники осуществляют редирект (перенаправление) пользователей, заходящих в интернет-магазин, на сторонние, конкурентные или поддельные фишинговые сайты.[4]

Проведение аудита информационной безопасности позволяет оценить текущее состояние системы защиты информации, а также принять необходимые меры, направленные на ее развитие и достижение критериев, на соответствие которым проводился аудит, однако владелец интернет-магазина чаще всего является начинающим бизнесменом и данный процесс для него является сложным. Но в реальности это не так.

На данном этапе исследования необходимо привести рассмотрение уязвимостей корпоративной сети, как телекоммуникационной транспортной среды, обслуживающей сам сервер интернет-магазина. Начать стоит с того, что необходимо классифицировать нарушителей. Это могут быть как нарушители, действующие в пределах сети (легитимные пользователи, сотрудники предприятия, в чьем управлении находится сеть) и инсайдеры (внешние пользователи, сумевшие обойти механизмы защиты).

В случае несанкционированных действий сотрудника, имеющего доступ её ресурсам сети, необходимо грамотно выстраивать политику аудита информационной безопасности, а также политику разграничений прав доступа. Например, сотрудник, установивший носитель нелегально и попытавшийся получить данные с персонального компьютера – реальная угроза. В рамках корпоративной сети необходимо продумать механизм защиты от подобных ситуаций. Также незадействованные порты коммутаторов необходимо выключать аппаратно, а вход в операционную систему коммутаторов и маршрутизаторов (как консольный, так и терминальный) необходимо осуществлять только при наличии пароля, известного администратору сети, который периодически меняется.

Необходимо понимать, что пользователи, действующие с целью похищения данных, могут работать удаленно. Также удаленно могут осуществлять деятельность и инсайдеры. Основной атакой инсайдера может стать пользовательский терминал или сервер. При получении доступа к этим ресурсам инсайдер может работать с информацией или менять конфигурацию сети так, как ему это необходимо. На Рисунке 1 приведена схема атак нарушителей из внешней или внутренней телекоммуникационной среды.

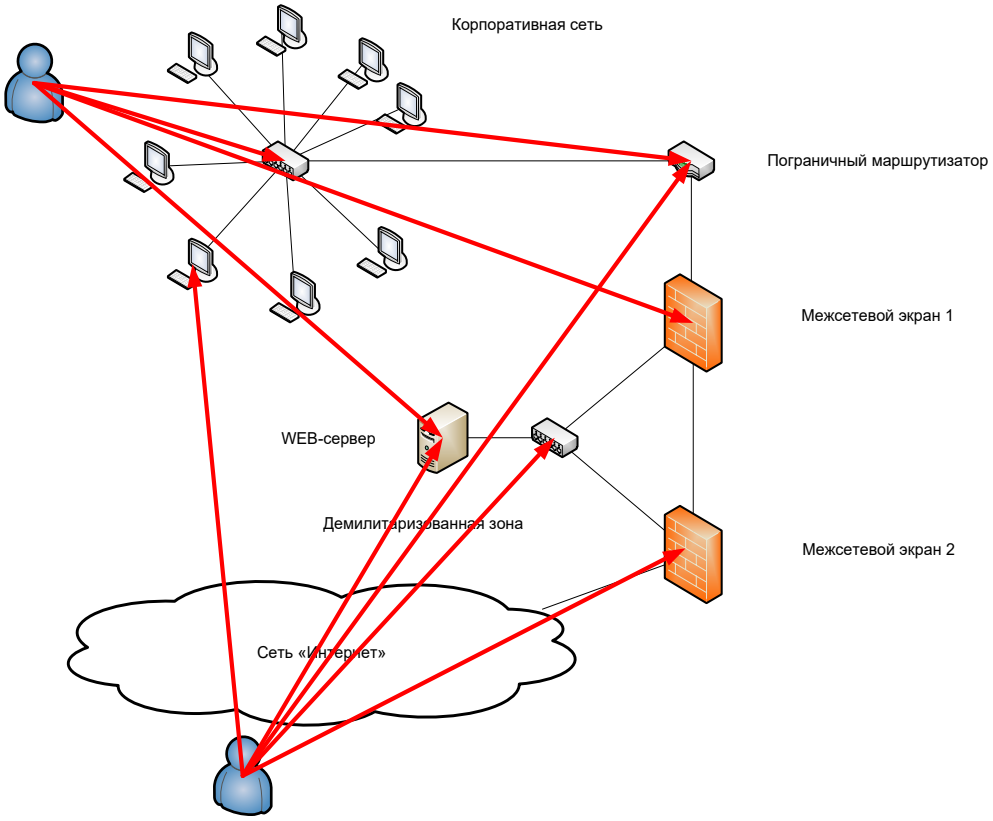


Рис. 1 – Схема атак на участки корпоративной сети

Данные атаки можно классифицировать таким образом:

Из внешней или внутренней среды – на межсетевые экраны (для изменения их политики фильтрации трафика), на маршрутизатор (для изменения таблицы маршрутизации), на коммутатор (для получения доступа к транспортной среде) на локальную рабочую станцию или сервер (для получения доступа к информации, хранящейся или обрабатывающейся на них).

Также на все устройства может быть оказано воздействие для получения отказа в обслуживании (когда устройство перестает обрабатывать запросы легитимных пользователей).

Подсистема активного аудита безопасности автоматически обнаруживает нарушения безопасности критически важных компонентов интернет-магазина и реагирует на них в режиме реального времени. Ключевыми компонентами интернет-магазина, которые, скорее всего, будут атакованы киберпреступниками, являются внешний безопасный шлюз в «Интернет», группа серверов и рабочие станции для управления интернет-магазином. Эта подсистема тесно интегрирована в подсистему регистрации и пассивного аудита, поскольку она частично использует данные аудита, полученные из этой подсистемы, для выявления атак и активации алгоритмов автоматического ответа. [3]

На данном этапе исследования предлагается создать простейший анализатор сетевого трафика в качестве подсистемы аудита информационной безопасности, который должен обнаруживать известные типы сетевых атак, включая атаки, направленные против следующих приложений:

– СУБД, Web, FTP, TELNET и почтовые серверы;
– Серверы NIS, DNS, WINS, NFS и SMB;
– Почтовые агенты и Web-браузеры.

Выявление сетевых и локальных атак и других нарушений безопасности интернет-магазина, а также реагирование на них должны осуществляться в реальном времени.

Графический интерфейс был реализован на виртуальной машине под операционной ситсемой Debian, на языке Phyton. Для его запуска необходимо ввести команду «python3 ui_vulners.py». Запустится графический интерфейс для работы со сканерами. Запуск скрипта представлен на Рисунке 2.

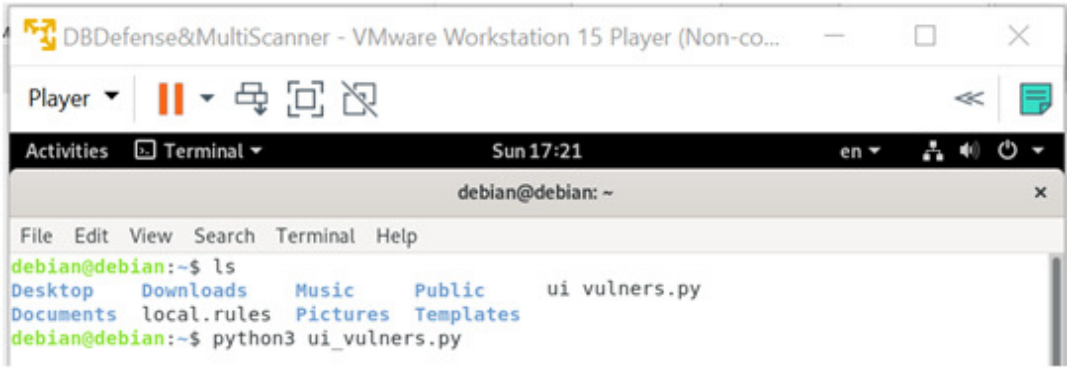


Рис. 2. Запуск скрипта.

Далее необходимо указать диапазон адресов в поле сверху, выбрать базу данных уязвимостей, используемую для сканирования слева (поставить «галочки»), нажать «Начать сканирование». Дождаться окончания сканирования, логи появятся в текстовом поле внизу. Для очистки логов нажать кнопку «Очистить логи».

Для закрытия графического интерфейса нажать на крестик в верхнем правом углу.

На данном этапе необходимо провести проверку срабатывания системы. Существуют известные базы уязвимостей, которые используются всем интернет-сообществом. В рамках реализации системы они будут подключаться к скрипту, поиск будет происходить по ним.

Пример сообщения о том, что, возможно, используется программное обеспечение, которое некоторое время раздавалось на одной из точек распространения с заложенным вирусом типа «троян» (CVE-1999-0661) приведен на Рисунке 3.

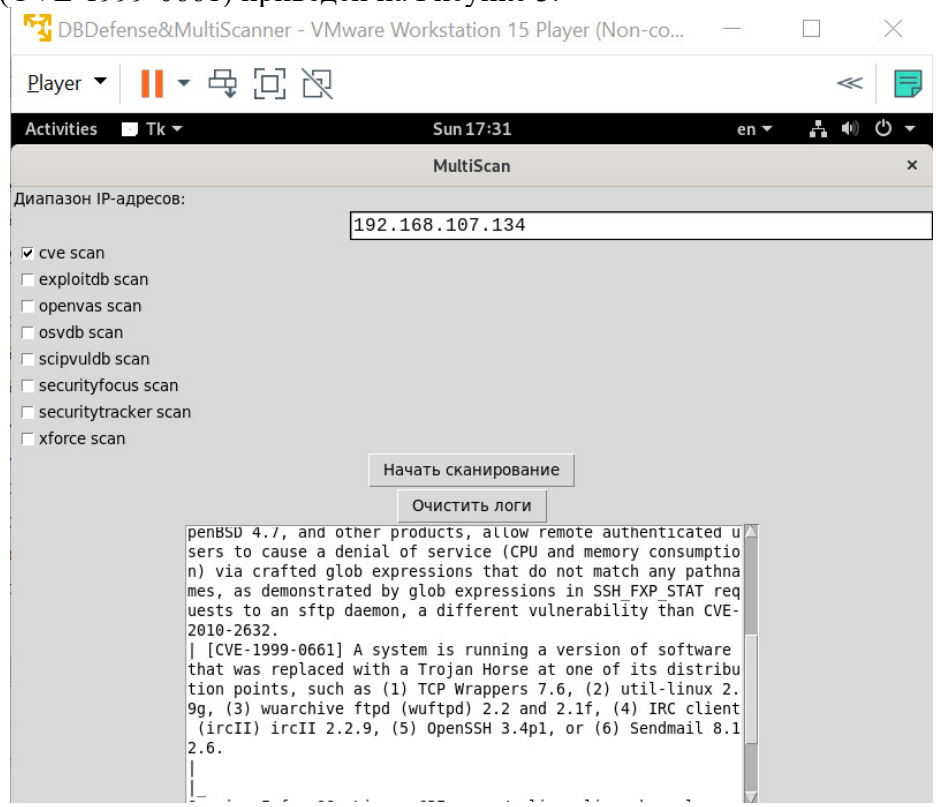


Рис. 3 – Пример срабатывания системы с помощью одной базы.

Можно выполнить сканирование с использованием сразу всех баз. Это приведено на Рис. 4.

Рисунок 4. Пример срабатывания системы с помощью всех баз.

Также можно выполнить сканирование при помощи другой базы, например, только базы OpenVAS. Это приведено на Рисунке 5.

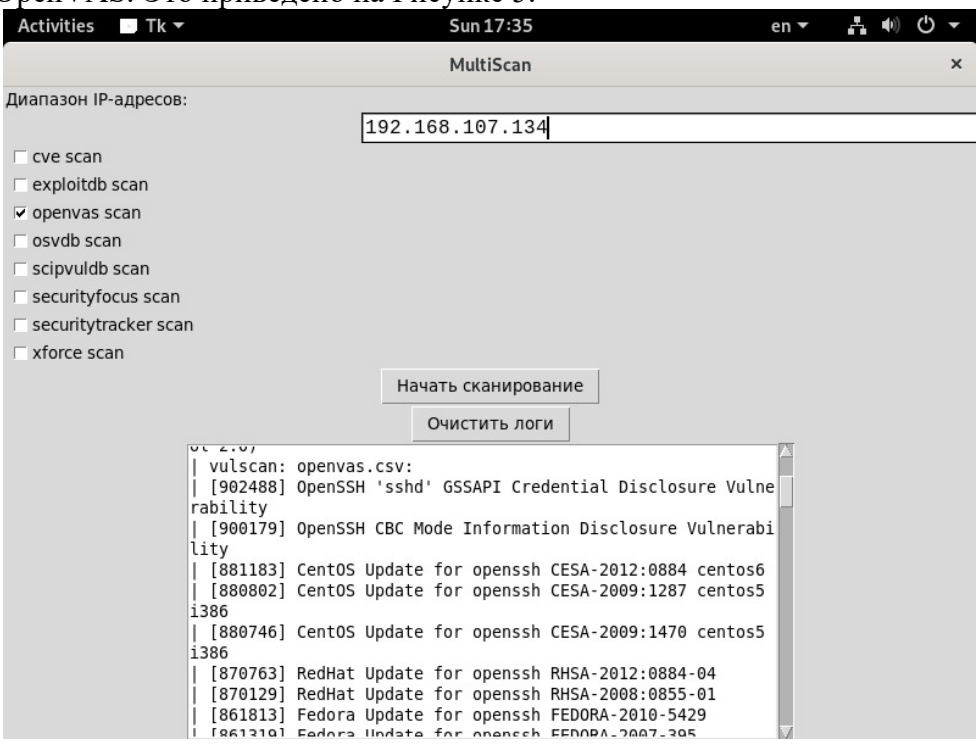


Рисунок 5. Пример срабатывания системы с помощью базы OpenVAS.

Также можно сканировать целые подсети (задавая их в стандартном для nmap формате), это приведено на Рис. 6.

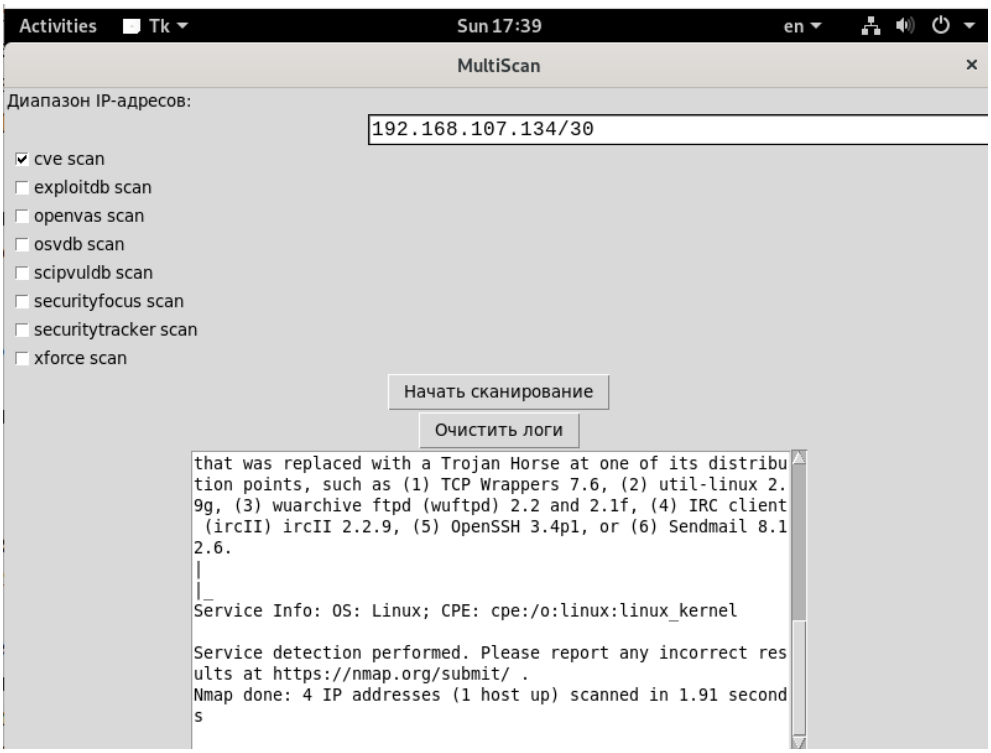


Рис. 6 – Пример сканирования подсети.

Это нужно для того, чтобы определить, какой из серверов является по сути WEB-сервером, так как интернет-магазин устанавливается на базе WEB-сервера.

Также данная система может работать по адресам сайтов. эксперимента необходимо узнать сетевое имя сервера, на базе которого запущен интернет-магазин. Это представлено на Рисунке 7.

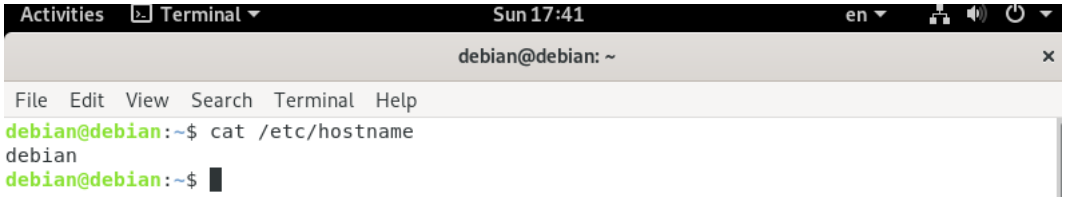


Рис. 7 – Идентификация сетевого имени узла.

Можно подставить его вместо адреса. Это приведено на Рисунке 8.

Рис. 8 – Проведение сканирования интернет-магазина.

Аналогично можно исследовать и другие сайты по их имени.

Стоит отметить, что сканирование доменных имен сайтов допускается только с разрешения владельца данного электронного актива в соответствии с законодательством Российской Федерации. Сканировать можно только то, на что владельцем дано прямое разрешение. На Рисунке 9 приведен пример использования, без непосредственного запуска. Сетевой узел с адресом www.e1.ru в реальности не сканировался.

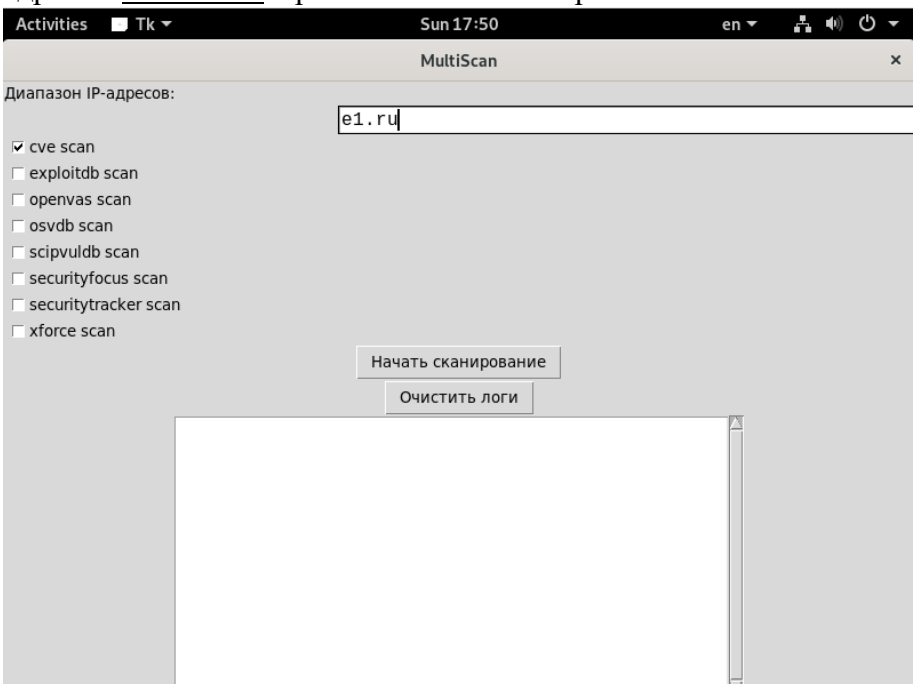


Рис.9 – Пример подстановки имени сетевого узла для сканирования.

В результате проведения исследования была разработана система автоматического аудита безопасности интернет-магазина. Использование этой системы позволяет выбирать, какие именно базы уязвимостей нужно подключить для проведения сканирования и получения данных, при помощи которых аудитор информационной безопасности будет делать вывод о защищенности веб-ресурса. Стоит также отметить, что использование стандартных средств – менее гибкое решение, так как они разработаны под универсальные требования, а программное обеспечение, спроектированное и реализованное в рамках настоящей работы может быть доработано, переконфигурировано, а также изменено по требованиям заказчика. Выбор баз уязвимостей, постоянно пополняемых пользовательским сообществом, также имеет высокую важность, ведь аудитор безопасности может определить, стоит ли тратить время на сканирование по определенным видам атак, либо необходимо сразу переходить к другим.

Все поставленные цели достигнуты и задачи решены.

Дальнейшие научные интересы автора лежат в области анализа существующих и подбору оптимальных решений для обеспечения безопасности функционирования веб-сервисов.

Список литературы:

1. Ларионцева Е. А. Проблемы и средства защиты информации. // Наука и образование. - 2017. - № 4.- С. 83-87.
2. Атре Ш. Структурный подход к организации баз данных. – М.: Финансы и статистика, 2018. – 320 с.
3. Маглинец Ю.А Анализ требований к автоматизированным информационным системам: Учебное пособие. – СПб.: Бином, 2017. – 200 с.
4. Щеглов А.Ю. Компьютерная безопасность. Вопросы комплексирования. Системный подход к построению системы защиты информации от несанкционированного доступа. [Электронный ресурс] – Режим доступа. - http://www.itsec.ru/articles2/Inf_security/voprosy-kompleksirovaniya (дата обращения: 31.03.2020).

5. Утебов Д.Р. Классификация угроз в системах управления базами данных // Вестник АГТУ. - 2019. - № 1.- С. 87-92.
6. Wapiti. URL: http://wapiti.sourceforge.net/ (дата обращения: 31.03.2020).

О.Д. Лобунец

СИСТЕМА ОДНОКАНАЛЬНОЙ МНОГОАБОНЕНТНОЙ СВЯЗИ С УПРАВЛЯЕМЫМ ПРИОРИТЕТОМ ПЕРЕДАЧИ СООБЩЕНИЙ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: система связи, абонент, канал, сообщение, передача, приоритет, управление, коэффициент использования.

В статье описана система для организации одноканальной многоабонентной связи со случайным доступом абонентов в канал передачи сообщений. Отличительной особенностью данной системы связи асинхронного типа является обеспечение возможности управления приоритетом передачи сообщений в соответствии с принятым списком, как на стадии подготовки, так и в процессе их передачи. При этом устройство одноканальной многоабонентной связи позволяет получить значения коэффициента использования канала связи близкие к единице.

O.D. Lobunets

SINGLE-CHANNEL MULTI-COMPONENT COMMUNICATION SYSTEM WITH MANAGED MESSAGE PRIORITY

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: communication system, subscriber, channel, message, transmission, priority, management, utilization factor.

The article describes a system for organizing single-channel multi-component communication with random access of subscribers to the message transmission channel. A distinctive feature of this asynchronous type communication system is the ability to control the priority of message transmission in accordance with the accepted list, both at the preparation stage and during their transmission. At the same time, the device of single-channel multi-component communication allows you to obtain values of the utilization factor of the communication channel close to one.

Важнейшими требованиями, предъявляемыми к системам передачи сообщений, являются своевременность и точность их воспроизведения в удаленных пунктах приема. Точность воспроизведения обычно достигается при увеличении помехоустойчивости и надежности технических средств передачи информации, а также путем использования эффективных корректирующих кодов. Своевременность передачи сообщений может быть достигнута при повышении скорости передачи информации и улучшении организации связи в многоабонентных каналах.

Так как синхронные системы связи [1,2] в принципе не могут обеспечить возможность управление приоритетом источников сообщений, то была разработана асинхронная система для одноканальной многоабонентной связи [3], которая имеет возможность управления приоритетом сообщений при их формировании, а также в процессе их передачи.

Каждый из абонентов системы состоит из приемопередающего устройства 1 (рис.), которое в составе имеет модулятор 2, приемопередатчик 3, фильтр 4, амплитудный дискриминатор 5 и устройство коммутации 6, а также элемент ИЛИ 7, формирователь 8, элемент задержки 9, RS-триггер 10, счетчик 11, дешифратор 12, формирователь 13 импульсов приоритета и блок 14 управления приемом и воспроизведением информации.

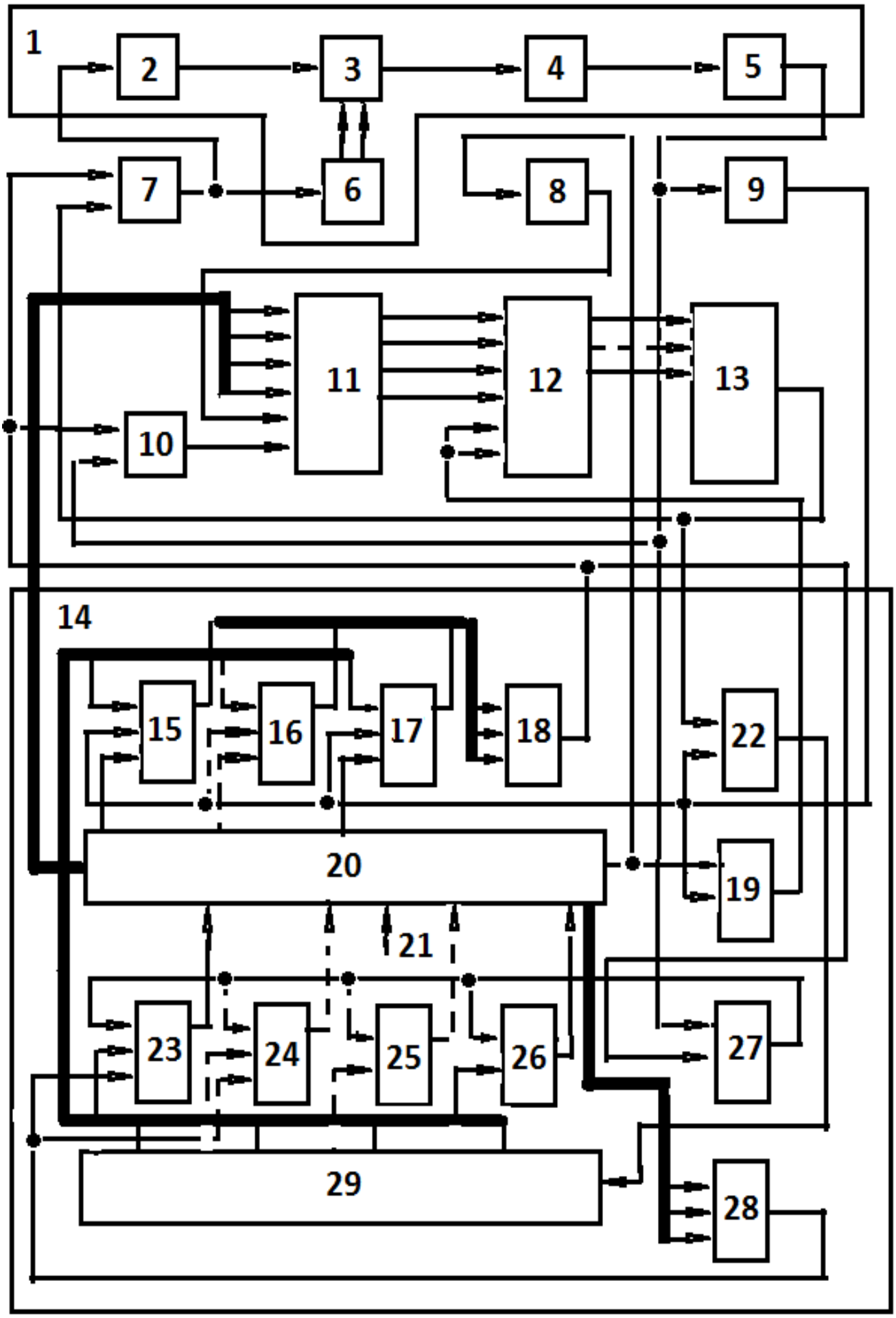


Рис. Схема устройства абонента системы одноканальной многоабонентной связи

Данный блок состоит из группы элементов 15 – 17, воспроизведения информации, первого и второго элементов И – НЕ 18, 19, регистра 20, имеющего вход управления 21, из третьего элемента ИЛИ 22, группы элементов 23 – 26 приема информации, первого элемента ИЛИ 27, элемента И 28 и распределителя 29.

При появлении сигнала на входе приемопередатчика 3 он усиливает этот сигнал и подает его на вход фильтра 4. После фильтрации форма сигнала восстанавливается амплитудным дискриминатором 5. Единичный сигнал на входе элемента задержки 9 вызывает появление сигнала нулевого уровня на его выходе и на вторых входах группы элементов И-НЕ 15 – 17 воспроизведения информации, на первом входе второго элемента И – НЕ 19 и на инверсном входе третьего элемента ИЛИ 22. При этом запрещается срабатывание группы элементов И - НЕ 15 – 17 воспроизведения информации, второго элемента И – НЕ 19 и появляется сигнал на выходе третьего элемента ИЛИ 22, запускающий распределитель 29.

Элемент задержки 9 дает на выходе нулевой сигнал, если на его входе всегда имеется единичный сигнал, и выключается при исчезновении с его входа единичного сигнала через интервал времени несколько больший, чем наибольший возможный интервал нулевого сигнала в любом сообщении, передаваемом в системе связи. Далее, поступающие с выхода амплитудного дискриминатора 5 импульсы через первый элемент ИЛИ 27подаются на первые входы группы элементов И – НЕ 23 – 26 приема информации и записываются в регистр 20 по мере поступления импульсов с выходов части группы элементов И –НЕ 25, 26 приема информации либо всей группы элементов И – НЕ 25 – 26 приема информации, которые возникают одновременно с появлением на выходах распределителя 29 тактовых импульсов. Для обеспечения правильной записи информации в соответствующие триггеры регистра 20 они устанавливаются в исходное состояние выходным сигналом одного из входящих в группу элементов И –НЕ 23 – 26 приема информации элемента И – НЕ 26.

Последовательность записываемых сигналов начинается с флага, представляющего из себя шесть единиц между двумя нулями. Далее следует, например, адрес получателя, адрес отправителя и собственно сообщение либо его фрагмент, если сообщение имеет большую длину. Сообщение заканчивается концевиком и вторым флагом. Если принятый адрес получателя совпадает с адресом данного абонента, то он с выхода регистра 20 вызывает появление единичного сигнала на выходе элемента И 28, что разрешает дальнейшую запись сообщения в регистр 20 данного абонента. В противном случае эта запись прекращается. После сеанса связи единичный сигнал на выходе элемента задержки 9 по окончании его выдержки времени восстанавливается, и система связи становится подготовленной к последующим сеансам связи.

Если канал связи свободен и время выдержки элемента задержки 9 истекло, то при появлении на выходе инициализации передачи сообщений регистра 20 единичного сигнала он подается на второй вход элемента И-НЕ 19 и через формирователь 8 – на вход записи счетчика 11. При этом информация о начальном приоритете сообщения переписывается из регистра 20 в счетчик 11. Вместе с этим сигнал с выхода второго элемента И-НЕ 19 включает дешифратор 12 и нулевой сигнал с одного из его выходов, поступая на соответствующий вход формирователя 13 импульсов приоритета, вызывает появление на его выходе импульса приоритета с длительностью, пропорциональной фиксированному значению кода приоритета данного сообщения. Этот импульс, складываясь с единичными импульсами флага, увеличивает длительность сформированной таким образом непрерывной последовательности сигнала, причем длительность импульсов приоритета может быть кратной или составлять часть от длительности импульсов устройства для многоабонентной одноканальной связи, что зависит от условий проведения связи. Импульс приоритета, поступая на вход второго элемента ИЛИ 7, инициирует передачу единичного сигнала в канал связи. Непосредственно после переднего фронта импульса приоритета следует шесть единиц сигнала флага. Переданная таким образом последовательность принимается всеми устройствами системы многоабонентной одноканальной связи согласно описанного случая передачи сообщения, приоритет сообщения которого был равен нулю, а канал связи был свободен.

Если формирователи импульсов приоритета двух или нескольких абонентов выдали свои сигналы одновременно, то абоненты, имеющие меньшие длительности импульсов приоритета, перейдут под воздействием сигнала абонента, имеющего большую длительность импульса

приоритета, из режима передачи в режим приема. Если же длительность обоих импульсов приоритета, сложенных с импульсами флага, совпадет, то эти абоненты продолжат работу в режиме передачи до тех пор, пока в передаваемой последовательности импульсов адреса получателя не окажется нуль у одного из абонентов и единица – у другого. При этом выключится абонент, передавший нулевой сигнал, но у него при выключении переключится в нулевое состояние RS-триггер 10, который ранее под воздействием импульсов с выхода первого элемента И-НЕ 18 был установлен в единичное состояние. При этом в счетчик 11 импульсов запишется дополнительно к начальному коду приоритета единица и приоритет данного сообщения возрастет. Если данный абонент окажется вновь выключенным, то приоритет его сообщения вновь возрастет, и будет увеличиваться до тех пор, пока сообщение не будет передано. Для повышения достоверности передачи адреса получателя его передают дважды, а с помощью концевика организуют контроль достоверности передачи сообщения.

Из описания принципа действия системы следует, что при наличии в сети достаточного числа абонентов, имеющих сообщения определенного объема, описанное устройство может обеспечить коэффициент использования канала связи, близкий к единице.

СПИСОК ЛИТЕРАТУРЫ:

1. Гордиенко, Е. Н. Оптические телекоммуникационные системы. Учебник для вузов / Н. Гордиенко. – М.: ГЛТ, 2011. – 368 с.
2. Крук Б. И. Телекоммуникационные системы и сети. Уч. пособие в 3-х томах / Б. И. Крук. – М.: ГЛТ, 2012.
3. Патент 2028733 РФ, МКИ6 Н 04 В 7/24. Устройство для многоабонентной одноканальной связи. / О. Д. Лобунец (РФ). – 6 с.: ил.

А.С. Петров, Е.В. Кислицын

ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ CRM - СИСТЕМ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: CRM - системы, система, клиент, интерфейс, проектирование, технологии, информация, функционал.

В статье представлены основополагающие принципы проектирования систем взаимоотношениями с клиентами. Были представлены различные технологии для построения функционала системы для определённых отраслей рынка, как отечественных, так и зарубежных. Приведена базовая последовательность процесса проектирования, для последующей правильности подготовки к внедрению в компании. Проведен обзор работ и литературы, содержащих описание процесса проектирования и разработки CRM-систем.

A.S. Petrov, E.V. Kislitsyn

CRM SYSTEM DESIGN PRINCIPLES

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: CRM systems, system, client, interface, design, technology, information, functionality.

The article presents the fundamental principles of designing customer relationship systems. Various technologies were presented to build the functionality of the system for certain sectors of the market, both domestic and foreign. The basic sequence of the design process is given, for the subsequent correct preparation for implementation in the company. A review of works and literature containing a description of the process of designing and developing CRM systems was carried out.

Возможности создать CRM - систему, есть у любого программиста, для этого ему достаточно компьютера и выхода в интернет. Важнее всего, чтобы сделанная система была надёжна и не обвалилась при первой ошибке. Именно для этого и нужно проектирование, ведь только имея чёткий план, можно рассчитывать на успешную реализацию конечного продукта.

Стереотипы о том, что разработать CRM - систему проще, чем, к примеру, ERP - систему, множество раз были опровергнуты на практике, но есть здесь и доля правды. CRM - систему, в некотором смысле, действительно проще сделать в плане масштабности программного обеспечения, но при проектировании может потребоваться большее количество поддержки специалистов финансовой, коммерческой, юридической, технологической, технической и экспертной сферы консалтинговых компаний.

При внедрении CRM - системы на предприятие, для начала, требуется определить спектр задач, которые должны выполнятся системой и выяснить, какие проблемы должны решатся. Не мало важно, сформулировать желаемые цели и конечный результат, ведь в последующем, именно эта информация и будет определять варианты использования CRM - системы. Обязательным этапом перед проектированием будет формирование команды, в который будет входить: руководство компании, консультанты проекта, специалисты технической поддержки, программисты, специалисты поддержки системы и системный администратор.

1. Предпроектное исследование

Первый этап традиционно необходим для оценки нужд организации и перспектив удовлетворить их при внедрении. Для такого нужно провести анализ и выяснить текущее состояние организации в области руководства взаимоотношениями с клиентами, определить проблемы и постичь как их решать. Лишь после такого, можно приступать к определению CRM - стратегии, которая будет двигаться в направлении совершенствования руководства.

Для любой организации создаётся оригинальная CRM-система, учитывающая индивидуальности процессов и системы организации. Проектирование CRM - систем осуществляется на базе типовых моделей жизненного цикла, но имеется ряд особенностей, особенно на начальных стадиях [3]. На рисунке 1 подробно представлена модель жизненного цикла CRM - системы.

Рисунок 1 – Модель жизненного цикла CRM-системы [3]

Сформированная CRM - стратегия не будет являться списком действий, которые готовы к срочному применению: ее нельзя купить или внедрить локально на отдельных участках бизнес-процессов. В ней должно быть всё, для эффективной организации работ с персоналом компании и клиентами.

2. Проектирование

На данном этапе наступает проектирование CRM - системы на внедряемом объекте. Ключевой ролью здесь будет являться описание требований к программе, которая обязана олицетворять функции и задачи, а также решать проблемы, которые были затронуты на прошлом этапе исследования.

Результатом этапа проектирования представляет собой техническое задание. Оно должно быть ясно как постановщику задания, так и программисту, и не обязано содержать неоднозначностей.

Техническое задание CRM - системы представляет собой документ, который идентифицирует требования к программе. Оно нужно в любом случае: создаёте вы новую систему, улучшаете сегодняшнюю или переходите на другую. В нём находится описание

требуемых настроек и изменений в программе, примеры экранных форм интерфейсов документов и отчетов, печатные формы отчетов или иной материал, который описывает, как станут реализованы требования к программе. Для аудитов итогов работы программы рекомендуем приготовить тестовые примеры (детальное описание сквозной типовой задачи).

Иными словами, без технического задания, у разработчиков был бы бесконечный механизм создания, ведь без точных рамок нельзя изложить целую картину. Да и число корректировок было бы гигантским количеством. С чётким планом того, что обязана представлять из себя система, результат обязан получится положительным.

По данным Software Advice (исследования и обзоры пользователей программных приложений для малого и среднего бизнеса), при разработке CRM обязательные функции — это управление контактами, отслеживание взаимодействия с клиентами и планирование. Остальные функции опциональны. На рисунке 2 представлены самые популярные функции CRM [4].

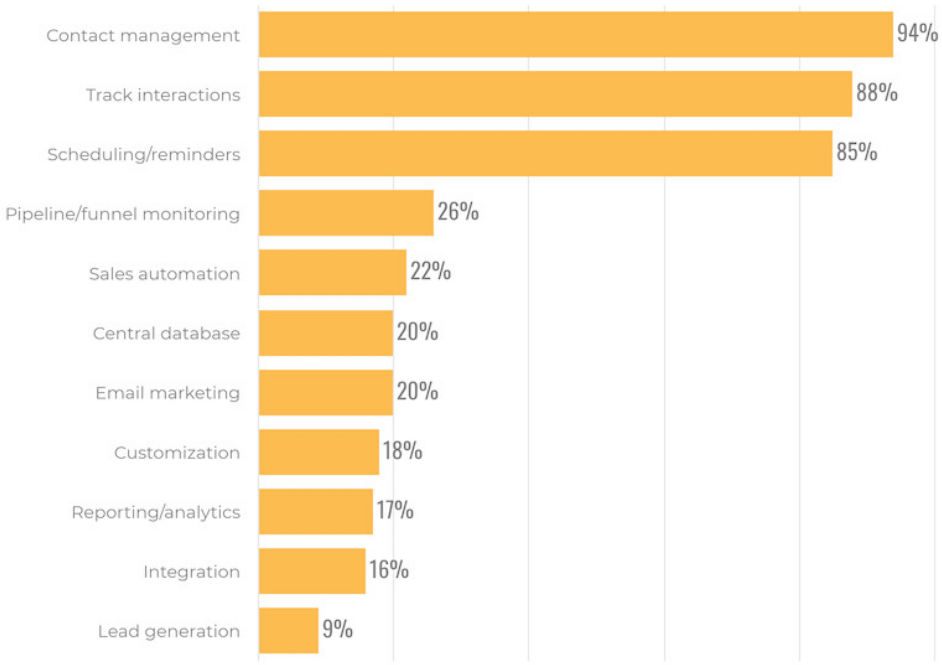


Рисунок 2 – Самые популярные функции CRM по данным Software Advice [4]

Каждая функция обязана быть в очень мелких деталях описана и понятными формулировками объяснена. Выбор функций CRM-системы находится в зависимости от тех задач, которые заказчик перед ней ставит. Не редко, на это выше всего оказывает влияние масштаб организации:

1) Частный бизнесмен. Традиционно одиночным пользователям необходима лишь База данных контрагентов для руководства и отслеживания связей с ними. Это значительно экономит время и нервы.

2) Малый коммерческий проект. Более крупным предпринимателям в большинстве инцидентов необходима Автоматизация отдела продаж вплоть до контроля и отслеживания поступков некоторых торговых представителей.

3) Средний коммерческий проект. Такие организации делают упор на автоматизацию продаж и маркетинга. Кроме того, им важна аналитика, которая позволяет планировать коммерческий проект-процессы и основать маркетинговые стратегии.

4) Крупный бизнес. Для больших корпораций важно все — от продаж до стратегии, поэтому они нуждаются в эффективных совместимых CRM-системах.

Автоматизация продаж представляет собой основой CRM-системы и обязана содержать следующие функции:

1) ведение календаря событий и разработка планов работы;

2) управление контактами (ни одно обращение потребителя не будет пропущено);

3) функционирование с клиентами (каждый клиент будет обслужен на очень высоком уровне благодаря зафиксированной истории нетворкинга с ним);

4) увеличение точности прогноза продаж;

5) предоставление информации о ценах;

6) машинальная подготовка хозяйственных предложений;

7) машинальное развитие отчетов по результатам работы;

8) организация продаж по телефону (формирование списка возможных контрагентов, машинальный спектр номеров, регистрация звонков, прием заказов) и ряд прочих вспомогательных функций.

Автоматизация обслуживания клиентов в последнее время приобретает первостепенное значение, так как в условиях жесткой конкуренции удержать прибыльного клиента можно прежде всего высоким качеством обслуживания [3]. Для быстрого, точнейшего и эффективного довольства индивидуальных нужд клиентов, необходимо гарантировать выполнение CRM-системой следующих структур:

1) анализ нужд клиента (работник отдела завсегда в курсе проблем и предпочтений каждого покупателя);

2) контроль проведения заявок (процесс контролируется механически);

3) контроль перепродаж (в любой момент времени можно присвоить информацию о свойстве выполненной оплаты, ее стоимости, неудовлетворённости клиентов, дедлайнах выполнения петиции и др.);

4) ведение авиабазы знаний;

5) надзор выполнения дилерских соглашений (дедлайны и условия следят автоматически);

6) ведение запросами покупателей с помощью присваивания приоритетов.

Кроме означенных можно обозначить общие подсистемы для этих двух правлений:

1) составление докладов для высшего командования;

2) интеграция с ERP-системами;

3) электронная коммерция (управление поставками с помощью систем электронной торговли типа B2B и B2C).

Нужно понимать, что не существует единых методологий и технологий строительства CRM-систем, применимых ко всем фирмам. Система ведения взаимоотношениями с покупателями должна возводиться на основе пиаровских целей и тактик. Только в этом случае CRM-система будет идти на повышение сверхприбыли компании в долгосрочной и надежной перспективе.

С мониторингом выбранной универсальности CRM-системы нельзя произвести реструктуризацию бизнес-процесса в сфере перепродаж, маркетинга и обеспечения клиентов, выстроив функциональную модификация «TO BE» для самой фирмы.

Впрочем, в последнее время, ряд экспертов утверждают, что такого плана формальная реструктуризация с целью подгонять бизнес-процесс под развертываемую в будущим CRM-систему может сделать работу компании неустойчивой. Поэтому в настоящий момент, как правила, рекомендуется сперва внедрить в фирму CRM-систему и только потом перестраивать, и улучшать бизнес-процесс самой фирмы, зафиксировав изменения в регулировках CRM-системы [1].

Заключение

Подводя итог, можно отметить, что принципы проектирования являются обязательным началом при построении любого CRM-проекта. Поскольку именно проектирование является незаменимым набором правил, от которого проще всего и правильнее будет начинать последующие этапы.

Конечный продукт проектирования, техническое задание, является основополагающим звеном всего построения CRM-системы. В последнее время все компании, использующие CRM-системы, как отечественные, так и зарубежные, проходили через описанные в статье этапы.

СПИСОК ЛИТЕРАТУРЫ:

1. ВОЛС.Эксперт. [Электронный ресурс]. URL: https://vols.expert/useful-information/obshhie-princzipy-proektirovaniya
2. 1C:CRM. [Электронный ресурс]. URL: https://1crm.ru/all/theory
3. StudRef. [Электронный ресурс]. URL: https://studref.com
4. MereHead. [Электронный ресурс]. URL: https://merehead.com/ru

С.М. Плеханов, И.В. Коробицын

СИСТЕМА ДИНАМИЧЕСКОЙ ЭВАКУАЦИИ ПРИ ПОЖАРЕ НА ОСНОВЕ IoT

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ) в г. Екатеринбурге (УрТИСИ СибГУТИ)

Ключевые слова: чекпоинт, пожар, эвакуация, алгоритм, IoT.

В статье приведен краткий анализ алгоритма по выявление маршрутов эвакуации и перестройка маршрута в случае обнаружение пожара на пути эвакуации.

S.M. Plekhanov, I.V. Korobitsyn

IoT-BASED DYNAMIC FIRE EVACUATION SYSTEM

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Key words: checkpoint, fire, evacuation, algorithm, IoT

The article provides a brief analysis of the algorithm for identifying evacuation routes and rebuilding the route in case of fire detection on the evacuation route.

На сегодняшний день подавляющее большинство систем эвакуации при пожаре представляет собой комплекс датчиков, которые при срабатывании активируют сигнализацию на посту охраны. Одна из таких систем представлена в литературе [1].

Такие системы могут нести за собой ряд значительных недостатков, таких как:

- не учтена позиция возникновения возгорания;
- отсутствие контроля количества эвакуирующихся людей в режиме реального времени;
- нет возможности динамической корректировки маршрута эвакуации.

Данные факторы могут привести к серьезным негативным последствиям при возникновении возгорания в зданиях.

В данной статье мы предложим концепцию системы динамической эвакуации при пожаре на основе систем Интернета вещей. Технологии IoT стремительно развивается в мире, в Российской Федерации, в частности. Применение «умных» устройств может дать необходимую гибкость при разработке системы эвакуации, как в плане выбора языка программирования для написания алгоритма, так и при подборе материальной базы.

Цель, поставленная перед проектом на данный момент: создать систему, которая на основе Интернета вещей, укажет наиболее правильный и быстрый путь эвакуации из здания при возникновении возгорания.

Комплекс задач, планируемый для реализации:

– разработать алгоритм принятия решения о нахождении кратчайшего пути;

– найти подходящую материальную базу для реализации;

– разработать код для микроконтроллеров, на основании материальной базы и выбранных протоколов связи, при этом обеспечить максимальную автономность работы;

– реализовать данную систему на основании макета.

Для демонстрации работы был взят план эвакуации здания, изображенного на рисунке 1.

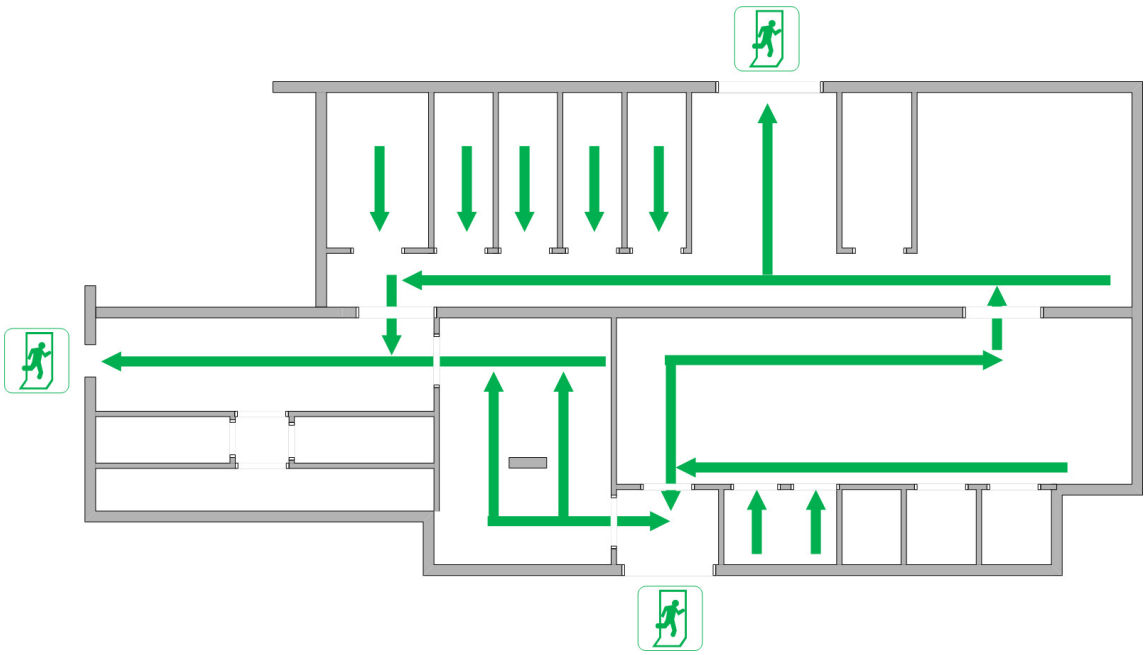


Рис. 1 – План эвакуации

Далее будет описана поэтапная работа системы эвакуации, предлагаемой в данной статье.

Этап 1: Расстановка контрольных точек:

Расстановка контрольных точек происходит в основных коридорах здания, следуя по основным направлениями для эвакуации, показанных на плане выше. Основная роль контрольных точек –путевые маркеры, которые содержат в себе ряд информации, для принятия решения о направлении к выходу. Также необходимо отметить выходы особым типом контрольных точек, так как они будут играть ключевую роль в работе алгоритма нахождения пути. В физическом исполнении контрольные точки будут представлять собой интерактивные указатели, которые будут показывать направление движения к наиболее безопасному выходу, в то же время, учитывая и длину маршрута до этого выхода.

Необходимой частью динамической системы эвакуации будет являться и пункт координации, который будет представлять собой сервер для обработки информации, поступающей с датчиков возгорания, принятие решения на основе данной информации и последующей отправки на контрольные точки.

Предполагается, что объем поступающих данных будет минимальным, что в свою очередь позволит, использовать в качестве сервера такие варианты как: одноплатный компьютер Raspberry PI или его аналоги.

Также стоит уделить особое внимание выбору протоколу связи, в [2] проблема энергопотребления ставиться одной из главных при работе систем IoT. В данном проекте планируется обеспечить контрольные точки беспроводным соединением, так как, нужно обеспечить максимальную живучесть системы при возгорании, а проводные соединения могут быть легко нарушены под воздействием экстремально высоких температур. Также стоит отметить, что не везде есть возможность подвести питание к контрольным точкам по проводу, поэтому предпочтение отдается аккумуляторам.

Но наиболее лучшим решением будет комбинированная система питания, в которой, аккумулятор будет присутствовать как запасной вариант, на случай выхода из строя основной линии.

Пример расстановки контрольных точек показан на рисунке 2.

Рис. 2 – Расстановка контрольных точек

Контрольные точки пути содержат в себе ряд информации:

– ID;
– метки пути;
– направление индикации.

ID – представляет собой идентификатор (номер) контрольной точки, который не должен повторяться с остальными точками. На основе данного номера, выстраивается для каждой точки эвакуационный маршрут.

Метки пути – их количество равняется количеству выходов и обозначает удаленность от того или иного из них. Например: метка пути «14» говорит о том, что данная контрольная точка находиться на удалении «4» от выхода «1», где «4» означает, что данная контрольная точка четвертая от выхода «1». Метки пути могут повторяться для контрольных точек с разным ID, например контрольные точки «12» и «16» находятся на удалении «4» от выхода «1».

Индикация – указывает направление наиболее верное для безопасной и быстрой эвакуации, служит для контроля системы со стороны человека.

Первоначальный расчет наиболее быстрого пути производиться заранее, далее происходит только его корректировка при возникновении возгорания.

Пример принятия решения о направлении эвакуации рассмотрен далее.

Выбор маршрута от контрольной точки с ID = 14:

Выбор маршрута основан на метках пути. В данном случае будет выбран путь до выхода «3» через контрольную точку с ID 15, так как, метка пути «32» говорит о том, что до выхода «3» осталось пройти 2 контрольные точки. Метка «14» говорит о том, что до выхода «1» осталось пройти 4 контрольные точки. Расчет до выхода «2» выполнятся по аналогии.

После выполнения расчета принимается решение о направлении индикации.

Также стоит рассмотреть сценарии корректировки маршрута при возникновении возгорания. Для визуализации процесса представлен рисунок 3.

Рис. 3 – Корректировка маршрута при возгорании

Корректировка маршрута с ID:14 при возгорании.

Допустим, что вблизи ID:15 произошло возгорание, тогда исходя из меток пути, будет выбран выход «1», так как он самый короткий, а сам маршрут будет пролегать через «чекпоинты» с ID: 13,16,17.

Принцип работы алгоритма представлен на рисунке 4. Алгоритм можно поделить на 3 части:

– первая часть. Запуск датчика пожарной сигнализации;

– вторая часть. Из запушенных датчиков составить общую карту помещения. Для каждого чекпоинта составить все возможные маршруты до эвакуационных выходов;

– третья часть. Запускается в случае обнаружение пожара. При обнаружение пожара, проверяется чекпоинт, на котором был зафиксирован пожар, и все остальные точки, выстраивают маршрут до ближайшего выхода, на котором не был зафиксирован пожар. В случае, если выходов несколько, и один из выходов перегружен, алгоритм выбирает в качестве пункта эвакуации, другой маршрут, чтобы разгрузить коридоры.

В литературе [3] представлен другой алгоритм работы системы обнаружения пожара. Данный алгоритм не берёт во внимание загруженность коридоров во время эвакуации людей, что может пагубно сказаться в будущем.

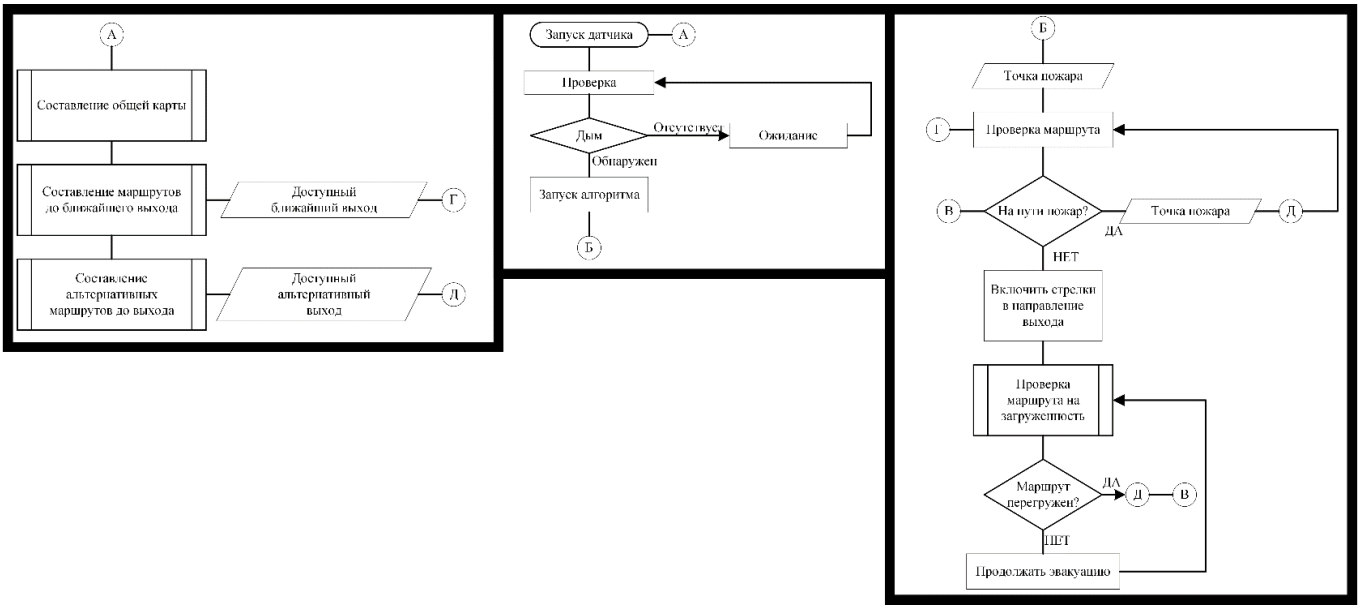


Рис. 4 – Блок-схема работы алгоритма

В заключение стоит отметить, что данная система пожарной эвакуации поможет избежать жертв при пожаре с помощью грамотного алгоритма эвакуации. При этом маршруты могут перестраиваться в случае перегрузки маршрута или непредвиденных обстоятельств, что позволит разгрузить поток людей, а также убедиться в том, что маршрут является безопасным.

СПИСОК ЛИТЕРАТУРЫ:

1. Fire Safety and Alert System Using Arduino Sensors with IoT Integration [Электронный ресурс] Режим доступа URL: https://dl.acm.org/doi/10.1145/3185089.3185121, свободный – Загл. с экрана. Дата обращения: 13.04.2023
2. Enhancing Energy Consumption in IoT [Электронный ресурс] Режим доступа URL: https://dl.acm.org/doi/10.1145/3436829.3436832 , свободный. – Загл. с экрана. Дата обращения: 07.04.2023.
3. Design of the building automatic fire alarm and fire -fighting system based on PLC [Электронный ресурс] Режим доступа URL: https://dl.acm.org/doi/10.1145/3436286.3436504, свободный. – Загл. с экрана. Дата обращения: 13.04.2023.

К.В. Свалухин, Д.И. Бурумбаев, И.И. Шестаков

ИММИТАЦИОННОЕ МОДЕЛИРОВАНИЕ КАК СРЕДСТВО ОПТИМИЗАЦИИ РАБОТЫ ПРЕДПРИЯТИЯ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: системы массового обслуживания, имитационные модели, инфокоммуникационные технологии, AnyLogic.

В статье представлено и проведено компьютерное моделирование систем массового обслуживания на базе модели банковского офиса, содержащее описание результатов исследований, а также их сравнительный анализ. Произведено исследование параметров системы массового обслуживания. Планирование выполнено на базе программного обеспечения AnyLogic.

K.V. Svalukhin, D.I. Burumbaev, I.I. Shestakov

SIMULATION MODELING AS A MEANS OF OPTIMIZING THE WORK OF THE ENTERPRISE

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: queuing systems, simulation models, infocommunication technologies, AnyLogic.

The article presents and conducts computer modeling of queuing systems based on a bank office model, containing a description of the research results, as well as their comparative analysis. The parameters of the queuing system were investigated. The planning is carried out on the basis of AnyLogic software.

Современная технология освоения методов самостоятельного построения имитационных моделей систем массового обслуживания на примере коммутационных устройств прогрессивно развивается, и то, что раньше делалось вручную, в настоящее время максимально автоматизировано и возможно при помощи программного обеспечения и персонального компьютера. Существует огромное количество программного обеспечения, которое направлено на создание имитационных моделей. Моделирование различных процессов позволяет предоставить, предугадать и запланировать поведение той или иной системы информационно-коммуникационных технологий [1].

Система массового обслуживания (СМО) — система, предназначенная для многократно повторяющегося (многоразового) использования при решении однотипных задач [1].

Под ИКТ системой подразумеваются технологии, предназначенные для совместной реализации информационных и коммуникационных процессов.

В качестве примера было рассмотрено моделирование банковской сети в программном обеспечении Anylogic.

AnyLogic — ведущий инструмент имитационного моделирования для бизнеса. Используется по всему миру в логистике, производстве, нефтегазовой отрасли, и других отраслях. Моделирование для обоснованных решений. AnyLogic — лидирующий инструмент имитационного моделирования для бизнеса. Он помогает аналитикам, инженерам и руководителям из разных отраслей получать детальное представление о бизнес-системах и процессах и оптимизировать их [2].

Постановка задачи. В банковский офис обращаются клиенты. Офис представляет собой автоматизированный пункт обслуживания, в котором установлен банкомат. Банкомат обслуживает одновременно одного клиента. Клиенты прибывают с интенсивностью = 0.8. Одновременно в офисе может находится не более 20 клиентов. Интервал времени работы банкомата подчиняется треугольному закону распределения с параметрами xmin=0.6, xmax=1.5 предпочтительное значение 3.9. Отделение банка представляет собой систему массового обслуживания (СМО), создается простейшая модель, в которой рассматривается массовое обслуживание клиентов банкоматом. После создания модели в ней уже находится один агент – Main, и один эксперимент – Simulation. Агенты являются главными строительными блоками модели в среде AnyLogic. В данном случае, агент Main служит местом, где задается вся логика модели: здесь расположится чертеж банковского отделения и задастся диаграмма процесса потока клиентов.

Рис.1 Имитация элементов банковского отделения

Характеристика используемых элементов представлена ниже:

Объект «Вход» генерирует заявки определенного типа. В статье в качестве заявок будут посетители банка, а объект вход будет моделировать их приход в банковское отделение.

Объект «Очередь» моделирует очередь заявок, ожидающих приема, следовательно моделироваться очередь клиентов, ждущих освобождения банкомата. Поступающие агенты помещаются в очередь в определенном порядке: либо согласно правилу FIFO, LIFO, либо согласно приоритетам. Очередь с приоритетами всегда примет нового входящего агента, вычислит его приоритет и поместит его в очередь в позицию, соответствующую его приоритету. Если очередь будет заполнена, то приход нового агента вынудит последнего хранящегося в очереди агента покинуть объект через порт outPreempted (верхний левый). В режиме таймаута агент покинет очередь через порт outTimeout (верхний правый), если проведет в очереди заданное количество времени.

Объект «Банкомат» задерживает заявки на заданный период времени, представляя в нашей модели банкомат, у которого посетитель банковского отделения тратит свое время на проведение необходимых ему операций.

Объект «Выход» ликвидирует поступившие заявки. Обычно он используется в качестве конечной точки потока заявок (и диаграммы процесса соответственно).

Чтобы изменить свойства определенного элемента, необходимо выделить его в графическом редакторе или в панели Проекты. Свойства элемента отразятся на панели свойства справа от графического редактора.

Настройка интенсивности прибытия людей к банкомату. К примеру, известно, что за 10 минут к банкомату в среднем подходит 8 человек.

Для этого выделяется блок «Вход», и в поле «Интенсивность» прибытия указывается число 0.8 человек в минуту.

Также выделяется, что вместительность зала ожидания у банкомата ограничена 20 местами. Изменим свойство вместимость блока вход, задав ему значение 20.

Настройка времени обслуживания заявки (людей) банкоматом. Принято, что минимальное время нахождения у банкомата равно 0.6, наиболее вероятное – 1.5, а максимальное – 3.8 минуты. Для моделирования случайных процессов используются вероятностные распределения. AnyLogic поддерживает большое количество разных вероятностных распределений. Чтобы получить случайное значение, сгенерированное согласно закону вероятностного распределения, нужно вызвать соответствующий метод. В данном случае воспользуемся треугольным законом распределения (Симпсона). В поле время задержки блока банкомат зададим следующий метод: triangular (0.6, 1.5, 3.8).

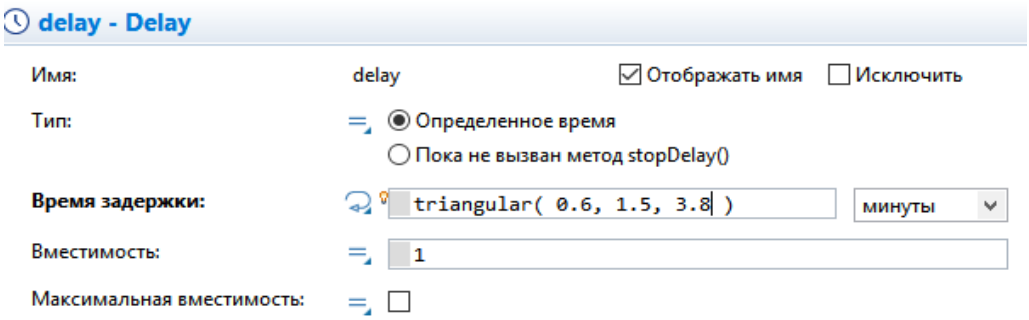


Рис. 2 Свойства блока delay

На данном этапе при выполнении эксперимента может возникнуть ошибка. Она связана с тем, что очередь переполняется и вновь поступающая заявка не может туда войти (так как настроена вместимость очереди – 20). Для решения данной проблемы создадним модель двухканальной СМО, так же создадим выход без обслуживания, если ожидание клиента составляет более 10 минут. Добавляется в модель банковского отделения зал обслуживания, в котором посетителей будут обслуживать операторы. В банковский офис приходят клиенты. Клиент может снять деньги в банкомате, либо получить консультацию у работников банка. Первый канал – очередь клиентов к банкомату, а второй канал – очередь к консультантам.

Для моделирования данного процесса можно также использовать элемент Банкомат. Но сложность заключается в том, что в этой части модели появляются ресурсы. Когда процесс обслуживания осуществляется неким автоматическим устройством, то логичнее использовать узел обслуживания (Банкомат). Но при необходимости привлечь к обслуживанию дополнительные ресурсы (сотрудники, инструменты, ограниченные помещение и т.д.) необходимо использовать так называемый бассейн ресурсов (Resource pool) в совокупности с сервисным узлом (Service).

Объект Service захватывает для агента заданное количество ресурсов, задерживает их, а затем освобождает захваченные им ресурсы. Эквивалентен последовательности объектов Seize, Delay, Release и должен использоваться в тех случаях, когда все, что требуется – это задержать захваченные ресурсы на заданное время, а затем их отпустить.

Объект SelectOutput направляет входящих агентов в один из двух выходных портов в зависимости от выполнения заданного (детерминистического или заданного с помощью вероятностей) условия. Условие может зависеть как от агента, так и от каких-то внешних факторов. Поступивший агент покидает объект SelectOutput в тот же момент времени.

Объект ResourcePool задает набор ресурсов, которые могут захватываться и освобождаться агентами с помощью объектов Seize, Release, Assembler и Service. Ресурсы могут быть трех типов: движущийся, статический и переносной. Статические ресурсы привязаны к определенному местоположению (например, узлу) внутри сети и не могут быть перемещаться или быть перемещены. Примером статического ресурса может быть учебный кабинет или суперкомпьютер во весь зал. Движущиеся ресурсы могут перемещаться сами по себе, они могут представлять персонал, транспорт, и т.д. Переносные ресурсы могут быть перемещены агентами или движущимися ресурсами, например флешка или микроскоп. Любой ресурс может быть либо свободен, либо занят. Объект собирает статистику занятости ресурсов.

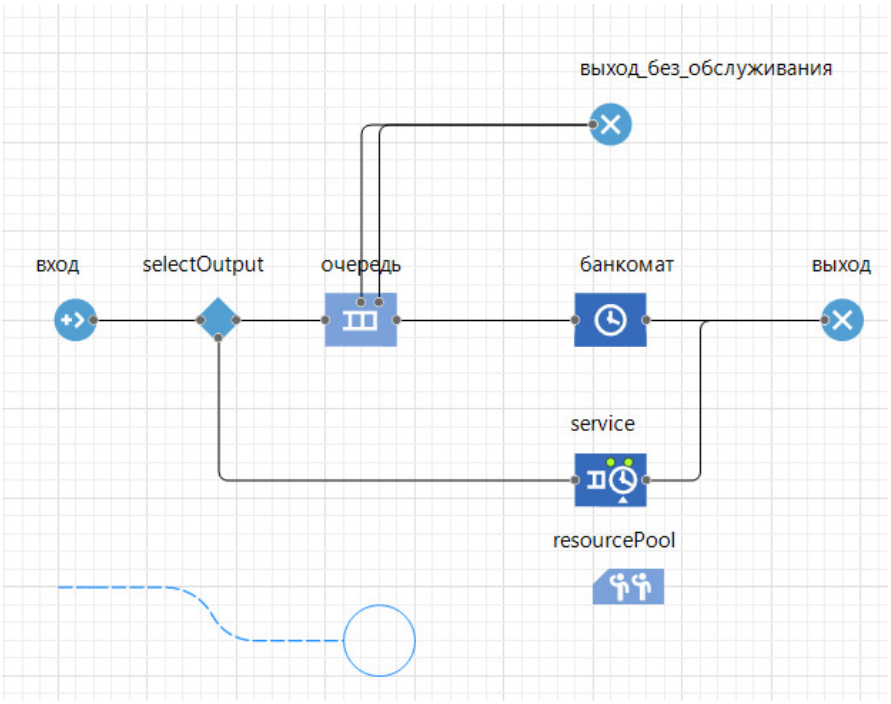


Рис. 3 Усовершенствованная логика модели

Исследование параметров СМО. Определятся следующие понятия: распределение времени ожидания обслуживания клиентом в системе и распределение времени, проведенного клиентом в системе. AnyLogic предоставляет пользователю удобные средства для сбора статистики по работе блоков диаграммы процесса. Наша задача создать две столбиковые диаграммы. Данная диаграмма будет отображать среднее время использования банкомата. Заголовок – среднее время использования банкомата.

У каждого объекта банкомат есть встроенный набор данных statsUtilization, занимающийся сбором статистики использования этого объекта. Функция mean() возвращает среднее из всех измеренных этим набором данных значений. Можно использовать и другие методы сбора статистики, такие, как min() или max().

Аналогичным образом добавим еще одну столбиковую диаграмму. Добавим на вторую диаграмму данные, с заголовком – среднее время в очереди к банкомату и значением – очередь statsSize.mean().

Рис. 4 Столбиковые диаграммы

Для сбора подробной статистики так же требуется запоминать время прибытия в банк и время начала ожидания в очереди к менеджерам, так же время появления клиента в системе и время начала ожидания обслуживания. Выбранное программное обеспечение будет рассчитывать все параметры, а также разницу между параметрами благодаря своей гибкой настройке и работе.

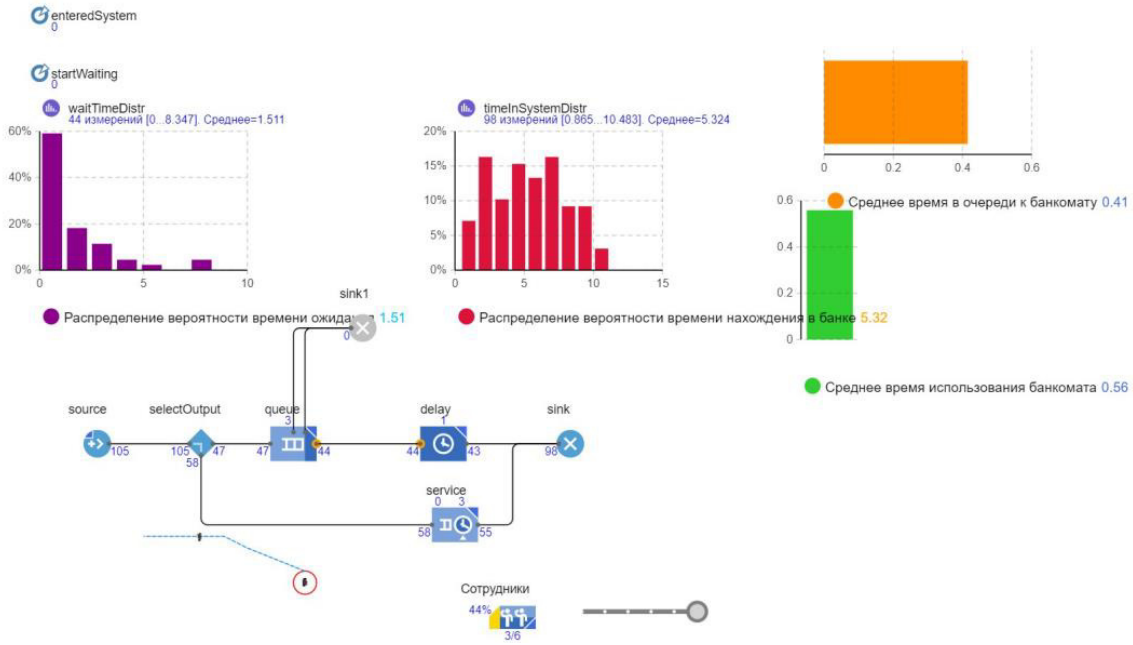


Рис.5 Модель банковского офиса при выполнении задач и приближенной к реалиям работы

Данная модель была выстроена по представленным в статье параметрам, протестирована и практически приближена к реальной работе банка.

Таким образом имитационное моделирование позволяет оптимизировать логистические процессы и режимы работы предприятий.

Список литературы:

1. Березин Д.А. Имитационное моделирование. Учебное пособие, Екатеринбург 2008. – 94 с.
2. Официальный сайт «The AnyLogic Company» [Электронный ресурс] – Режим доступа: https://www.anylogic.ru/

А.А. Сергеев, М.В. Малый, Е.В. Стойчина

Научный руководитель: директор учебно-научного центра «Информационная безопасность», доктор технических наук, профессор Поршнев С.В.

РАЗРАБОТКА И ПРИМЕНЕНИЕ КОРПОРАТИВНОЙ СИСТЕМЫ WEB-ФИЛЬТРАЦИИ

Уральский федеральный университет, Институт радиоэлектроники и информационных технологий-РТФ в г. Екатеринбурге, Россия

Ключевые слова: Персональные данные, сетевой трафик, система защиты информации, локальная сеть, межсетевое экранирование.

Корпоративная система web-фильтрации - это программное обеспечение, которое используется компаниями для ограничения доступа к определенным сайтам и веб-приложениям внутри организации. Это позволяет улучшить безопасность сети, предотвратить утечки конфиденциальной информации и увеличить производительность сотрудников.

Применение корпоративной системы web-фильтрации может иметь множество преимуществ для компании. Она может помочь улучшить безопасность сети, предотвратить утечки конфиденциальной информации и снизить риск заражения вредоносным программным обеспечением. Кроме того, она может увеличить производительность сотрудников, предотвращая доступ к ненужным сайтам и приложениям во время рабочего времени.

A.A. Sergeev, M.V. Maly, E.V. Stoichina

Scientific supervisor: Director of the educational and Scientific center "Information Security", Doctor of Technical Sciences, Professor S.V. Porshnev

DEVELOPMENT AND APPLICATION OF CORPORATE WEB FILTERING SYSTEM

Ural Federal University, Institute of Radio Electronics and Information Technologies-RTF in Yekaterinburg, Russia

Keywords. Personal data, network traffic, information security system, local area network, firewall.

A corporate web filtering system is software that is used by companies to restrict access to certain websites and web applications within an organization. This allows you to improve network security, prevent leaks of confidential information and increase employee productivity.

The use of a corporate web filtering system can have many advantages for a company. It can help improve network security, prevent leaks of confidential information and reduce the risk of infection with malicious software. In addition, it can increase employee productivity by preventing access to unnecessary websites and applications during working hours.

Работа в глобальной сети «Интернет» в большинстве своем представляет из себя процедуру, при которой пользователь с помощью клиента выполняет запросы к серверу, чтобы получить в результате какие-то данные, например, музыкальные и видеофайлы, а также отправить или получить электронную почту.

Но существует и обратная сторона, несмотря на большое количество положительных моментов, которые пришли в жизнь общества с появлением сети Интернет.

Но рост популярности сети «Интернет» и сервисов данной сети становится объектом внимания правонарушителей и преступников, которые стараются реализовать различные угрозы для пользовательских данных, а также режимов работы пользовательского и сетевого

оборудования. Сегодня число атак и угроз, которые нарушители реализуют, отличаются многообразием и изобилием инструментов, при помощи которых возможна их реализация.

В рамках настоящего исследования будет разработана система WEB-фильтрации пользователей, выходящих в сеть «Интернет» из локальной сети предприятия.

На данном этапе необходимо поставить задачу на текущую разработку.

В рамках реализации задачи руководством компании А поставлена цель – создание системы WEB-фильтрации из локальной сети

Созданная система WEB-фильтрации должна отвечать установленным требованиям, а именно:

Иметь удобный пользовательский интерфейс для администратора;

Иметь возможность выполнять фильтрацию по IP-адресу;

Иметь исходный открытый код и быть установленной на вычислительную машину, входящую в состав организации.

Для этого руководством предприятия предложено построить такую схему, которая показана на Рисунке 1.1.

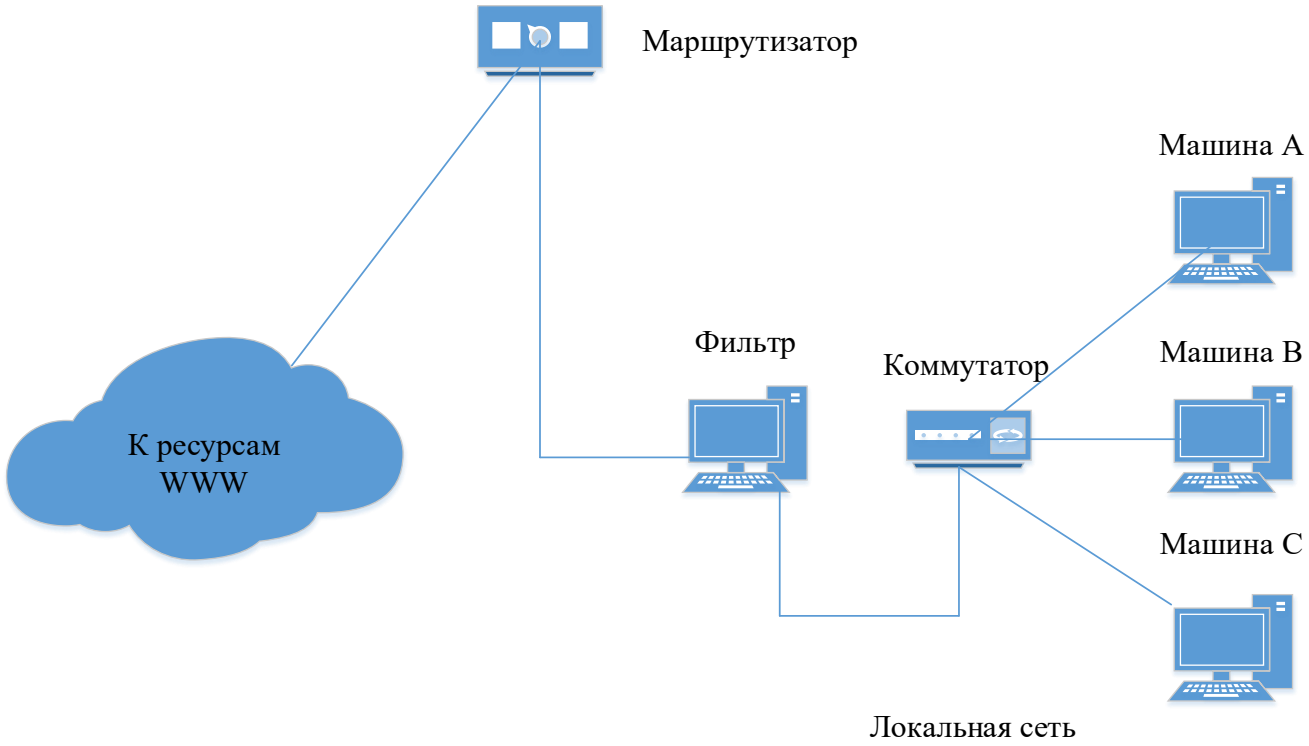


Рисунок 1.1 - Структура локальной сети и фильтр в ней

В рамках этого фильтра, который изображен на Рисунке 1.1, будет устанавливаться программный комплекс WEB-фильтрации, разработанный в рамках настоящего исследования.

Функционал данного программного обеспечения и требования к вычислительной машине, на базе которой будет происходить установка должны быть следующими:

- во-первых, программное обеспечение устанавливается на вычислительную машину, у которой будет 2 сетевые карты, соединенные в режиме «мост»;
- во-вторых, трафик, который идет по этому мосту, будет «слушать» разработанное программное обеспечение – это означает, что весь трафик будет проходить через данное программное обеспечение и в части, касающейся анализироваться им;
- в-третьих, к данному трафику будут применены правила, которые будут содержаться в одной из таблиц разработанного программного обеспечения;
- в-четвертых, за счет этого будет происходить WEB-фильтрация трафика, которая исходит от всех имеющихся в сети персональных оконечных абонентских устройств – компьютеров и администратор сети будет решать, какому пользователю, работающему за

компьютером и какие привилегии по доступу к ресурсам сети «Интернет» предоставить. IP-адрес же будет присвоен машинам в жестком статическом формате, в рамках настоящего исследования данное требование определено Заказчиком исходя из того, что сеть является малой и это наилучший вариант, когда исключена путаница и все будет работать хотя и статически, но без ошибок и сбоев.

На данном этапе необходимо описать процедуру физического проектирования фильтра. Необходимо помнить, что для запуска возможно потребуется переопределить значение константы HOSTS внутри файла myfw\fw\views.py. Кроме того, приложение необходимо запускать под правами администратора.

Нужно также помнить о том, что необходимо делать процедуру логаута, то есть выхода из приложения по соответствующей кнопке, иначе придется вручную править файл HOSTS, это особенности операционной системы.

Основная идея разрабатываемого приложения «Файрволл» заключается в следующем – путем модификации системного файла hosts, который располагается по следующему пути: [папка Windows]\System32\drivers\etc\hosts). Если говорить конкретнее, это добавление в конец файла строк вида ‘127.0.0.1 имя домена’. Благодаря этому происходит перенаправление пользователя на указанный IP адрес 127.0.0.1 при обращении по указанному имени хоста.

Принцип действия описан в заголовке файла hosts операционной системы Windows, который содержит следующую информацию: «Это пример файла HOSTS, используемого Microsoft TCP/IP для Windows. Этот файл содержит сопоставления IP-адресов с именами хостов. Каждая запись должна быть сохранена на отдельной строке. IP-адрес должен помещается в первый столбец, за которым следует соответствующее имя хоста. IP-адрес и имя хоста должны быть разделены хотя бы одним пробелом. Например:102.54.94.97 rhino.acme.com».

Так как в процессе модифицируются файлы, расположенные в системных папках, то для запуска приложения необходимы права администратора. Например, можно запустить программу через системную консоль cmd.exe открыв её с правами администратора.

Данная иллюстрация приведена на Рисунке 2.2.

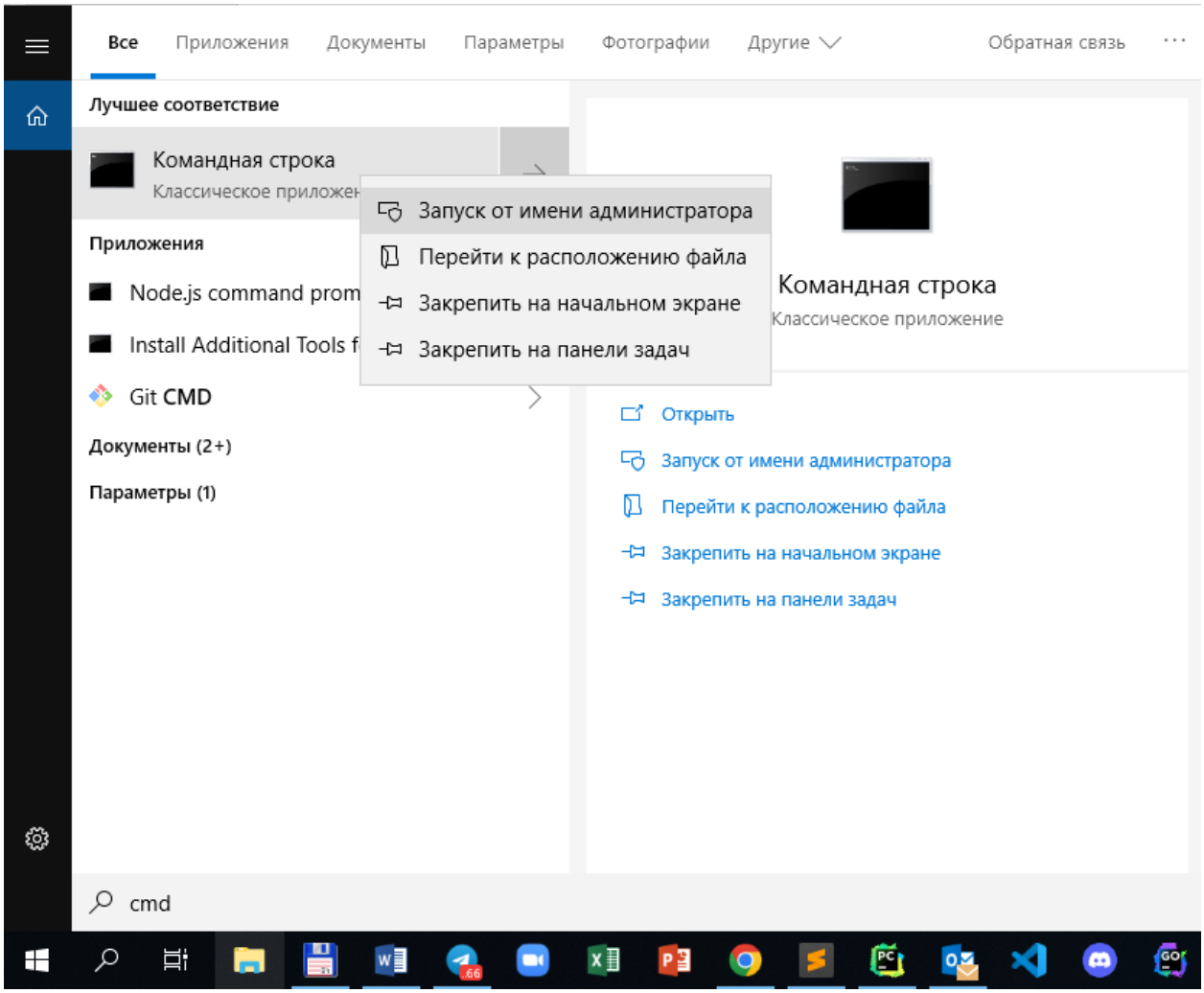


Рисунок 2.2 – Запуск в режиме администратора

Для работы программы также должны быть заранее настроены записи в соответствующих таблицах базы данных. Проще всего это сделать, запустив приложение командой python manage.py runserver которую нужно ввести в папке приложения. Это приведено на Рисунке 2.3.

```
C:\Code\myfw>python manage.py runserver
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).
June 13, 2022 - 18:30:34
Django version 4.0.3, using settings 'myfw.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

Рисунок 2.3 – Настройка соответствующих таблиц баз данных

Начальная страница приложения Fw открывается по адресу: http://127.0.0.1:8000/fw/.

Панель администратора расположена по адресу: http://127.0.0.1:8000/admin/, она приведена на Рисунке 2.4.

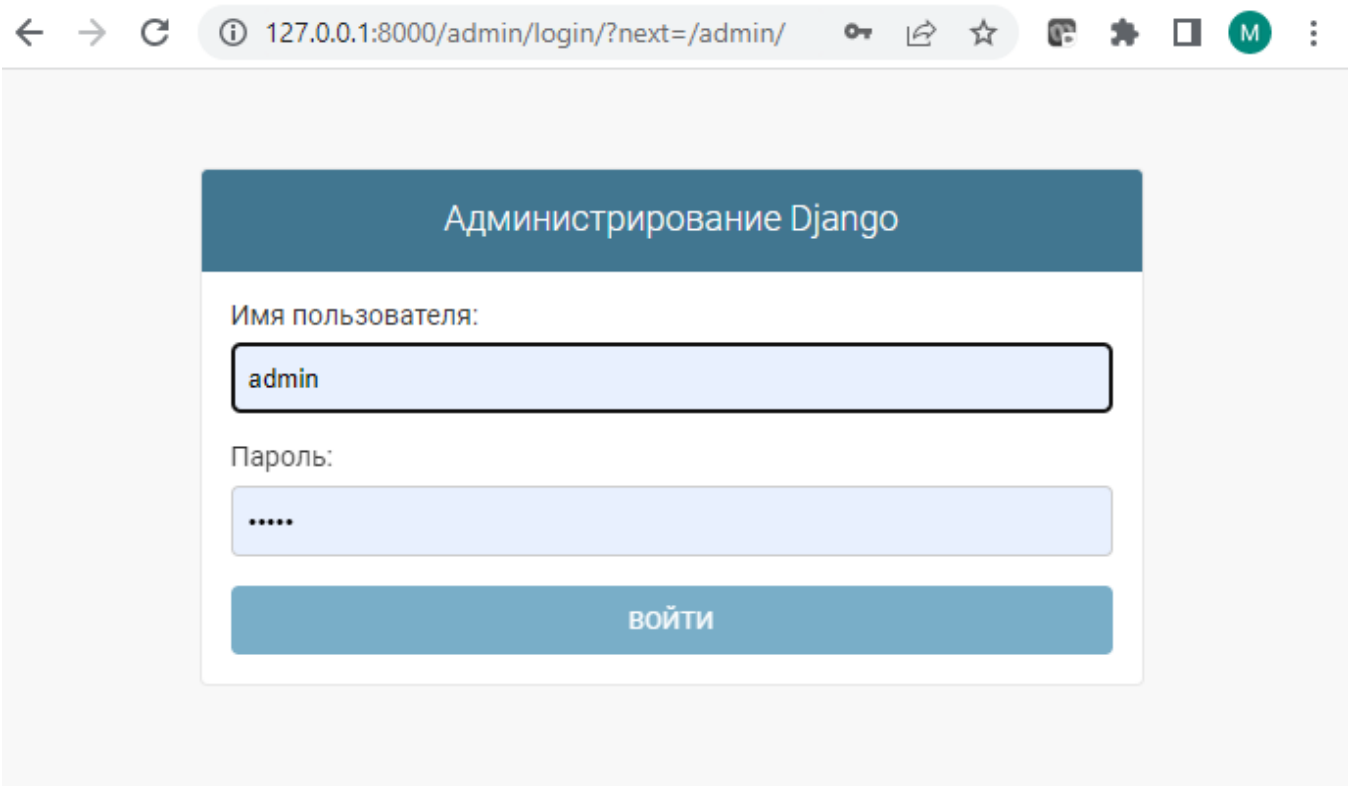


Рисунок 2.4 – Панель администратора

По умолчанию задано имя пользователя admin и пароль admin. После входа пользователь попадает в основное окно административного приложения, где он получает доступ к редактированию записей трёх таблиц приложения, которые приведены на Рисунке 2.5.

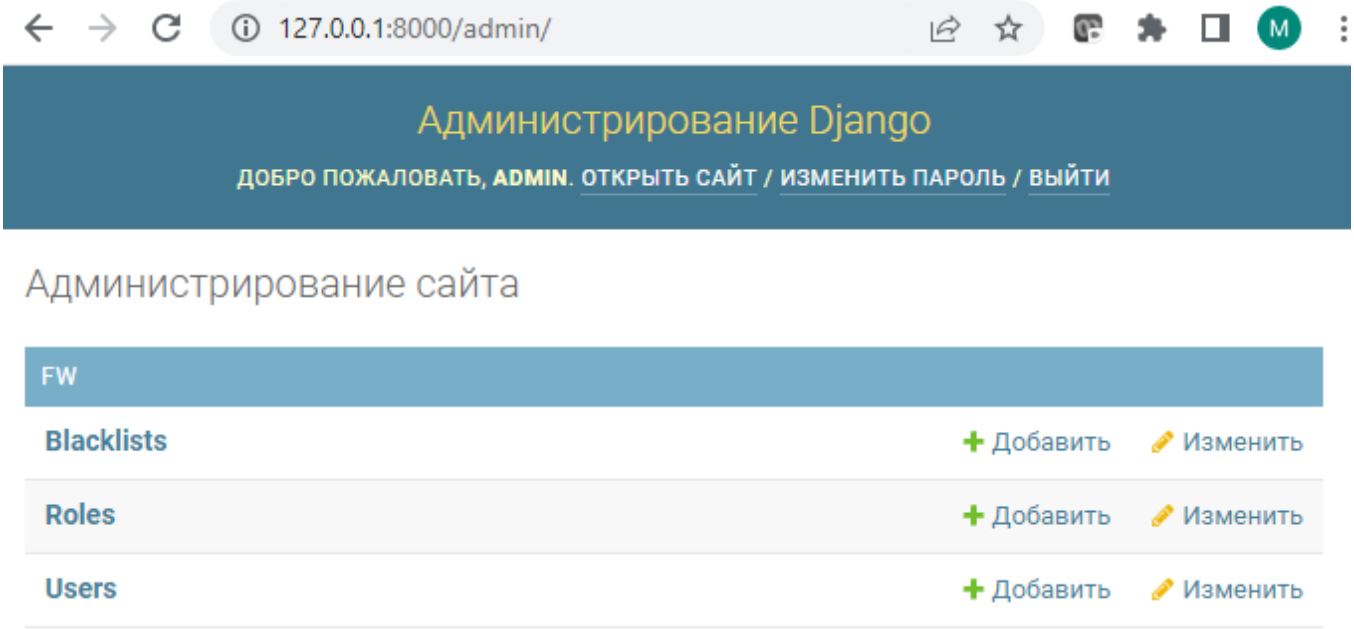


Рисунок 2.5 – Основное окно административного приложения

Назначение таблиц описано ниже:

- Users – содержит список пользователей с указанием роли (отношение один-ко-многим)
- Roles – содержит список ролей пользователей которые ссылаются на записи из таблицы blacklist, содержащие имена хостов (DNS-имена) к которым запрещен доступ пользователю соответствующей роли (отношение многие-ко-многим)
- Blacklist – содержит список блокируемых доменных имен.

В базе данных созданы записи о трёх пользователях:

- Иванов
- Петров
- Сидоров

Три роли:
- administrator
- manager
- user

И шесть записей о блокируемых доменах:
- e1.ru
- ekb.rbc.ru
- rbc.ru
- yandex.ru
- google.com
- none – специальная запись которая используется для обозначения что пользователю с ролью administrator разрешен доступ ко всем доменам.

Основная логика приложения реализована в файле Views.py в частности, определены функции вызываемые при старте приложения – index(). При входе пользователя – login() и выходе – logout(). Служебные функции login_proceed(), blacklist_proceed() и logout_proceed() вызываются при успешном входе и выходе приложения – они осуществляют манипуляции с файлом host – сохраняя его бэкап-версию (файл backup_hosts будет помещен в папку приложения), добавляя новые строки в файл и восстанавливая оригинальный файл из бэкапа.

ЗАКЛЮЧЕНИЕ

В рамках настоящего исследования была разработана система WEB-фильтрации пользователей, выходящих в сеть «Интернет» из локальной сети предприятия.

При выполнении разработки был поставлен ряд задач, среди которых: Приведение теоретических сведений и описание предметной области;
- Постановка задачи на проектирование;
- Проведение обоснования проектных решений по видам обеспечения;
- Описание технического обеспечения, информационного обеспечения, а также программного обеспечения;
- Разработка функциональной модели;
- Инфологическое и физическое проектирование;
- Разработка руководства пользователя;
- Рассмотрение вопросов экономической эффективности и смежных вопросов/

В рамках настоящего исследования все поставленные задачи выполнены, а цель достигнута. Разработанная программа может иметь практическое применение на базе корпоративных локальных сетей малых предприятий.

Список литературы:

1. Тидвелл Д. Разработка пользовательских интерфейсов. – СПб: Питер, 2018. – 416с.
2. Дюбуа П. MySQL, 3-е издание. — М.: «Вильямс», 2016. — 1168 с.
3. Дейт К. Введение в системы базы данных, 8–е издание К. Дейт: пер. с англ. – М.: Издательский дом «Вильямс», 2015. – 1328 с.
4. Буч Г., Якобсон А. UML Г.Буч. - СПб.:Питер, 2005.-736 с.
5. Холмогоров В. Основы WEB-мастерства. Учебный курс. 2-е изд. – СПб: Питер, 2020. – 320 с.
6. Справочное руководство по Python. [Электронный ресурс]. URL: http://www.mysql.ru/docs/man/Features.html (дата обращения: 20.05.2022)
7. Каминский В.Н. Язык JavaScript: лабораторный практикум - БГТУ «ВОЕНМЕХ». – СПб, 2018. - 58 с.
8. Купер А. Программирование на языках высокого уровня. СПб: Символ-Плюс, 2015. 336 с.
9. Петров В. Н. Информационные системы — СПб.: Питер, 2018. — 688 с.
10. Соколов С. А. JavaScript в примерах, типовых решениях и задачах. Профессиональная работа. М.: Издательский дом «Вильямс», 2021. – 592 с.

11. Дунаев В. В. HTML, скрипты и стили. – СПб: БХВ – Петербург, 2016. – 832 с.
12. Смирнов Н. В. Проектирование информационных систем: пособие по курсовому проектированию; Балт. гос. техн. ун-т. – СПб., 2019. – 61 с.
13. Колисниченко Д.Н. PHP и MySQL. Разработка Web-приложений. — СПб.: БХВ-Петербург, 2019. — 560 с.
14. Хокинс С. Администрирование Web-сервера Apache и руководство по электронной коммерции. - М.: Вильямс, 2021. -336 с.
15. В. В. Дригалкин. HTML в примерах. Как создать свой Web-сайт. Самоучитель. – М.: Диалектика, 2020. – 192 с.

К.Л. Стойчин, Е.В. Стойчина, М.В. Михайленко

Научный руководитель: директор учебно-научного центра «Информационная безопасность», доктор технических наук, профессор Поршнев С.В.

АЛГОРИТМ АНАЛИЗА КЛАВИАТУРНОГО ПОЧЕРКА В ПРОЦЕССЕ АУТЕНТИФИКАЦИИ В КОРПОРАТИВНОЙ СЕТИ

Уральский федеральный университет, Институт радиоэлектроники и информационных технологий-РТФ в г. Екатеринбурге, Россия

Ключевые слова: Информационная безопасность, аутентификация, системный анализ, алгоритм.

Анализ клавиатурного почерка является методом биометрической аутентификации, основанным на изучении индивидуальных особенностей ввода текста пользователя. Данное исследование указывают, что использование анализа клавиатурного почерка может быть полезно для автоматизации процесса аутентификации в корпоративной сети, особенно в случае, когда другие методы аутентификации не могут быть использованы (например, из-за отсутствия дополнительных устройств).

K.L. Stoichin, E.V. Stoichina, M.V. Mikhailenko

Supervisor: Director of the Educational and Scientific center "Information Security", Doctor of Technical Sciences, Professor S.V. Porshnev

AN ALGORITHM FOR ANALYZING KEYBOARD HANDWRITING DURING AUTHENTICATION IN A CORPORATE NETWORK

Ural Federal University, Institute of Radio Electronics and Information Technologies-RTF in Yekaterinburg, Russia

Keywords: Information security, authentication, system analysis, algorithm.

Keyboard handwriting analysis is a biometric authentication method based on the study of the individual characteristics of the user's text input. This study indicates that the use of keyboard handwriting analysis can be useful for automating the authentication process in a corporate network, especially when other authentication methods cannot be used (for example, due to the lack of additional devices).

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Современные компьютерные технологии существенно расширили возможности обмена различной информацией и в информационно-телекоммуникационных сетях промышленного назначения (ИТКС ПН). Аутентификация играет критически важную роль в защищенной информационной системе различных уровней, поскольку после ее прохождение пользователем все последующие решения, влияющие на безопасность, принимаются на основании достоверности предоставленных пользователем регистрационных данных. Эти данные подвержены угрозам хищения или нарушения целостности со стороны злоумышленника для

различных целей. Чтобы реализовать тот или иной тип угрозы, злоумышленник применяет один или несколько видов атак, в зависимости от степени защищенности данных или объекта.

Поэтому задача обеспечения защищенности процесса аутентификации в целях подтверждения подлинности пользователей в условиях повсеместного развития и внедрения новых ИТКС ПН является актуальной.

В настоящее время приобретают все большую популярность системы биометрической аутентификации, основанные на поведенческих признаках (использующих поведенческие метрики), в которых главный фокус сосредоточен на изучении поведения пользователя во время его взаимодействия с вычислительной системой с целью аутентификации. Частным случаем поведенческих признаков пользователей является биометрическая динамика работы с клавиатурой персонального компьютера, или клавиатурный почерк.

Биометрическое распознавание динамики работы с клавиатурой персонального компьютера включает в себя выявление поведенческих признаков, связанных с действиями пользователя, их анализ для извлечения сигнатур, которые являются уникальными для каждого пользователя. Главным преимуществом технологии аутентификации на основе анализа биометрической динамики работы с клавиатурой персонального компьютера при формировании графического изображения является способность непрерывного контроля разрешенных и запрещенных пользователей (непрерывная аутентификация). Для выполнения задач непрерывной аутентификации видится целесообразным применение научно-методического аппарата нейронных сетей и теории прогнозирования. Ключевой проблемой в непрерывной аутентификации является процесс сбора данных, который требует больше времени для формирования достаточного количества действий пользователя с клавиатурой персонального компьютера для точной аутентификации пользователя.

Объектом исследования в работе является система аутентификации пользователей компьютерных систем промышленного назначения.

Предметом исследования является способы и алгоритмы аутентификации на основе действий пользователя при работе с клавиатурой персонального компьютера с использованием нейронных сетей.

Информационную базу исследования составили нормативные правовые акты, ГОСТы, а также документы ФСТЭК России. Большое значение для разработки темы имели материалы периодической печати, как российской, так и зарубежной. Также использовались различные статистические и технические данные с официальных сайтов производителей.

Целью исследования является проведение анализа возможностей использования идентификации по клавиатурному почерку с использованием обучаемой нейронной сети на основе действий пользователя для компьютерных систем промышленного назначения.

На данном этапе необходимо также рассмотреть такое явление, как наличие ошибки первого и второго рода в системе аутентификации по клавиатурному почерку. Данные ошибки присущи любой физической системе, основанной на конкретном математическом аппарате, ее природой является неточность, возникающая при проведении математического расчета. В ходе исследования будут рассмотрены также вопросы, связанные с возможным применением методов компьютерного зрения для реализации процесса идентификации. В работе будут изучены возможности применения методов компьютерного зрения, а также методы обучения нейронных сетей для решения задач, возникающих при идентификации по клавиатурам.

Ошибка же второго рода в рамках настоящего исследования может классифицироваться, как ложноотрицательная идентификация легитимного субъекта доступа. Ошибка первого рода традиционно обозначается λ, а ошибка второго рода – β. Существует также такое понятие, как «мощность критерия», определяется значением $1-\beta$. Данный параметр характеризует способность критерия ошибки второго рода не упустить значимое с точки зрения системы аутентификации событие, однако в случае настоящего исследования, в котором рассматривается система аутентификации, основанная на вероятностном прогнозировании, данный параметр значения не имеет, так как значимое событие аутентификации оправляется установленным порогом вероятности.

Необходимо отметить, что для настоящего исследования определение ошибки первого и второго рода является максимально актуальным, так как исследование базируется на вероятностной классификации объекта.

Оценить возникновение ошибок первого и второго рода в рамках настоящего исследования предлагается на основе проведения ряда экспериментов. Нейронная сеть, являющаяся основой алгоритма аутентификации, может содержать обучающую выборку о восьми пользователях. Эксперимент будет основан на введении четырех легитимных (биометрическим данным которых нейронная сеть обучена) и четырех нелегитимных (биометрическим данным которых нейронная сеть не обучена). Так как настоящая система аутентификации основана на вероятностном прогнозировании легитимности пользователя, каждый пользователь имеет максимум 15 попыток ввода текстового сообщения при помощи клавиатуры, тем самым указывая свой клавиатурный почерк. При достижении пользователем совпадений по биометрическим параметрам не менее 90 процентов (минимальное количество – два запуска для исключения ложноположительного срабатывания и влияния ошибки первого рода на работу подсистемы аутентификации), пользователь признается легитимным. После 15 итераций, если пользователь не превысил установленный вероятностный порог, подсистема аутентификации блокирует дальнейшие попытки доступа и формирует сигнал «авария». На данном этапе будет проведена экспериментальная часть с порогом достоверности 90 процентов, то есть легитимным признается тот пользователь, у которого более 90 процентов совпадений биометрических данных с обучающей выборкой для нейронной сети.

Таблица 2.1 – Эксперимент с 90 процентным порогом достоверности

Наименование пользователя	Номер запуска и значение вероятностного совпадения с обучающей выборкой в %															Итоговое вероят-ностное совпадение
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Легитимный пользователь 1	78	94	96	92	93	Вероятностное совпадение достигнуто										90,09377
Легитимный пользователь 2	92	94	Вероятностное совпадение достигнуто													92,98925
Легитимный пользователь 3	92	40	98	93	92	81	98	96	95	98	97	97	93	99	97	86,61795

Легитимный пользователь 4	91	91	Вероятностное совпадение достигнуто													91
Нелегитимный пользователь 1	41	44	43	44	32	44	90	41	45	55	21	22	34	32	30	36,58073
Нелегитимный пользователь 2	70	99	41	16	33	32	34	34	31	34	54	31	21	20	19	30,34284
Нелегитимный пользователь 3	55	54	55	55	44	45	53	52	23	45	61	11	41	21	34	34,84027
Нелегитимный пользователь 4	91	12	23	21	12	34	32	23	45	56	32	21	11	9	7	17,92717

Для лучшего представления необходимо на основании полученных данных построить графики зависимости. На Рисунке 2.1 приведена иллюстрация экспериментальной части для легитимных пользователей.

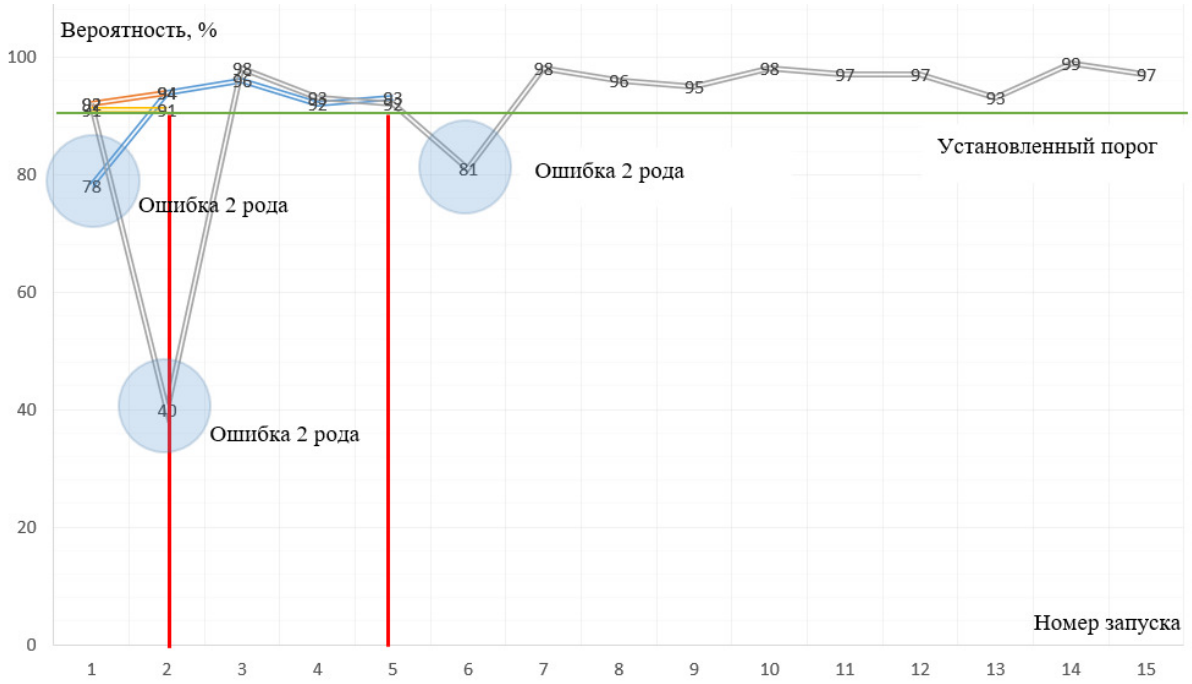


Рисунок 2.1 – Результат экспериментальной части для легитимных пользователей

Данные, представленные в Таблице 2.1 и на Рисунке 2.1 необходимо было проанализировать и в результате анализа можно сказать следующее:

- ошибки второго рода (ложноотрицательная аутентификация) возникает неравномерно и псевдослучайным образом. Данная ошибка может возникать как в результате индивидуальных биомеханических действий пользователя, так и в результате природы нейросетевого алгоритма);
- в результате аутентификации пользователя под номером 3, не смотря на высокие показатели во всех итерациях, кроме второй, низкое значение вероятностного совпадения во второй итерации не позволило преодолеть 90 процентный предел, в результате ошибки второго рода легитимный пользователь алгоритмом был спрогнозирован, как нелегитимный;
- при увеличении порога достоверности выше 90 процентного значения количество ошибок второго рода возрастает, а при снижении – падает. Для настоящего эксперимента установление порога в 40 процентов означает отсутствие ошибок второго рода.

Сейчас необходимо привести данные для нелегитимных пользователей, графическое отображение приведено на Рисунке 2.2.

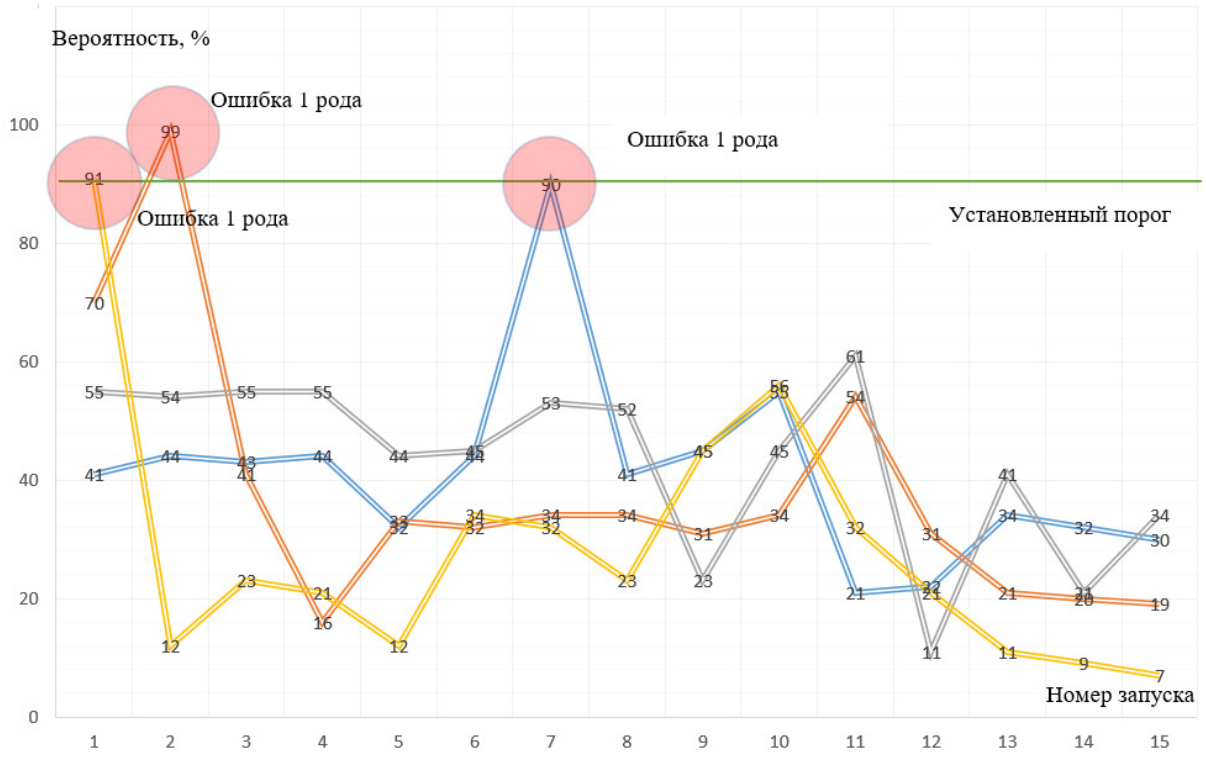


Рисунок 2.2 – Результат экспериментальной части для нелегитимных пользователей

Данные, представленные в Таблице 2.1 и на Рисунке 2.2 необходимо было проанализировать и в результате анализа можно сказать следующее:

- ошибки первого рода (ложноположительная аутентификация) возникает неравномерно и псевдослучайным образом. Данная ошибка может возникать как в результате индивидуальных биомеханических действий пользователя как преднамеренного, так и непреднамеренного характера, так и в результате природы нейросетевого алгоритма);
- Нелегитимный пользователь под номером 4 добился ложноположительной аутентификации в первой итерации, тем самым создал прецедент возникновения ошибки первого рода;
- при снижении порога достоверности ниже 90 процентного значения количество ошибок первого рода возрастает, а при увеличении – падает. Для настоящего эксперимента установление порога в 99 процентов означает отсутствие ошибок первого рода.

Предложения по улучшению работы алгоритма и анализ возможности применения в системах аутентификации.

На данном этапе необходимо предложить варианты по улучшению работы алгоритма. Для этого необходимо увеличивать обучающую выборку, на базе которой происходит обучение нейронной сети. Также данная выборка должна пополняться динамически, при этом пользователь не должен знать, что выполняет тестовое задание, он должен выполнять процедуру ввода с клавиатуры данных для прохождения процедуры аутентификации, при этом обучающая выборка должна меняться и дополняться.

Это необходимо делать в связи с тем, что клавиатурный почерк у пользователя может меняться – некоторые пользователи за достаточно краткий период, до полугода могут освоить технологии печати на клавиатуре «в слепую», а также существенно увеличить скорость печати. При проектировании программного обеспечения, направленного на возможность идентификации по клавиатурному почерку необходимо учитывать данный факт.

Также необходимо подводя итог исследования привести возможные варианты использования алгоритма идентификации по клавиатурному почерку. Такой алгоритм будет иметь вероятностный характер, использовать его в системах, время аутентификации в которых жестко ограничено и использовать его, как единственный алгоритм идентификации нельзя, так

как из анализа, проведенном в рамках настоящего исследования можно сделать вывод о том, что ошибки первого и второго рода возникают в рамках работы данного алгоритма.

Но алгоритм может стать инструментом прогнозирования легитимности пользователя в процессе предъявления им идентификатора, то есть в процессе аутентификации. На данном этапе необходимо привести пример применения подобного алгоритма, лежащего в основе программного обеспечения.

Для этого необходимо представить ситуацию, когда существует ИТКС, оконечный терминал, при помощи которого выполняется процедура аутентификации по предъявляемым пользователям идентификаторам, в рамках данного эксперимента это будет двухфакторная аутентификация с вводом пароля и предъявлением физического носителя. Пользователь А завладел идентификаторами пользователя Б – узнал его пароль и владеет физическим идентификатором. Пользователь А получает доступ к ресурсам ИТКС, введя пароль пользователя Б и предъявив физический идентификатор пользователя Б, в результате процедура аутентификации пользователя А пройдена, но идентифицирован он, как пользователь Б. Создан инцидент информационной безопасности.

Однако, существует подсистема безопасности, которая при предъявлении идентификаторов в процессе аутентификации запрашивает у пользователя ввод с клавиатуры ряда буквенно-цифровых последовательностей, в результате анализа которых можно выделить уникальные свойства клавиатурного почерка и составить прогноз, тот ли пользователь находится в процессе аутентификации, чьи идентификаторы предъявлены. Подобная система может работать в фоновом режиме и выдавать тревожную сигнализацию администратору безопасности в случае отсутствия преодоления вероятностного порога совпадений уникальных особенностей клавиатурного почерка, установленного администратором безопасности. К таким особенностям могут относиться: скорость ввода символов, время пауз при вводе символов и прочие. На рисунках 2.3 и 2.4 приведена графическая иллюстрация применения подобного алгоритма в случае аутентификации легитимным пользователем и нелегитимным пользователем.

Рисунок 2.3 – Результат аутентификации легитимного пользователя

Рисунок 2.4 – Результат аутентификации нелегитимного пользователя

Как можно увидеть из вышеописанного, алгоритм, анализирующий клавиатурный почерк способен прогнозировать легитимность предъявляемым пользователем идентификатором. В случае прогноза нелегитимного использования необходимо вмешательство администратора безопасности.

В рамках написания статьи были определены качественные и количественные показатели работы нейронной сети, лежащей в основе алгоритма, а также даны предложения по улучшению работы алгоритма. На примере моделирования реальной ситуации проведен анализ возможности применения подобного алгоритма в системах аутентификации пользователей.

Список литературы:

1. Яцкевич Ю.Э. Сети ЭВМ.: Учеб. пособие/Ю. Э. Яцкевич; Санкт-Петербург. гос. техн. ун-т. - СПб.: СПбГТУ. -1995. - 124 с.
2. Локальные вычислительные сети: [Справочник : В 3 кн.] / Под ред. С.В. Назарова. - М.: Финансы и статистика. -1995. -246 с.: ил.
3. Климанов В.П. Методы разработки аналитических моделей для анализа локальных вычислительных сетей, используемых в управлении технологическими процессами: Учеб. пособие по курсу «Методы анализа вычисл. систем» / В.П. Климанов; Под ред. А.П. Еремеева; Моск. энерг. ин-т. - М.: Изд-во МЭИ. -1995. - 115 с.
4. Лапшинский В.А. Локальные сети персональных компьютеров: [Учеб. пособие] / В.А. Лапшинский; Центр. банк Рос. Федерации, Моск. гос. инж. -физ. ин-т (техн. ун-т). - М.: МИФИ(ТУ). -1995. -214 с.:.
5. Халсалл Фред. Передача данных, сети компьютеров и взаимосвязь открытых систем / Ф. Халсалл; Пер. с англ. Т.М. Тер-Микаэляна. - М.: Радио и связь. -1995. -407 с.
6. Хаусли Тревор. Системы передачи и телеобработки данных / Т. Хаусли; Пер. с англ. Под ред. Ю.М. Мартынова. - М.: Радио и связь. -1994. -452 с.
7. Doty N. Mitigating Browser Fingerprinting in Web Specifications // W3C

К.Л. Стойчин, Д.С. Крысин, Н.А. Пятков

Научный руководитель: директор учебно-научного центра «Информационная безопасность», доктор технических наук, профессор Поршнев С.В.

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Уральский федеральный университет, Институт радиоэлектроники и информационных технологий-РТФ в г. Екатеринбурге, Россия

Ключевые слова: Персональные данные, корпоративная информационная система, система защиты информации, корпоративные сеть, информационная безопасность.

Промышленные предприятия, как правило, имеют сложную сетевую инфраструктуру, которая включает в себя множество устройств и систем. В связи с этим, обеспечение безопасности корпоративной сети промышленного предприятия является критически важной задачей. Обеспечение безопасности корпоративной сети промышленного предприятия требует комплексного подхода и использования различных технологий и методов защиты. Важно учитывать специфику промышленной среды и принимать меры для обеспечения безопасности всех устройств и систем, находящихся в сети.

K.L. Stoichin, D.S. Krysin, N.A. Pyatkov

Supervisor: Director of the Educational and Scientific center "Information Security", Doctor of Technical Sciences, Professor S.V. Porshnev

THE PROBLEM OF ENSURING THE SECURITY OF THE CORPORATE NETWORK OF AN INDUSTRIAL ENTERPRISE

Ural Federal University, Institute of Radio Electronics and Information Technologies-RTF in Yekaterinburg, Russia

Keywords: Personal data, corporate information system, information security system, corporate network, information security.

Industrial enterprises, as a rule, have a complex network infrastructure, which includes many devices and systems. In this regard, ensuring the security of the corporate network of an industrial enterprise is a critical task. Ensuring the security of the corporate network of an industrial enterprise requires an integrated approach and the use of various technologies and methods of protection. It is important to take into account the specifics of the industrial environment and take measures to ensure the security of all devices and systems on the network.In general, ensuring the security of the corporate network of an industrial enterprise requires an integrated approach and the use of various technologies and methods of protection. It is important to take into account the specifics of the industrial environment and take measures to ensure the security of all devices and systems on the network.

В связи с высокой популярностью сети «Интернет», ее ресурсы стали добычей преступников. Кража личной информации компьютеров пользователей, чьи компьютеры находятся в корпоративной сети, искажение представления информации на веб-сайтах, внедрение паразитного программного обеспечения на легитимные веб-ресурсы с целью его распространения – это далеко не весь список преступлений, которые сегодня актуальны в киберпространстве. Стоит отметить, что борьба с кибернетической преступностью, чрезвычайно развитой на сегодняшний день – глобальная задача, требующая непрерывного выполнения и постоянного совершенствования. Основными объектами атаки являются корпоративные сети,

поэтому такая тема работы, как «проведение анализа защищенности корпоративной сети с выходом в Интернет по указанным направлениям» крайне актуальна и имеет высокую практическую значимость. В результате исследования и классификации атак можно будет говорить о выработке рекомендаций по противодействию атакам на корпоративные сети, что может существенным образом повлиять на работоспособность организаций, которым они принадлежат.

Целью любой коммерческой организации является получение прибыли. Эффективное распределение и использование ресурсов компании – основная задача, выполнение которой необходимо для увеличения доходов компании с целью дальнейшего развития. Для решения данной проблемы используются корпоративные сети.

Нарушение работы корпоративной сети или несанкционированный доступ к ее ресурсам приводит к убыткам компании. При недостаточном уровне безопасности существует вероятность банкротства. Так же, на сегодняшний день по данным аналитических отчетов компаний в области ИБ лишь 8% компаний имеют достаточный уровень защищенности корпоративной сети от внешних атак при постоянно возрастающем количестве угроз ИБ.

Для поддержания оптимального уровня безопасности корпоративной сети коммерческой организации необходимо использовать оценку защищенности, чтобы иметь понимание, в какой степени внедренные меры защиты соответствуют внешней среде.

На сегодняшний день известные методы оценки защищенности носят либо субъективный характер [1], либо не в полной степени подходят для корпоративной сети [2]. Введение метода количественной оценки для корпоративных сетей, основанной на не устаревших данных, помогает не только определить текущий уровень защищенности объективно, но и своевременно отобразить его при появлении новых данных о возможных нарушителях или новых уязвимостях. Данные свойства помогают эффективнее модернизировать состав защитных мер и расходовать ресурсы компании на ИБ чем при известных методах оценивания защищенности, что ведет к повышению уровня защищенности корпоративной сети коммерческой организации. Таким образом, исследования на тему выпускной квалификационной работы «Совершенствование методики оценки защищенности корпоративной сети коммерческой организации с помощью способа построения маршрутов атаки и метода градации информации» являются актуальными.

Объектом исследования являются корпоративные сети коммерческой организации.

Предметом исследования являются методы, алгоритмы и процедуры обеспечения информационной безопасности и защиты информации корпоративной сети коммерческой организации в условиях воздействия внутренних и внешних угроз информационной безопасности.

Целью исследования является описание метода и алгоритма оценки защищенности корпоративной сети коммерческой организации.

Анализ действующих международных стандартов [3], учебников и практических пособий [4] дает понимание, что принцип работы локальных вычислительных сетей лежит в основе корпоративных сетей. Другими словами, коммерческая организация использует локальные вычислительные сети для доступа и распределения ресурсов приложений, необходимых для реализации деятельности компании.

Корпоративная сеть – это взаимосвязанная совокупность средств приема, обработки и передачи данных, участвующая в бизнес-процессах компании, обеспечивающая сотрудникам компании дистанционный доступ к ее ресурсам и коллективное использование этих ресурсов в рамках этой коммерческой организации. Пример типовой корпоративной сети представлен на Рисунке 1.

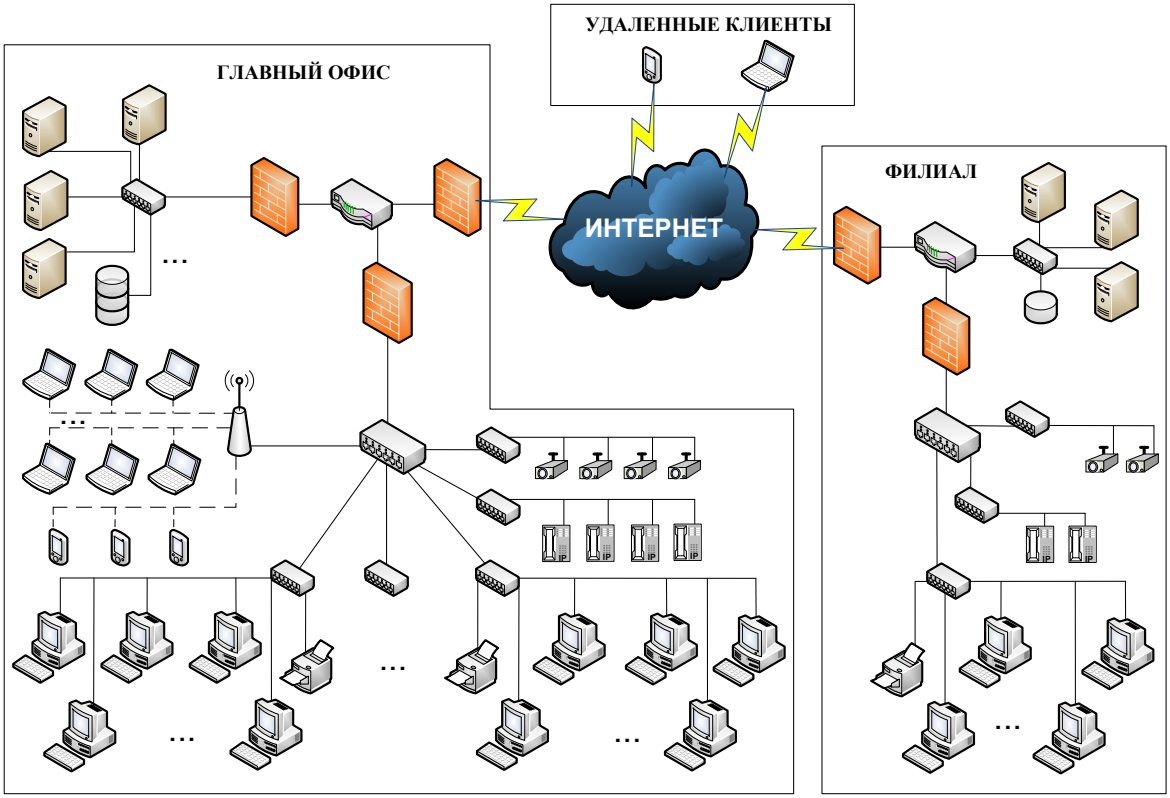


Рис. 1 – Пример корпоративной сети

При анализе актуальных угроз ИБ в рамках повышения защищенности КС было выделено два основных класса угроз:

- угрозы, воздействующие на информацию внутри сети;
- угрозы, направленные на нарушение работоспособности этой сети.

Все остальные известные виды угроз являются производными от этих угроз.

Формой реализации (проявления) угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств ИБ объекта(ов) защиты.

Событие ИБ КС [10-11]: идентифицированное возникновение состояния сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Инцидент ИБ КС: любое непредвиденное или нежелательное событие, которое может нарушить деятельность коммерческой организации или ИБ КС.

У каждой угрозы есть три общих элемента: источник, использованная уязвимость и объект, на который она направлена. Процесс реализации угрозы ИБ для КС представлен на Рисунке 2.

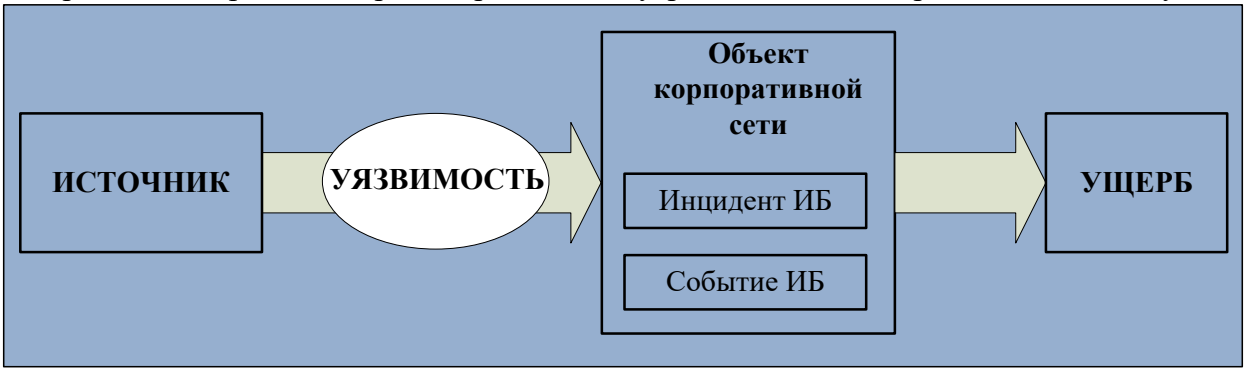


Рис. 2 – Процесс реализации угрозы

В соответствии с методологией ФСТЭК России [4-6,54] источники бывают антропогенными, техногенными и стихийными. Под вторым видом понимаются отказы и сбои

оборудования, под третьим – непредвиденные стихийные бедствия (наводнения, землетрясения и т.д.). При грамотном построении мер защиты вероятность их появления слишком мала по сравнении с антропогенным источником. Поэтому они в меньшей мере задействованы в исследовании.

Что касается антропогенного источника угроз, то это – нарушитель. Основываясь на своих навыках, возможностях и мотивации он начинает искать возможность проникновения в корпоративную сеть. При этом существуют случаи, когда сотрудники компании по неосторожности или недостаточном уровне компетенции создавали ситуации, нарушающие безопасность корпоративной сети. Их можно рассматривать с двух позиций, как внутреннего нарушителя (хоть действия были непреднамеренными) или как уязвимость.

В соответствии с классификацией ФСТЭК России [6, 54], нарушитель обладает следующими характеристиками: тип нарушителя (внешний / внутренний), его потенциал (базовый / базовый повышенный / высокий) и способ доступа (физический / локальный / удаленный).

Нарушитель реализует свою атаку исходя из того, какую информацию он смог собрать о структуре сети, какие есть уязвимости и какими он может воспользоваться исходя из своего потенциала.

Что касается уязвимостей [4, 5], их существует огромное количество, и они постоянно растут. В рамках данной работы была выдвинута следующая классификация уязвимостей: по области происхождения, по типу недостатков, по точке входа в корпоративную сеть. Разделение на классы более детально представлено на Рисунке 3.

При этом уязвимости могут обладать сразу несколькими видами недостатков. Так, например, уязвимость [54] процесса Data-in-Motion (DMo) платформы Cisco IOx позволяет выполнить произвольный код с root-привилегиями. В соответствии с целями могут быть использованы разные типы недостатков. Их перечень представлен на Рисунке 4.

Область происхождения уязвимости	**Типы недостатков**	**Точка входа уязвимости**
- уязвимость кода - уязвимость когфигурации - уязвимость архитектуры - организационные уязвимости - многофакторные уязвимости	- неправильная настройка - неполнота проверки вводимых данных - недостатки, связанные с процессами аутентификации и идентификации - возможность прослеживания структуры - внедрение произвольного кода (инъекция) - утечка/раскрытие информации ограниченного доступа - недостатки, связанные с криптографическими преобразованиями - управление ресурсами - исчерпание ресурсов	- уязвимости в конечном оборудовании - средства защиты - клиентская часть - серверная часть - уязвимости в сетевом оборудовании - уязвимости в каналах связи

Рисунок 3 – Классификация уязвимостей

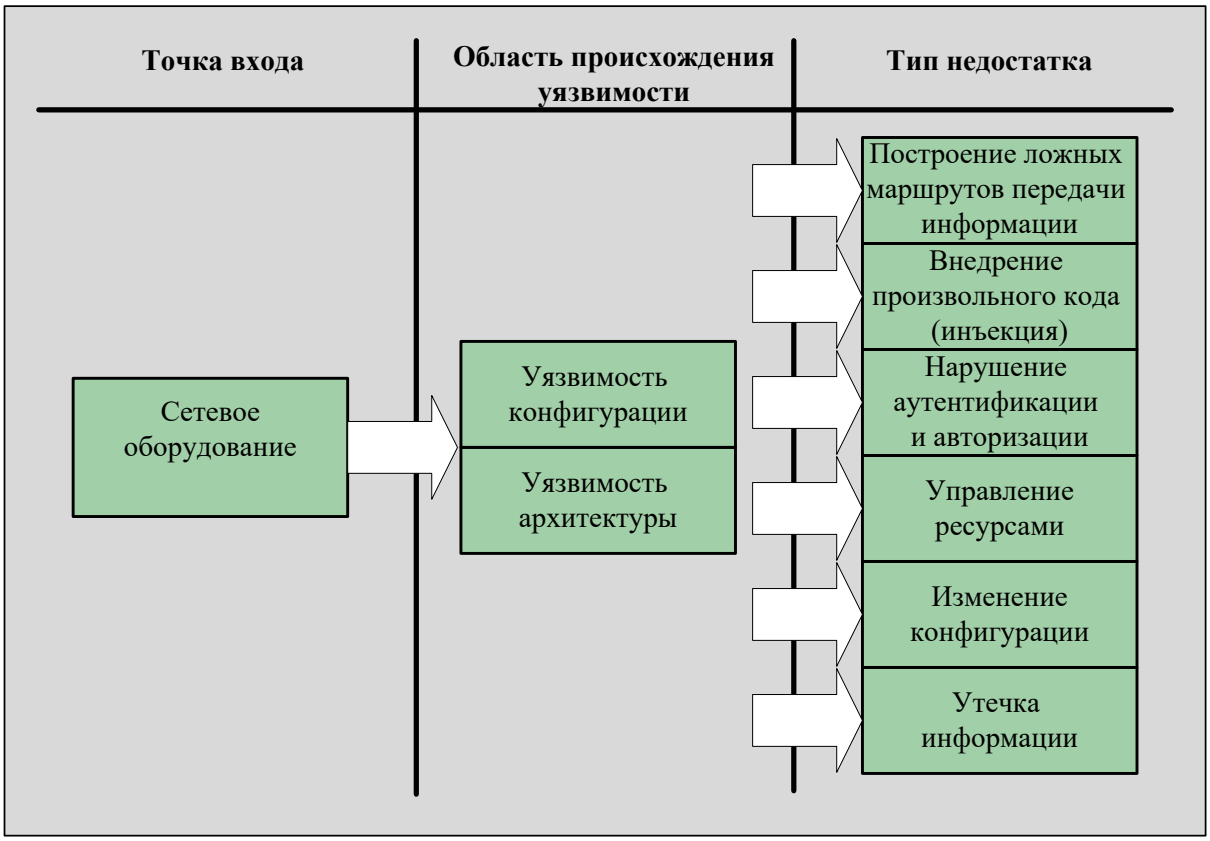


Рисунок 4 – Уязвимость BDU:2017-02494

На Рисунке 5 представлены возможные сценарии реализации угрозы для внешнего и внутреннего нарушителя на главный офис компании. Синим цветом обозначен внешний нарушитель, красным – внутренний. Крест – объект атаки. Окружность – начало атаки.

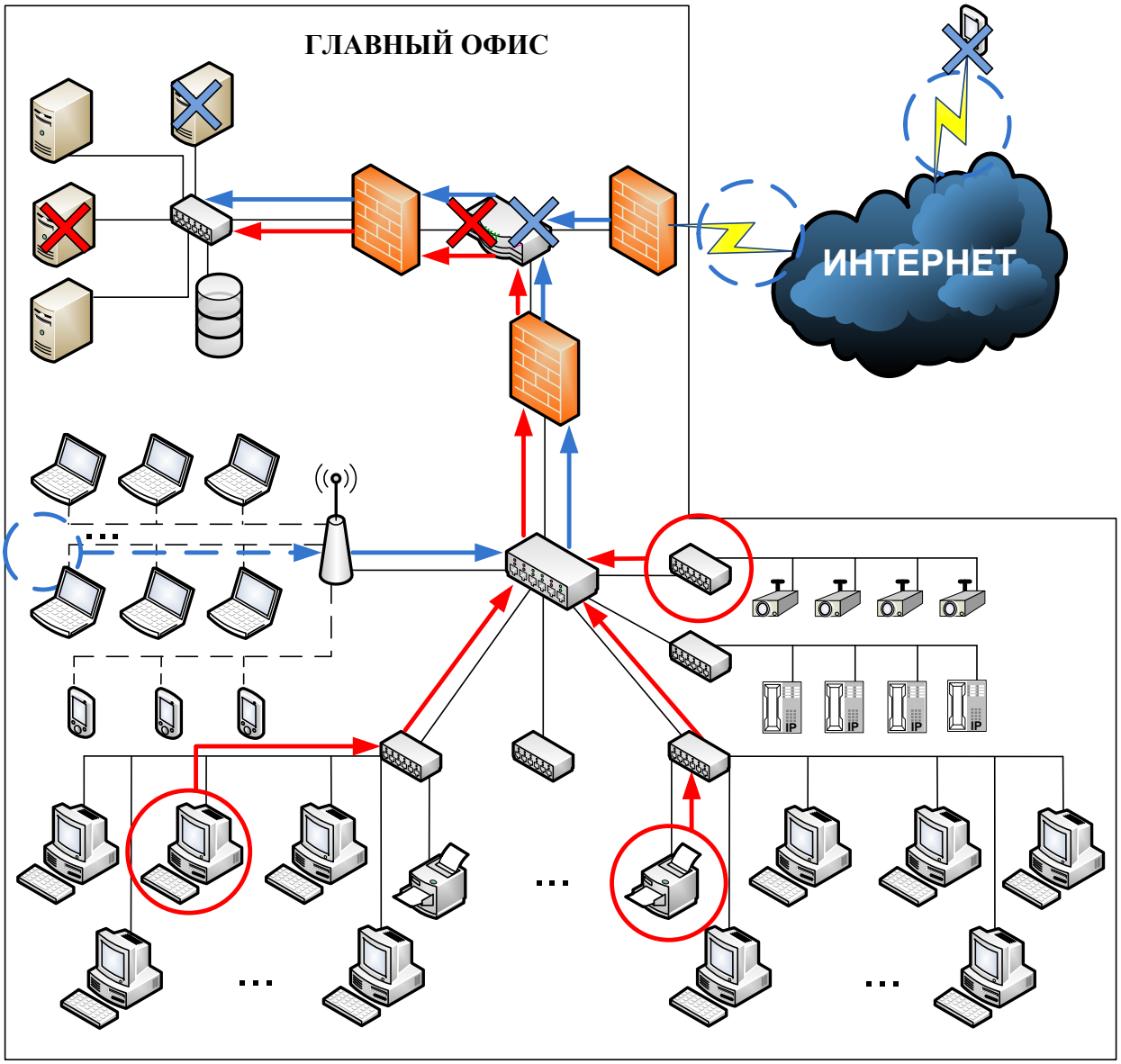


Рис. 5 – Направления атак нарушителей

Способы нарушения защищенного периметра у внешнего нарушителя – начало любой его атаки. Так он может либо найти уязвимость в МЭ, либо искать беспроводную точку доступа, сигнал которой выходит за территорию контролируемой зоны (далее – КЗ). Также внешний нарушитель может найти сотрудника, на которого сможет оказывать влияние (шантаж, подкуп, манипулирование и т.д.). В таком случае следует уже рассматривать внешнего нарушителя, как внутреннего, но с возросшим потенциалом. Вешний нарушитель может подключиться к каналу связи сотрудников, работающих удаленно.

Как правило, нарушитель начинает атаку внутри КЗ. Она может начинаться с любого конечного устройства или канала связи, куда не контролируется физический доступ. МЭ внутри настроен более лояльно, так как необходима эффективная работа компании, а значит более быстрый обмен информацией. И у сотрудника есть легитимные права в соответствии с должностью.

Самым ценным является сетевое оборудование и серверная часть конечного оборудования. Это и есть основные цели атаки.

Алгоритм действий нарушителя следующий. Первым этапом идет сбор информации. На сегодняшний день возможно собрать следующие виды информации [3]: состав и структуру корпоративной сети, виды и версии установленного ПО, а также технических и программно-аппаратных средств и статистические свойства трафика. Знание протоколов передачи

информации, принципов обмена, анализ открытых источников дают возможность составить перечень известных угроз, или обнаружить новые.

Вторым этапом идет определение цели атаки и маршрута. При этом маршрут строится из двух принципов. Позволяют ли имеющиеся у нарушителя ресурсы обнаружить уязвимость, и позволяют ли они воспользоваться ею. После определения маршрутов к цели идет выбор самого оптимального (время на реализацию, шанс обнаружения нарушителя). После этого атака начинается. Реализация зависит от принятых службой безопасности мер защиты.

Строить систему защиту необходимо исходя из условия, что атаки возможны с использованием еще неизвестных уязвимостей. Создание принципиально нового способа воздействия на информацию или на устройства в сети достаточно трудоемкий и маловероятный процесс. Строить систему защиты необходимо из предположения, что уязвимости всегда существуют и их еще не обнаружили, но они обладают рядом похожих признаков. Следовательно, меры защиты должны быть направлены на классы уязвимостей.

Во-вторых, необходимо поддерживать постоянную работоспособность передающих устройств и серверов, где расположены приложения, критичные для обеспечения БП компании. Строить модель защиты надо, опираясь на то, что они – главные цели.

В-третьих, конечные устройства и каналы связи должны быть разделены в соответствии с выполняемыми функциями. Это необходимо для затруднения действий внутреннего нарушителя. Таким образом, разграничение и разделение доступа – необходимый шаг для создания нескольких периметров обороны, что повышает защищенность.

ЗАКЛЮЧЕНИЕ

В рамках исследования было приведено описание современного состояния проблемы обеспечения заданного уровня защищенности корпоративной сети. Для этого был проведен анализ проблемы обеспечения и оценки защищенности корпоративной сети, проведен анализ актуальных угроз, уязвимостей и способов защиты корпоративной сети коммерческой организации.

Список литературы:

1. Введение в информационную безопасность: учеб. пособие для студентов вузов / А. А. Малюк [и др.] ; под ред. В.С. Горбатова. М. : Горячая линия-Телеком, 2013.
2. Лапин В.В. Основы информационной безопасности органов внутренних дел: учеб. пособие (в вопросах и ответах). МосУ МВД России. М. : МосУ МВД России, 2012.
3. Основы информационной безопасности : учеб. пособие для вузов / Е.Б. Белов и [др.] М. : Горячая линия-Телеком, 2011;
4. Яковец Е.Н. Правовые основы обеспечения информационной безопасности Российской Федерации: учебное пособие. – 2-е инд., доп. и перераб. – М.:, Юрлитинформ, 2014.
5. Журавленко Н.И. Тайна частной жизни и защита персональных данных: монография. Уфа: РИЦ БашГУ, 2013.
6. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Москва, 2009.
7. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации Пособие для руководителей и специалистов подразделений по защите информации. М.: МО РФ, 1998. 224 с.
8. Шелупанов А.А., Зайцев А.П. и др. Основы защиты информации, часть 2, Томск: Изд-во «В-Спектр», 2010. В трех частях. Ч.2. 186 с.
9. Зайцев А.П., Шелупанов А.А. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации, Томск: Изд-во Томск. Гос. ун-та систем управления и радиоэлектроники, 2004. 204 с.

А.А. Ступникова, Н.И. Горлов

ТЕНДЕНЦИИ РАЗВИТИЯ ВОЛОКОННО - ОПТИЧЕСКИХ ДАТЧИКОВ

Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ), г. Новосибирск, Россия

Ключевые слова: волоконная оптика, волоконно-оптические датчики, оптическое волокно, рассеяние, сердцевина, оболочка.

Оптические способы измерений уже много лет играют важную роль в технической диагностике и мониторинге состояния. Наличие оптических волокон с малыми потерями привело к революции в сфере волоконно-оптической связи и значительно повысило интерес к волоконно-оптическим датчикам. В статье приведены краткое ознакомление с теоретическими основами волоконно-оптических датчиков, представлен обзор технологий волоконных датчиков, показаны преимущества волоконно-оптических датчиков.

A.A. Stupnikova, N.I. Gorlov

TRENDS IN THE DEVELOPMENT OF FIBER-OPTIC SENSORS

Siberian State university of telecommunications and informatics in Novosibirsk (SibGUTI), Russia

Keywords: fiber optics, fiber-optic sensors, optical fiber, scattering, core, shell.

Optical measurement methods have long played a special role in technical diagnostics and condition monitoring. The presence of silica fibers with low losses led to a revolution in the field of fiber-optic communication and significantly increased interest in fiber-optic sensors. The article provides a brief introduction to the theoretical foundations of fiber-optic sensors, provides an overview of water technologies, and shows the advantages of fiber-optic sensors.

Первое упоминание о волоконно-оптических датчиках относится к гибким эндоскопам, которые были разработаны в начале двадцатого века. Посредством чего произошла революция в области медицины, которая длится до сих пор [1]. Тем не менее, начало развития современных ВОД приходится на 1977 год (имеется ввиду для телекоммуникаций на большие расстояния), и за последние четыре с половиной десятилетия они испытали экспоненциальный рост. Сенсорные приложения являются малым побочным продуктом этой технологии, пользующимся преимуществом разработок в области оптоэлектронных компонентов и концепций. К 1982 году акустические, магнитные, датчики температуры, уровня жидкости давления, перемещения, ускорения, гироскопа, фотоакустические датчики, датчики крутящего момента, тока и датчики деформации уже были среди разработанных и исследуемых волоконно-оптических датчиков [2]. Благодаря разработке оптических волокон с чрезвычайно низкими потерями в конце 1970-х годов, стал возможен этот современный век волоконно-оптических датчиков [1].

Оптическое волокно представляет из себя симметричную структуру в виде цилиндра, состоящую из центральной сердцевины диаметром 9 мкм (одномодовое волокно), 62,5 или 50 мкм (многомодовое волокно) и равномерным показателем преломления [3]. Сердцевина окружена оболочкой, показатель преломления которой меньше показателя преломления сердцевины примерно на 1%. Оболочка улавливает световые волны, выдерживаемые в сердцевине посредством отражения на границе раздела между сердцевиной и оболочкой. Чтобы обеспечить волокну механическую и экологическую защиту, оболочка может быть покрыта внешним пластиковым покрытием. В зависимости от назначения кабели могут быть:

- магистральные – используются для линий связи (ЛС), передающие информацию на большие расстояния;

• городские - используются для передачи информации в пределах относительно небольшого расстояния;

• объектовые – обеспечивают высокоскоростное соединение локальной сети, используются на небольших площадях объектов коммерческого или промышленного назначения.

Так как оптическое волокно является средой физической, то оно неизменно подвергается действию внешних возмущений. Следовательно, оно претерпевает оптические и геометрические изменения из-за этих же возмущений. Для телекоммуникационных приложений желательно минимизировать данные эффекты, чтобы обеспечить надежные приём и передачу сигналов. Тем не менее, реакция на данные внешние индуцированные эффекты умышленно увеличивается при волоконно-оптическом зондировании [4]. Такое изменение некоторых свойств направленного света может быть произведено снаружи (в другой среде) или внутри оптического волокна. Таким образом, можно выделить два различных типа датчиков: внешние и встроенные. Во внешних волоконно-оптических датчиках чувствительным элементом является само оптическое излучение, которое находится вне оптического волокна, по которому излучение доставляется к месту измерений. Тогда как во встроенных волоконно-оптических датчиках одно или несколько оптических волокон являются чувствительным элементом, в котором одна или несколько характеристик, таких как длина волны, интенсивность, спектр, поляризация, время или фаза распространения оптического излучения, зависят от измеряемой величины.

В свою очередь, каждый из этих классов волокон имеет различные подклассы, и даже в некоторых случаях подклассы подклассов, состоящие из большого количества волоконно-оптических датчиков (ВОД). Существуют различные способы классификации волоконных датчиков в зависимости от рассматриваемых свойств, т.е. точки измерения, область применения, процесс модуляции и демодуляции и т.д. Всё же, их можно разделить на три основных класса: датчики на основе решеток, распределенные датчики и интерферометрические датчики [5] (рис. 1).

Интерферометра, используемый для контролирования различных показателей, работает по принципу интерференции двух световых лучей, распространяющихся по нескольким или одному оптическим волокнам разными оптическими путями. Разделение и объединение лучей часто осуществляется с помощью ответвителей. Существует четыре типа интерферометров: интерферометры Маха–Цендера, Фабри–Перо, Саньяка и Майкельсона.

Датчик на основе решеток — это оптический датчик, изготовленный посредством бокового действия на сердцевину одномодового волокна ультрафиолетовым лазерным излучением с периодичной интенсивностью. Действие приводит к постоянному увеличению показателя преломления сердцевины волокна, образовывая модуляцию с фиксированным показателем, известную как решетка. Решетка внутри сердцевины оптоволокна должна отражать определенную длину волны входного света, известную как длина волны Брэгга, коррелирующую с периодом решетки, и пропускать все остальное.

Распределенное зондирование - это технология, которая обеспечивает непрерывные измерения в режиме реального времени по всей длине волоконно-оптического кабеля. В отличие от традиционных датчиков, которые полагаются на дискретные датчики, измеряющие в заранее определенных точках, распределенное зондирование не зависит от изготовленных датчиков, а использует оптическое волокно.

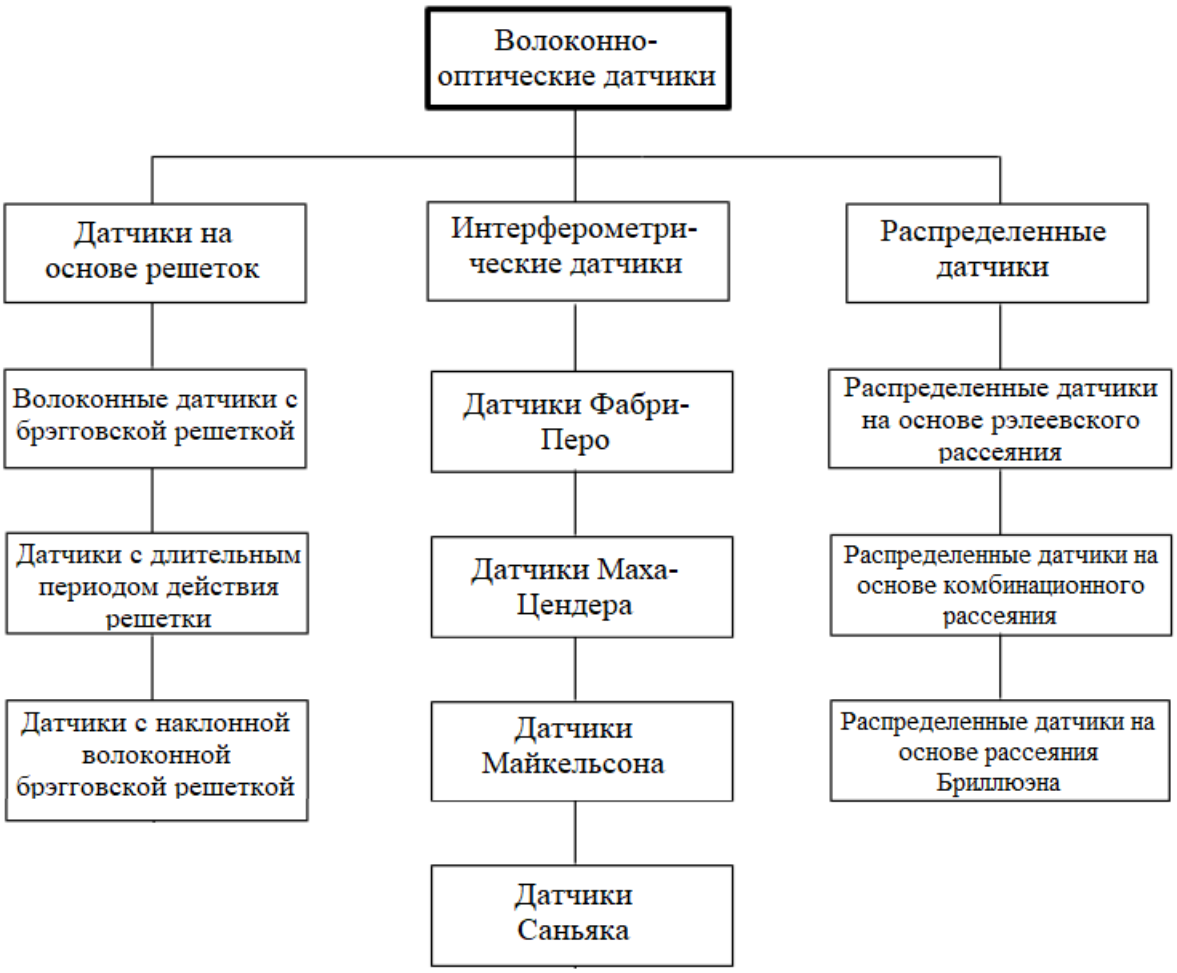


Рисунок 1 - Обзор технологий волоконно-оптических датчиков

Промышленность волоконно-оптической связи точно произвела революцию в телекоммуникационной области, снабдив более доступные, надежные и высокопроизводительные телекоммуникационные линии связи. Вместе со снижения цен на компоненты и улучшением качества сырья, улучшилась и способность волоконных датчиков замещать более привычные электрические датчики [6].

Пользование волоконными датчиками имеет множество безусловных преимуществ. К которым можно отнести:

- устойчивость волоконных датчиков к электромагнитным помехам;
- малый вес;
- небольшие размеры;
- высокую чувствительность;
- характеристики при высоких температурах;
- устойчивость к коррозии;
- большую пропускную способность.

Первоначальное внедрение технологии ВОД было относительно медленным, так как ВОД непосредственно конкурировали с традиционными сенсорными технологиями в последние два десятилетия прошлого века. В большинстве случаев это было связано с высокой стоимостью нужных компонентов. Однако с тех пор эта ситуация изменилась, и прогнозы на будущее весьма оптимистичны, что показывает рисунок 2.

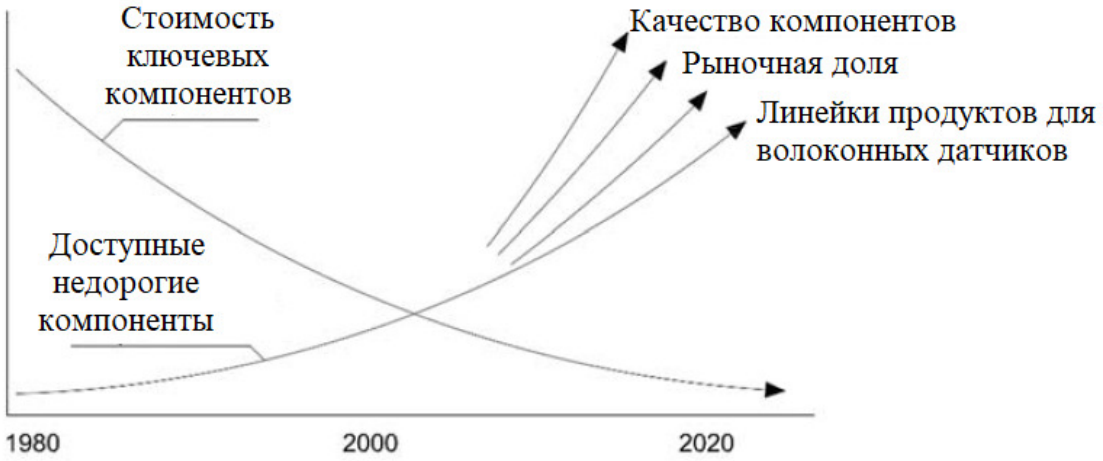


Рисунок 2 - Тенденции развития волоконно-оптических датчиков

С разработкой каждого нового успешного волоконно-оптического продукта стоимость существующих и повторно вводимых компонентов продолжает уменьшаться. К 2025 году существует множество областей, в которых ожидается быстрый рост применения волоконых датчиков. От промышленного и аэрокосмического применения, медицинского приборостроения до систем оценки ущерба в гражданских сооружениях и мониторинга состояния конструкций - постоянно растущие возможности и более низкая стоимость этой технологии делают ее очень привлекательной для пользователей. Методы мониторинга на основе волоконно-оптических датчиков широко используются для неразрушающей оценки всех типов инженерных сооружений главным образом по следующим причинам:

- датчики могут выживать в химически агрессивных средах;
- датчики не могут быть разрушены ударами молнии;
- датчики могут быть интегрированы в очень труднодоступные участки конструктивных элементов;
- датчики способны формируйте сенсорные цепочки, используя одно волокно.

СПИСОК ЛИТЕРАТУРЫ:

1. Удд Э.; Спиллман У.Б.-младший. Волоконно-оптические датчики: введение для инженеров и ученых, 2-е изд.; John Wiley & Sons: Хобокен, Нью-Джерси, США, 2011.
2. Джаллоренци, Т.Г.; Букаро, Дж. А.; Дандридж, А.; Сигел, Г.Х.; Коул, Дж. Х.; Рэшли, С.С.; Прист, Р.Г. Технология волоконно-оптических датчиков. Перевод IEEE. Микроу. Теоретическая техника. 1982, 30, 472-511.
3. Гупта Б.Д. Волоконно-оптические датчики: принципы и приложения; Издательство New India Publishing: Нью-Дели, Индия, 2006.
4. Голамзаде Б.; Набовати Х. Волоконно-оптические датчики. Инт. J. Электр. Вычислить. Энергетический электрон. Коммуна. Англ. 2008, 2, 1107-1117.
5. Го Х.; Сяо Г.; Мрад Н.; Яо Дж. Волоконно-оптические датчики для мониторинга состояния конструкций воздушных платформ. Датчики 2011, 11, 3687-3705.
6. Ю Фрэнсис, Т.С.; Шичжуо Инь. Волоконно-оптические датчики. 2002, Marcel Dekker Inc., Нью-Йорк

Е.С. Тарасов, Н.В. Будылдина, А.С. Никитин, Д.А. Фастов

РАЗРАБОТКА ПРОТОКОЛА КОММУТАЦИИ РЕАЛЬНОГО ТРАФИКА В ВИРТУАЛЬНЫХ СЕТЯХ

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: коммутатор, таблица коммутации, протокол, беспроводная сеть, кадр Ethernet, MAC - адрес, виртуальная сеть.

В статье представлена структурная схема виртуальной системы передачи данных с обработкой реального трафика. Проведен анализ теоретической работоспособности протокола коммутации реального трафика в виртуальной сети.

E.S. Tarasov, N.V. Budyldina, A.S. Nikitin, D.A. Fastov

DEVELOPMENT OF A VIRTUAL COMMUNICATION SYSTEM WITH PROCESSING OF REAL WIRELESS NETWORK TRAFFIC

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: switch, switching table, protocol, wireless network, Ethernet frame, MAC address, virtual network.

The article presents a block diagram of a virtual data transmission system with real traffic processing. The analysis of the theoretical operability of the real traffic switching protocol in a virtual network is carried out.

Введение

Сложившаяся политическая обстановка в мире подталкивает правительство Российской Федерации пересмотреть возможность применения иностранного оборудования в важных областях деятельности государства, одной из которых является связь. Современные сети связи Российской Федерации в основном построены на иностранном оборудовании, вендоры которых заявили об уходе с рынка России – отказались поставлять оборудование и ПО и поддерживать уже развернутые решения, поэтому стоит важная задача о его замене.

Существуют отечественные компании по поставке телекоммуникационного оборудования, такие как: Eltex, Qtech и Nateks. Все эти компании производят аппаратную продукцию, комплектующие к которым приходится закупать у дружественных стран, что сильно влияет на стоимость при построении сетей передачи данных. Помимо затрат на стадии организации, дальнейшее обслуживание сетей передачи данных также требует значительных финансовых затрат, что выражается в закупке нового сетевого оборудования и кабеля.

Для уменьшения затрат на организацию и обслуживание небольших корпоративных сетей в УрТИСИ СибГУТИ было решено провести исследование, с целью определения такой возможности. Чтобы решить данную проблему, было решено максимально исключить применение аппаратной части, поэтому оптимальным решением является применение беспроводных сетей, которые позволят заменить провода, и виртуализации для замены аппаратных средств. В статье рассматривается один из вариантов использования виртуальных сетей с обработкой реального трафика.

Целью исследования является разработка виртуальной среды, способной обрабатывать реальный трафик, а также разработка протокола для коммутации трафика внутри виртуальной сети.

1 Технологии виртуализации

Виртуализация — это создание виртуальной версии чего-либо, например операционной системы (ОС), сервера, устройства хранения или сетевых ресурсов.

Виртуализация использует программное обеспечение, которое имитирует функциональность оборудования для создания виртуальной системы. Эта практика позволяет ИТ-организациям работать с несколькими операционными системами, несколькими виртуальными системами и различными приложениями на одном сервере. К преимуществам виртуализации относятся более высокая эффективность и экономия за счет масштаба.

Виртуализация обеспечивает большую гибкость, контроль и изоляцию за счет устранения зависимости от конкретной аппаратной платформы. Первоначально предназначенная для виртуализации серверов, концепция виртуализации распространилась на приложения, сети, данные и рабочие столы [2].

Виртуализация может применяться как в проводных, так и в беспроводных сетях. И при использовании беспроводной среды важно учитывать ее особенности, например, затухание, мобильность, широковещательная передача. Помимо всего прочего, виртуализация беспроводной сети зависит от конкретных технологий доступа, а беспроводная сеть содержит гораздо больше технологий доступа по сравнению с виртуализацией проводной сети, и каждая технология доступа имеет свои особые характеристики, что затрудняет совместное использование с другими сетями и элементами сетей [3].

В настоящее время существует большое количество симуляторов и эмуляторов сетевого оборудования для возможности обучения или демонстраций. Основными примерами являются Cisco Packet Tracer или EVE-NG. Их главным недостатком является то, что они только эмулируют работу реального оборудования и сети. За обработку реального трафика отвечает аппаратные устройства, при этом для построения сети требуется кабель, который является олним из самых дорогих элементов любой проводной сети передачи данных.

2 Структурная схема сети связи

Чтобы уменьшить затраты на создание и обслуживания сетей в компаниях и предприятиях, используются беспроводные сети. Самым главным достоинством является снижение использования кабеля. Для исследования будет использоваться стандарт IEEE802.11n, ввиду его популярности на данный момент.

Кроме кабеля, основные затраты приходятся и на аппаратные устройства, к примеру коммутаторы или маршрутизаторы. В таком случае, это оборудование можно представить в программном виде и установить на один аппаратный сервер. В данной статье будут рассматриваться только программные коммутаторы, которые объединяются в виртуальную сеть.

На рисунке 1 показана структурная схема созданной системы связи.

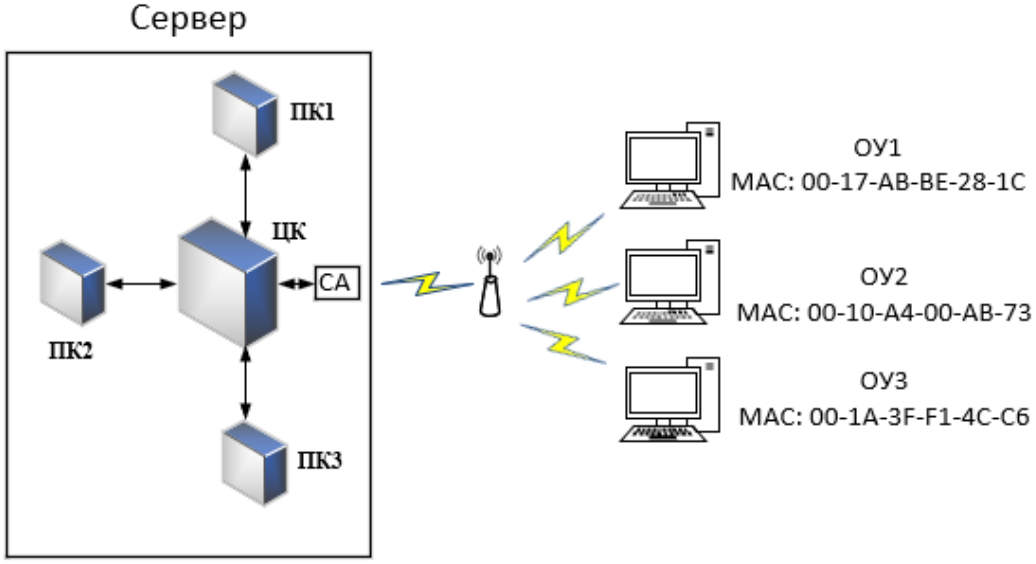


Рисунок 1 – Структурная схема системы связи

На все компьютеры, обозначенные как оконечные устройства (ОУ) будут установлены сетевые адаптеры стандарта IEEE802.11n для обеспечения беспроводной сети. Такой же сетевой адаптер (СА) будет помещен и в сервер. Для обеспечения связи между ОУ и сервером будет также использоваться точка доступа (ТД). Однако если сеть будет иметь небольшой размер, то точка доступа будет необязательной.

Сервер является аппаратной составляющей и служит, чтобы организовать виртуальную сеть внутри него, которая будет обрабатывать тот трафик, который поступает из беспроводной сети. Виртуальная сеть представляет собой один или несколько программных коммутаторов (ПК) для обеспечения передачи данных. Программный коммутатор являет собой специальную программу с функциями классического аппаратного коммутатора.

Количество ПК напрямую будет зависеть от количества рабочих станций, подключенных в сеть, так как при использовании только одного ПК может быть большой трафик, что существенно скажется на времени обработки всех данных.

Для коммутации трафика между несколькими ПК следует создать отдельный центральный коммутатор (ЦК), в задачу которого будет входить коммутация трафика между ПК и СА.

В классических аппаратных коммутаторах для возможности обмена данными каждое оконечное устройство подключается в физически порт коммутатора при помощи кабеля UTP. Однако в созданной системе все ОУ подключаются через одну точку доступа к виртуальной сети. И при необходимости использования, например VLAN, STP и т.д., необходимо подключать ОУ к отдельным портам. Поэтому следует на ПК создать логические порты, к которым логически будут подключаться рабочие станции или другие ОУ. [4]

Ранее для сопряжения виртуальной и беспроводной сети был разработан протокол WVNIP, принцип работы которого заключался в добавлении в кадр Ethernet [1] специального поля «Идентификатор логической связи» (ИЛС) на оконечном оборудовании, после чего кадр передавался по беспроводной связи на виртуальную сеть. [4] Данный протокол работоспособен, однако имеет свои недостатки. Самым главным недостатком являлось то, что, изменяя кадр Ethernet, менялся сам стандарт. Также так, появление нового поля в кадре означало, что он будет более длинным, что скажется на пропускной способности при передаче данных. В связи с этим было решено разработать альтернативный ему протокол SNSP.

3 Формат кадра протокола SNSP

Информация о логическом подключении рабочей станции к программному коммутатору будет находиться в таблицах коммутации на каждом ПК. Данные полей «MAC» и «Порт» задаются администратором и являются статичными. Нулевой порт (0) предназначен для связи ПК с ЦК. Допустим, на ПК1 зарегистрированы оконечные устройства (ОУ) 1 и 2, а на ПК2 зарегистрировано ОУ3. В таком случае, таблица коммутации ПК1 имеет вид, как показано на таблице 1.

Таблица 1 – Таблица коммутации ПК1

MAC	Порт
	0
00-17-AB-BE-28-1C	1
00-10-A4-00-AB-73	2

В столбце «MAC» записаны физические адреса ОУ, которые зарегистрированы на данном ПК. В столбце «Порт» указывается номер логического порта, к которому логически подключаются ОУ, с соответствующими MAC-адресами.

Для передачи кадра между ЦК, СА и ПК необходимо в кадр Ethernet добавить специальное поле ИЛС, когда он поступает на центральный коммутатор. При помощи данного поля кадр будет продвигаться внутри виртуальной сети. Формат кадра с полем ИЛС показан на рисунке 2.

6 байт	6 байт	1 байт	2 байта	46-1500 байт	4 байта
Адрес получателя	Адрес отправителя	ИЛС	Тип	Данные	Контрольная сумма

Рисунок 2 – Формат кадра Ethernet с полем «ИЛС»

Таким образом, коммутация внутри виртуальной сети будет осуществляться по протоколу SNSP (Software network switching protocol - протокол коммутации в программных сетях).

4 Принцип работы протокола SNSP

Рассмотрим принцип коммутации кадров, когда два ОУ зарегистрированы на одном ПК. Допустим, ОУ1 и ОУ2 зарегистрированы на ПК1. Администратор сформировал таблицу коммутации (таблица 1). Необходимо передать кадр с ОУ1 на ОУ2.

ОУ1 формирует кадр Ethernet и отправляет его по беспроводной сети на точку доступа, которая в свою очередь передает кадр на сетевой адаптер сервера. Далее с сетевого адаптера кадр передается на ЦК, где в него добавляется поле «ИЛС» (рисунок 2), в котором устанавливается значение 0. Это показывает, что кадр только поступил в ЦК. После чего ЦК рассылает данный кадр широковещательно на нулевые порты всех ПК.

Первоначально каждый ПК анализирует кадр по полю «Адрес отправителя» и сверяет его со своей таблицей коммутации. В данном случае ОУ1 есть в таблице адресов ПК1. Тогда ПК1 приписывает кадр к логическому порту 1, в соответствии с таблицей 1.

ПК2 и ПК3 также сверяют кадр со своими таблицами адресов (таблица 2 и 3). Так как адрес получателя и отправителя в таблицах не найдены, то кадр отбрасывается.

Таблица 2 - таблица коммутации ПК2

MAC	Порт
	0
00-1A-3F-F1-4C-C6	1

Таблица 3 - таблица коммутации ПК3

MAC	Порт
	0

ПК1 после того, как приписал кадр за первым логическим портом, также анализирует кадр по полю «Адрес назначения». Обнаружив MAC-адрес получателя, он приписывает его к логическому порту 2, в соответствии с таблицей 1.

Так как получатель и отправитель зарегистрированы на одном ПК, то кадр следует отправить на сетевой адаптер для дальнейшей передачи на ОУ2. Для этого в поле «ИЛС» кадра ПК1 ставится значение 0. Затем ПК1 отправляет кадр на ЦК по нулевому порту. ЦК анализирует поле ИЛС и сверяет по своей таблице коммутации (таблица 4).

Таблица 4 - Таблица коммутации ЦК

Значение ИЛС	Направление
0	СА
1	ПК1
2	ПК2
3	ПК3

Так как в поле ИЛС кадра указано значение 0, это значит, что кадр должен быть передан на сетевой адаптер. Перед отправкой кадра удаляется поле ИЛС, после чего кадр перенаправляется на сетевой адаптер, от куда передается на точку доступа, которая в дальнейшем отправляет его на ОУ2.

Рассмотрим принцип коммутации кадров, когда два ОУ зарегистрированы на разных ПК. Допустим, ОУ1 зарегистрирован на ПК1, а ОУ3 зарегистрировано на ПК2. Администратор сформировал таблицы коммутации (таблица 1 и 2). Необходимо передать кадр с ОУ1 на ОУ3.

Принцип коммутации тот же, что и в первом случае до момента, когда ПК1 анализирует поле адреса получателя. ПК1 проверяет таблицу коммутации на наличие MAC-адреса получателя. Так как его нет, то он ожидает результата проверки от остальных ПК.

MAC-адрес получателя обнаруживает у себя ПК2, в соответствии с таблицей 2. При помощи служебного кадра, ПК2 широковещательно сообщает всем ПК о том, что получатель зарегистрирован у него. ПК1, получив эту информацию, устанавливает в поле ИЛС кадра значение 2, что означает, что кадр должен быть передан на ПК2. Далее, кадр отправляется на ЦК, откуда, в соответствии с таблицей коммутации, передается на ПК2 и приписывается к логическому порту 1, в соответствии с таблицей 2.

Дальнейшая передача кадра получателю осуществляется аналогично, как описано выше.

Заключение

Разрабатываемая виртуальная система связи позволит небольшим компаниям значительно снизить расходы, при организации и обслуживании сетей передачи данных, а также упростить их эксплуатацию, так как станет меньше применяемых аппаратных средств. Разработанный протокол SNSP, в сравнении с протоколом WVNIP, является более оптимальным, так как служебное поле ИЛС добавляется только внутри сервера, и не нагружает беспроводную сеть передачей дополнительной служебной информации.

Разработанная виртуальная система передачи данных, в совокупности с протоколом SNSP, показала свою теоретическую работоспособность, а значит, в перспективе, может использоваться для работы в организациях, что позволит им снизить затраты на организацию и обслуживание корпоративной сети передачи данных.

СПИСОК ЛИТЕРАТУРЫ:

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : Учеб. для студентов, аспирантов и техн. специалистов, работающих в обл. сетевых технологий / В. Г. Олифер, Н. А. Олифер. - СПб. и др. : Питер, 1999. - 668 с.
2. Что такое виртуализация. [Электронный ресурс] – Режим доступа: https://www.techtarget.com/searchitoperations/definition/virtualization (Дата обращения: 8.04.2023).
3. Использование виртуальных сетей. [Электронный ресурс] – Режим доступа: https://en.wikipedia.org/wiki/Network_virtualization (Дата обращения: 8.04.2023).
4. Тарасов Е. С., Будылдина Н. В., Никитин А. С., Фастов Д. А. Разработка виртуальной системы связи с обработкой виртаульного трафика беспроводной сети // Инфокоммуникационные технологии: Актуальные вопросы цифровой экономики. Сборник научных трудов III Международной научно-практической конференции. 25-26 мая 2023 г., г. Екатеринбург, с. 82-87.

И.И. Шестаков, Е.И. Гниломёдов

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ МНОГОУРОВНЕВЫХ ФОРМАТОВ МОДУЛЯЦИИ В ДЛИННОПРОЛЕТНЫХ СЕТЯХ DWDM

Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

Ключевые слова: модуляция оптической несущей, технология DWDM, коэффициент ошибок.

В работе выполнено исследование эффективности применения многоуровневых форматов модуляции в длиннопролётных сетях DWDM. Для оценки их эффективного применения, выполнено программное моделирование в САПР OptiSystem. Для каждого формата многоуровневой модуляции (ASK, PSK, QAM и OFDM и их разновидности) в OptiSystem разработаны блок-схемы, позволяющие оценить коэффициент ошибок в зависимости от OSNR на входе приемника. Параметр OSNR изменялся путем увеличения количества усилительных участков. Стоит отметить, исследование проводилось в рамках одного оптического канала DWDM. Результатом моделирования является обобщенный график зависимости коэффициента ошибок от количества усилительных участков, для рассмотренных форматов модуляции. Анализируя результаты моделирования, можно утверждать то, что наиболее эффективным многоуровневым форматом модуляции в длиннопролетной системе DWDM является формат QPSK, DP-QPSK, DP-M-QAM. Эти форматы модуляции более устойчивы к аккумулируемому шуму линейных усилителей.

I.I. Shestakov, E.I. Gnilomedov

INVESTIGATION OF THE EFFECTIVENESS OF MULTI-LEVEL MODULATION FORMATS IN LONG-SPAN DWDM NETWORKS

Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

Keywords: optical carrier modulation, DWDM technology, error coefficient.

The paper investigates the effectiveness of the use of multilevel modulation formats in long-span DWDM networks. To evaluate their effective application, software modeling in OptiSystem CAD was performed. For each multi-level modulation format (ASK, PSK, QAM and OFDM and their varieties), OptiSystem has developed flowcharts that allow estimating the error coefficient depending on the OSNR at the receiver input. The OSNR parameter was changed by increasing the number of amplifying sections. It is worth noting that the study was conducted within the framework of a single optical DWDM channel. The result of the simulation is a generalized graph of the dependence of the error coefficient on the number of amplifying sections for the considered modulation formats. Analyzing the simulation results, it can be argued that the most effective multi-level modulation format in a long-span DWDM system is the QPSK, DP-QPSK, DP-M-QAM format. These modulation formats are more resistant to the accumulated noise of linear amplifiers.

Транспортные сети связи, реализуемые на базе технологии DWDM, позволяют организовать пропускную способность десятки петабит в секунду, и зависит это от формата модуляции оптической несущей канала WDM [1]. Однако, увеличении пропускной способности зависит не только от формата модуляции, но и от количества линейных усилительных участков. Дело в том, что оптический усилитель вносит в полезный сигнал собственные (спонтанные) шумы, уровень которых зависит от их количества. Увеличение количества оптических усилителей на прямую влечет к уменьшению OSNR (отношение сигнала/шум), что сказывается на росте коэффициента ошибок на приеме.

В системах DWDM в качестве современных форматов модуляции применяются многоуровневые форматы, такие как:

1) четырехпозиционная амплитудная модуляция формата 4-ASK;
2) четырехпозиционная фазовая модуляция формата DQPSK, QPSK и DP-QPSK;
3) квадратурная модуляция формата 4-QAM, DP-16QAM и DP-32QAM;
4) ортогональное частотное мультиплексирование формата OFDM-4QAM, OFDM-DP-QPSK, OFDM-DP-16QAM.

Стоит отметить, что наибольшую популярность, получили форматы модуляции класса M-PSK и QAM. Формат модуляции класса OFDM является относительно новым видом модуляции в системах DWDM, на практике не применяется, но, широкое внимание ему уделяется в области научных исследований. Что касается формата модуляции 4-ASK, то, как показали научно-исследовательские работы и работа реальных системы DWDM с данным видом модуляции, этот формат целесообразно применять в системах DWDM с пропускной способностью канала до 40 Гбит/с на участках до 80 км. Несмотря на это, для обобщенного анализа, в работе выполнен сравнительный анализ этих видов модуляции.

Для этого выполнено программное моделирование в САПР OptiSystem. В работе рассмотрено моделирование одного оптического канала DWDM. Это позволит уменьшить объем графического код программы, тем самым уменьшить нагрузку на процессор при математических вычислениях.

Эффективность применимости многоуровневых форматов модуляции оценивалась значением коэффициента ошибок в зависимости от величины OSNR (Optical Signal Noise Ratio – отношение оптической мощности полезного сигнала к оптической мощности шума). Значение OSNR зависит как от длины оптической линии связи, так и от уровня шума. Как известно [2], в ВОСП источником шума является лазерный диод, фотодиод и оптический усилитель. Как правило, эти источники вносят постоянную величину шума и можно говорить о том, что значение OSNR имеет постоянную величину. Но это не так. Во-первых, при распространении полезного сигнала в оптической линии наблюдается уменьшение его оптической мощности, тем самым уменьшается величина отношение сигнал/шум. Во-вторых, на оптических линиях связи где задействуется не один, а несколько оптических усилителей, наблюдается аккумуляция шумов всех усилителей, то есть наблюдается увеличение мощности оптического шума, что также ведет к уменьшению соотношения сигнал/шум. Таки образом, рассмотрена модель одноканальной оптической линии связи большой протяженностью, реализуемой за счет применение оптических усилителей. Это позволит полноценно (от длины линии и количества усилительных участков) оценить коэффициент ошибок в канале DWDM для рассматриваемых форматов модуляции.

Сравнительный анализ форматов модуляции проводился для ВОСП, представляющей собой передатчик и приемник с несколькими усилительными участками длиной по 80 км, с километрическим затуханием оптоволокна 0,2 дБ/км и рабочей длиной волны 1550 нм. Мощность спонтанных шумов в усилителях составила 4 дБ [1,2], что соответствует реальным значениям для EDFA усилителя (Erbium Doped Fiber Amplifier – эрбиевый волоконно-оптический усилитель).

В библиотеке САПР OptiSysytem имеются все необходимые компоненты для моделирования приемо-передающие оптических модулей, для генерации и приема оптических сигналов с многоуровневой модуляцией формата ASK, PSK, QAM и OFDM. В библиотеке САПР OptiSysytem, в разделе оптические передатчики и приемники имеются готовые передающие и приемные модули оптических сигналов с форматом модуляции 8-PSK, 16-PSK, 32-PSK, 4-QAM, 8-QAM, 16-QAM и 32-QAM как без поляризационного, так с поляризационным

мультиплексированием. Такие готовые решения позволили уменьшить время на разработку блок-схемы и уменьшить размеры разрабатываемой блок-схемы. Для генерации и приема оптического сигнала с другими форматами модуляции, например, 4-ASK или OFDM, готовых компонентов в библиотеке САПР OptiSysytem, их пришлось разрабатывать (моделировать).

Для разработки передающих и приемных оптических модулей (4-ASK и OFDM) были задействованы такие компоненты как генератор псевдослучайной двоичной последовательности, генератор многоуровневых электрических сигналов, источник оптического излучения, фотодиоды, модуляторы Маха-Цендера, оптические кросс-объединители/разветвители, поляризационные сплиттеры, оптический элемент фазовой задержки сигнала, электрические фильтры нижних частот, оптические фильтры, модуляторы и демодуляторы электрических сигналов M-PSK и M-QAM, компоненты для работы с OFDM, PSK и QAM сигналом.

Для моделирования ВОЛС состоящей и нескольких равных участков протяжённостью 80 км были использованы такие компоненты как: оптическое волокно, усилитель EDFA и петлевой контроллер для модуляции нескольких усилительных участков.

Для сбора результатов моделировал были применены приборы (инструменты), позволяющие измерить коэффициент ошибок, снять спектрограмму оптического и электрического сигнала, снять глаз-диаграмму электрического сигнала и снять I/Q-диаграмму (созвездие) многоуровневого формата модуляции.

На рисунках 1 – 3 представлены разработанные блок-схемы модели канала DWDM с модуляцией QPSK, DP-QPSK, DP-M-QAM, которая показала наилучший результат.

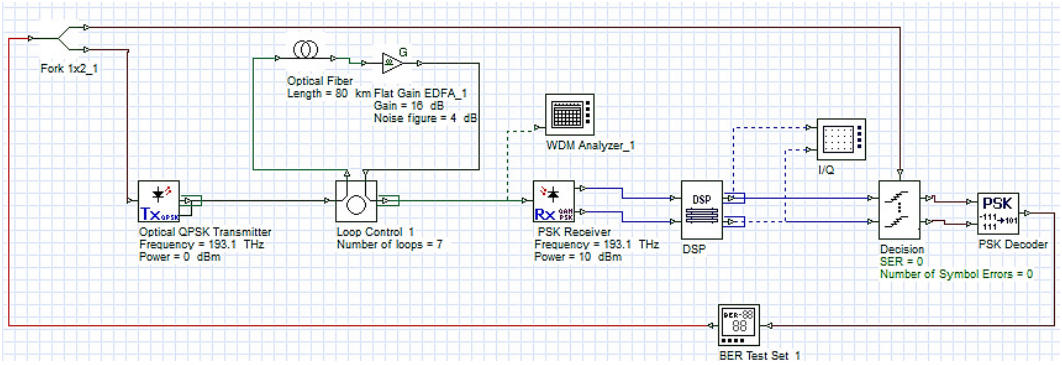


Рис. 1. Блок-схема модели канала DWDM с модуляцией QPSK

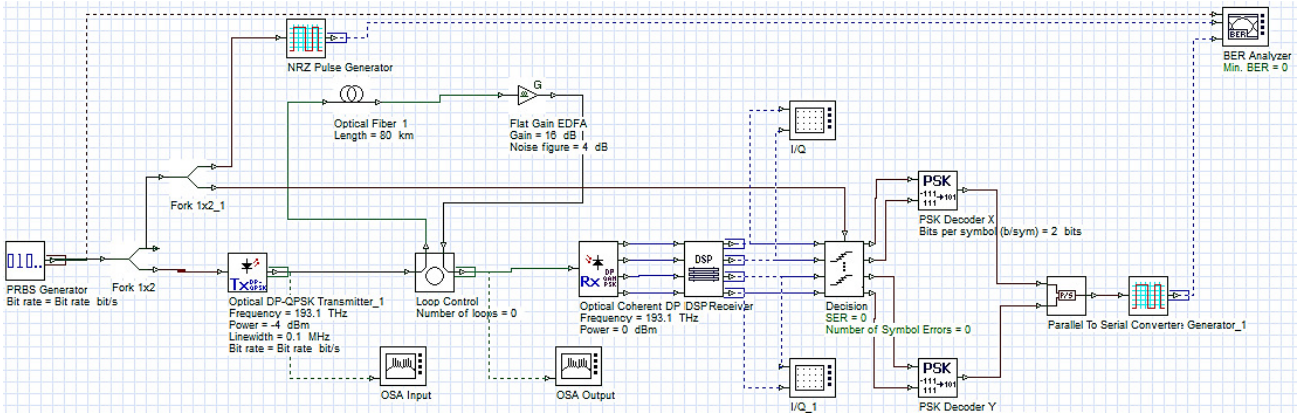


Рис. 2. Блок-схема модели канала DWDM с модуляцией DP-QPSK

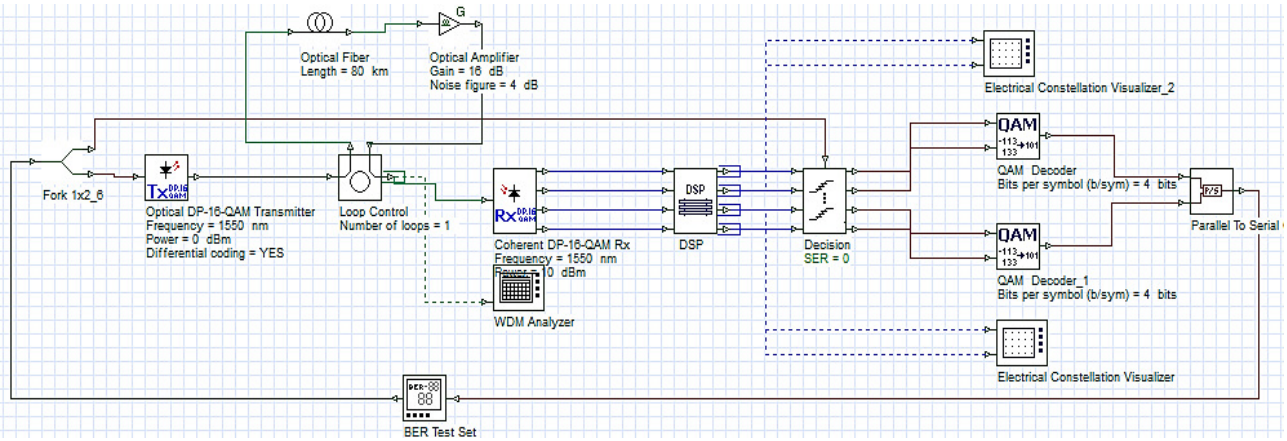


Рис. 3. Блок-схема модели канала DWDM с модуляцией DP-16QAM

Результат моделирования многоуровневых форматов модуляции представлен на рисунке 4 в виде зависимости коэффициента ошибок от количества оптических усилителей, а фактически от длины ВОЛС. Характер полученных зависимостей имеет сходство с аналитическими и теоретическими аспектами в области многоуровневой модуляции [3-5].

Анализируя графики зависимости, можно говорит о том, что для организации длиннопролетных ВОЛС DWDM, с пропускной способностью канала 100 и более Мбит/с, перспективными форматами модуляции являются: QPSK, DP-QPSK, DP-M-QAM. Эти форматы модуляции более устойчивы к аккумулируемому шуму линейных усилителей, и обеспечивают приемлемый коэффициент ошибок на приеме [6]. Однако, анализирую спектрограммы и I/Q-созвездие, рекомендуется применять компенсаторы дисперсии, устанавливаемые в усилительных пунктах, а также применять компенсацию дисперсии на приеме на электрическом уровне, что позволит реализовать ВОСП DWDM протяженностью до 600 км.

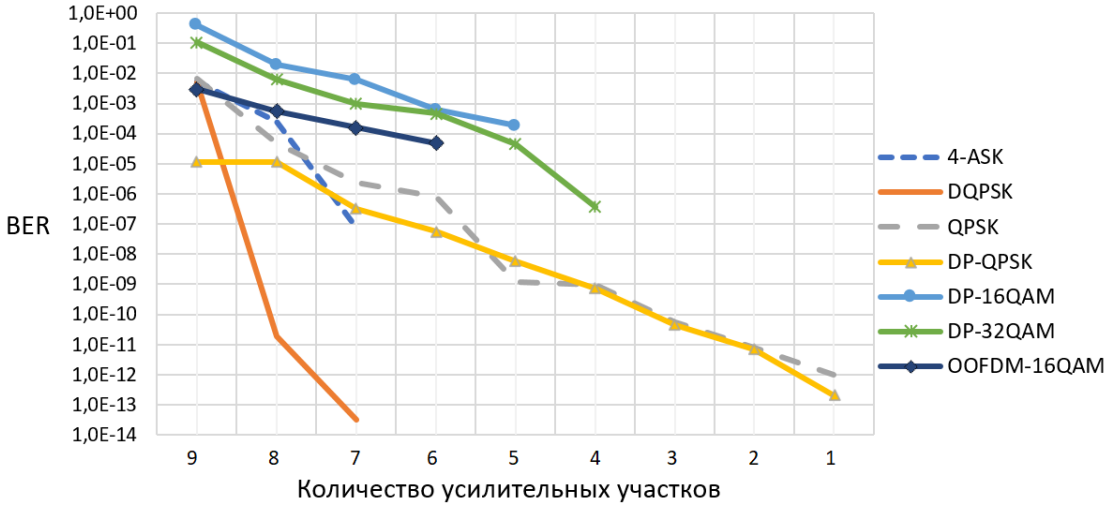


Рис. 4. Графики зависимости BER от количества усилительных участков протяженностью 80 км

СПИСОК ЛИТЕРАТУРЫ:

1. Фокин В.Г. Оптические системы с терабитными и петабитными скоростями передачи [Электронный ресурс]: учебное пособие / В.Г. Фокин, Р.З. Ибрагимов. – Электрон. текстовые данные. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2016. – 156 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/54790.html
2. Татаркина О.А. Волоконно-оптические системы передачи: Конспект лекций/О.А. Татаркина. – Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2008. – 160 с.
3. Величко М.А., Наний О.Е., Сусьян А.А. Новые форматы модуляции в оптических системах связи. LIGHTWAVE Russian Edition №4 (2005). С.21-36. [Электронный ресурс]. – Режим доступа: https://t8.ru/wp-content/uploads/2012/01/20.pdf

4. Gurkin N.V., Nanii O.E., Novikov A.G., Plaksin S.O., Treshchikov V.N., Ubaidullaev R.R. Nonlinear interference noise in 100-Gbit/s communication lines with the DP-QPSK modulation format. Quantum Electron., 43 (6) (2013), pp. 550-553 [Электронный ресурс]. – Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-84879816435&origin=inward&txGid=34cf6aafa58cff7dc955c2d 0df2d9f4d
5. Cheng M., Cheng-Ting Tsai and Lin G. Master-to-slave injection-locked WRC-FPLD pair with 16 DWDM-PON channels for 16-QAM OFDM transmission. OFC 2014, San Francisco, CA, 2014, pp. 1-3 [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/6886904
6. Рекомендация ITU-T G.696.1 (07/2010). Series G: Transmission systems and media, digital systems and networks. [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/T-REC-G.696.1-201007-I

В.П. Шувалов, И.Г. Квиткова

К ВОПРОСУ О СНИЖЕНИИ ИНТЕНСИВНОСТИ ДЕГРАДАЦИОННЫХ ОТКАЗОВ ПРИ КОРРЕКТИРУЮЩЕМ ОБСЛУЖИВАНИИ

Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ),
г. Новосибирск, Россия

Ключевые слова: эксплуатация оптического кабеля, элементарный участок оптического кабеля, деградационный отказ, локальный отказ, замена участка, критическая интенсивность отказов.

В процессе эксплуатации оптического кабеля происходят отказы, локальные или глобальные, вызванные различными причинами. Вследствие чего может осуществляться замена поврежденного участка кабеля. В статье рассматривается марковская модель процесса деградации оптического кабеля, с помощью которой оценивается влияние замены участков оптического кабеля на деградационные процессы вследствие локальных отказов и заданного значения критической интенсивности отказов. Приведены примеры для двух случаев критической интенсивности отказов оптического кабеля, характеризующей состояние деградации кабеля на последнем интервале времени эксплуатации. Построены зависимости процентного уменьшения интенсивности отказов участка при разных значениях критической интенсивности отказов.

V.P. Shuvalov, I.G. Kvitkova

ON THE PROBLEM OF REDUCING THE DEGRADATION FAILURE RATE UNDER CORRECTIVE MAINTENANCE

Siberian State University of Telecommunications and Informatics (SIBSUTIS),
Novosibirsk, Russia

Keywords: optical cable operation, an elementary section of an optical cable, degradation failure, local failure, replacement of a section, critical failure rate.

During the optical cable operation, failures occur, local or global, caused by various reasons. As a result, the damaged section of the cable can be replaced. The article considers the Markov model of the optical cable degradation process, which is used to assess the impact of replacing sections of optical cable on degradation processes due to local failures and a given value of the critical failure rate. Examples are given for two cases of critical failure rate of an optical cable characterizing the state of cable degradation at the last operating time interval. The dependences of the percentage reduction in the failure rate of the section at different values of the critical failure rate are constructed.

В процессе эксплуатации оптического кабеля происходят отказы, вызванные различными причинами. При этом появление отказа сопровождается заменой участка оптического кабеля (ОК), на котором произошел отказ. В процессе эксплуатации возможен ряд замен участков ОК. Вследствие деградации оптического кабеля, которая сопровождается накоплением повреждений [1], наступает время, когда от тактики замены участков следует перейти к замене ОК в целом вследствие его отказа, который назовем деградационным или глобальным отказом. Отказы, сопровождающиеся заменой (ремонтом) отдельных участков ОК, назовем локальными отказами.

Как правило, задача по замене оптического кабеля в целом решается путем вычисления времени γ-процентной вероятности отказа с учетом нагружения участков ОК [2, 3] или вычисления наступления времени некоторого, так называемого, критического отказа.

Критическое значение интенсивности отказов ОК задается для установленного значения времени эксплуатации кабеля и является характеристикой состояния деградации на последнем интервале гарантийного времени эксплуатации.

Одной из основных причин деградационных отказов является наличие микротрещин на поверхности оптоволокна [4, 5]. Глубина этих микротрещин со временем только растет, что приводит к снижению прочности оптоволокна [5, 6] и к росту интенсивности отказов. При этом сам процесс деградации моделируется марковским процессом чистой гибели [6, 7]. Используя для моделирования теорию марковских процессов, поставим задачу поиска в общем виде оценки влияния на деградационные процессы замены участков ОК вследствие локальных отказов и заданного значения критической интенсивности отказов.

В процессе эксплуатации оптического кабеля происходит процесс накопления повреждений, т.е. его деградация. Будем называть состоянием деградации количество накопленных повреждений. Повреждение – это событие, заключающееся в нарушении исправного состояния объекта при сохранении его работоспособного состояния. Под исправным состоянием понимется состояние объекта, при котором он соответствует все требованиям, установленным для него в документации. Исправный объект всегда работоспособен, неисправный объект может быть и работоспособным, и неработоспособным. Работоспособный объект может быть исправен и неисправен, неработоспособный объект всегда неисправен [8].

В процессе деградации способность обеспечивать передачу информации по оптическому кабелю со временем падает [9]. До наступления глобального отказа имеет место несколько локальных отказов и, соответственно, ремонтов ОК. Замену ОК в целом на новый следует производить, если ремонт ОК становится дороже, чем его замена. Таким образом, задача о времени замены ОК на новый является, в общем случае, технико-экономической задачей, которая в настоящее время, как правило, решается только как задача по вычислению γ-процентной вероятности отказа с учетом нагружения участков ОК. [2]

Спустя некоторое время интенсивность отказов ОК достигнет критического значения. Отказ любого участка при этом условии является глобальным и приводит к замене всего ОК в целом. Обоснование критического значения суммарной интенсивности отказов ОК должно производиться в рамках специального технико-экономического исследования.

Критическое значение интенсивности отказов ОК задаётся для установленного гарантийного времени эксплуатации ОК. Считается, что критическое значение интенсивности отказов является характеристикой состояния деградации на последнем интервале гарантийного времени эксплуатации ОК.

Пусть ОК состоит из N элементарных участков одинаковой длины $l_э$, которые находятся в одинаковых условиях эксплуатации. Время эксплуатации ОК разбито на интервалы (отрезки времени) одинаковой длины T. На каждом интервале времени каждый элементарный участок находится в некотором состоянии, характеристикой которого является интенсивность отказов. При переходе от i-го состоянии деградации к (i+1)-му состоянию происходит накопление повреждений, что характеризуется увеличением интенсивности отказов при переходе от i-го интервала времени к (i+1)-му.

Таким образом, характеристикой состояния деградации участка является интенсивность отказов. С накоплением повреждений растет интенсивность отказов. Отказ участка ОК может произойти в любом состоянии деградации. После отказа происходит замена элементарного участка кабеля на новый, и его эксплуатация на следующем интервале времени начинается с начального состояния деградации. Если на некотором интервале времени отказ не происходит, то на следующем интервале времени происходит переход в следующее состояние.

На каждом интервале времени ОК находится в некотором состоянии деградации, характеристикой которого является суммарная интенсивности отказов всех элементарных участков.

При формировании модели приняты следующие условия и допущения.

1. На одном интервале времени отказ любого участка в любом состоянии деградации может произойти только один раз.

2. Эксплуатация любого участка начинается с начального состояния деградации.

3. После замены кабеля на одном участке эксплуатация этого участка продолжается с начального состояния деградации.

4. Рост интенсивности отказов элементарного участка во времени происходит по линейному закону. [10]

С использованием приведенных условий можно описать процесс эксплуатации одного участка. Если на i-м интервале времени отказ (локальный отказ) не происходит, то происходит переход ОК в следующее состояние деградации на (i+1)-м интервале. Если на i-м интервале времени происходит отказ (локальный отказ) участка, то замена кабеля на новый производится только на этом участке, и эксплуатация этого участка продолжается на следующем интервале времени, начиная с начального состояния.

Диаграмма с пятью состояниями деградации, удовлетворяющая условиям модели, приведена на рис. 1. Данная диаграмма соответствует марковским моделям чистого размножения с переходом в поглощающие состояния при завершении гарантированного срока службы ОК.

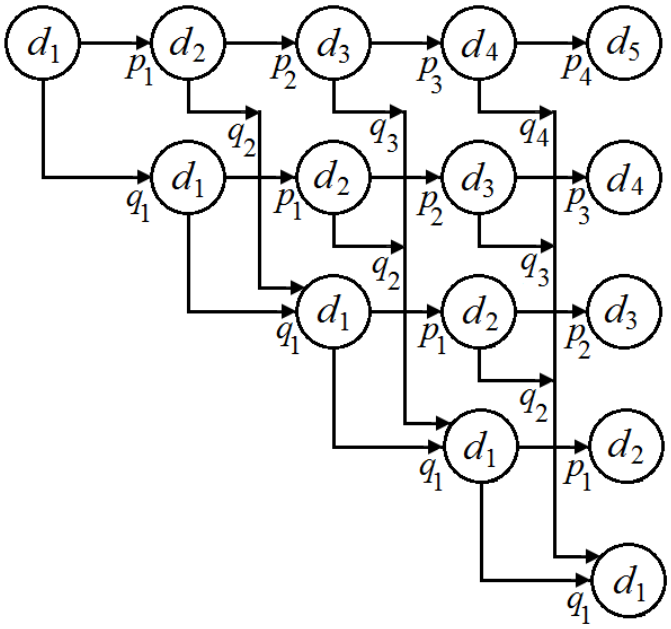


Рис. 1. Диаграмма состояний участка на пяти интервалах

На диаграмме рис.1 обозначено: d_i – состояние деградации участка, i = 1, 2,..., 5; d_1 – начальное состояние деградации одного участка; p_i – вероятность перехода между состояниями деградации $d_i \rightarrow d_{i+1}$, i = 1, 2,..., 4; q_i – вероятность перехода между состояниями деградации $d_i \rightarrow d_1$,i = 1, 2,..., 4.

Положим, что критическая интенсивность отказов всего ОК задана. В соответствии с принятыми условиями и допущениями вычисляются критическая интенсивность отказов одного участка ($\Lambda_{круч}$), интенсивность отказов (локальных отказов) участка в состоянии d_1 (λ_1) и d_i (λ_i):

$$\Lambda_{круч} = \Lambda_{кр} / N \ , \ \lambda_1 = \Lambda_{круч} / M \ , \ \lambda_i = i \cdot \lambda_1 \, , \qquad (1)$$

где $\Lambda_{кр}$ – критическая интенсивность отказов всего ОК;

N – число элементарных участков ОК;

M – число интервалов времени, на которое разбивается гарантированное время эксплуатации ОК.

Вероятность того, что состояние деградации d_i не изменится на интервале T, равна $p_i = \exp(-\lambda_i \cdot T)$, а вероятность изменения состояния в результате отказа $q_i = 1-\exp(-\lambda_i \cdot T)$. С вероятностью p_i происходит переход в следующее состояние деградации d_{i+1} на следующем интервале времени, а с вероятностью q_i происходит отказ (локальныый отказ) участка. Таким образом, переход на следующий интервал $d_i \rightarrow d_{i+1}$ происходит с вероятностью p_i, а переход $d_i \rightarrow d_1$ происходит с вероятностью q_i, i = 1, 2,..., M − 1. Поскольку при переходах между состояниями происходит накопление повреждений, то $\lambda_1 < \lambda_2 < ... < \lambda_M$.

Для посторения модели используется матричный метод [11]. Полагая $M = N = 5$, запишем матрицу переходных вероятностей между состояниями деградации на одном участке, соответстующую приведенной на рис. 1 диаграмме:

$$P = \begin{pmatrix} q_1 & p_1 & 0 & 0 & 0 \\ q_2 & 0 & p_2 & 0 & 0 \\ q_3 & 0 & 0 & p_3 & 0 \\ q_4 & 0 & 0 & 0 & p_4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Эксплуатация участка начинается с состояния d_1. Поэтому начальное распределение вероятностей состояний задается вектором $p(0)$ = (1 0 0 0 0). Распределение вероятностей состояний деградации на i-м интервале определяется по формуле:

$$p(i) = p(0)\cdot P^{i-1},\ i = 1, 2,..., M. \qquad (2)$$

Среднее значение интенсивности отказов на i-м интервале времени для участка вычисляется по формуле:

$$\lambda_{\text{ср}i} = p(i)\cdot\lambda = \sum_{j=1}^{M} p(i,j)\cdot\lambda_j, \qquad (3)$$

где $p(i)$ определяется из выражения (2);

λ - столбец интенсивностей отказов в состояниях деградации (элементами этого столбца являются интенсивности λ_i).

Параметр $\lambda_{\text{ср}i}$ из (3) характеризует изменение интенсивности отказов участка с учетом замены участка кабеля при локальных отказах.

Приведенные ниже примеры соответствуют диаграмме рис. 1. При этом приняты следующие исходные данные для расчетов: гарантийное время эксплуатации ОК $T_{\text{экс}}$ = 25 лет; N = 100; M = 5; T = 5 лет.

Рассмотрим два варианта процесса даградации участка. В первом варианте примем $\Lambda_{\text{кр}}$ = 1 1/год, а во втором варианте – $\Lambda_{\text{кр}}$ = 1 1/мес. Все вычисления проведены в единицах интенсивности отказов 1/час. Параметры этих исходных вариантов приведены в таблице 1. Результаты вычислений для этих вариантов приведены в таблицах 2 и 3.

Таблица 1. Исходные данные для числовых примеров

Параметр	Первый вариант	Второй вариант
$\Lambda_{\text{кр}}$	1 1/год = $1{,}142\cdot10^{-4}$ 1/час	1 1/мес = $1{,}366\cdot10^{-3}$ 1/час
$\Lambda_{\text{круч}} = \Lambda_{\text{кр}} / N$	$1{,}142\cdot10^{-6}$ 1/час	$1{,}366\cdot10^{-5}$ 1/час
$\lambda_1 = \Lambda_{\text{круч}} / M$	$2{,}283\cdot10^{-7}$ 1/час	$2{,}732\cdot10^{-6}$ 1/час
T	5 лет = $4{,}380\cdot10^{4}$ час	

Таблица 2. Результаты вычислений для первого варианта ($\Lambda_{\text{кр}}$ = 1/год)

i	λ_i(1/час)	p_i	q_i	$p(i)$	$\lambda_{\text{ср}i}$	ρ_i
1	$2{,}283\cdot10^{-7}$	0,990	0,010	(1 0 0 0 0)	$2{,}283\cdot10^{-7}$	100,0
2	$4{,}566\cdot10^{-7}$	0,980	0,020	(0,010 0,990 0 0 0)	$4{,}543\cdot10^{-7}$	99,5
3	$6{,}849\cdot10^{-7}$	0,970	0,030	(0,020 0,010 0,970 0 0)	$6{,}737\cdot10^{-7}$	98,4
4	$9{,}132\cdot10^{-7}$	0,961	0,039	(0,029 0,020 0,009 0,942 0)	$8{,}822\cdot10^{-7}$	96,6
5	$1{,}141\cdot10^{-6}$	0,951	0,049	(0,038 0,029 0,019 0,009 0,905)	$1{,}076\cdot10^{-7}$	94,3

Таблица 3. Результаты вычислений для второго варианта ($\Lambda_{\text{кр}}$ = 1/мес)

i	λ_i(1/час)	p_i	q_i	$p(i)$	$\lambda_{\text{ср}i}$	ρ_i
1	$2{,}732\cdot10^{-6}$	0,887	0,113	(1 0 0 0 0)	$2{,}732\cdot10^{-7}$	100,0
2	$5{,}464\cdot10^{-6}$	0,787	0,213	(0,113 0,887 0 0 0)	$5{,}156\cdot10^{-7}$	94,4
3	$8{,}197\cdot10^{-6}$	0,698	0,302	(0,202 0,100 0,698 0 0)	$6{,}822\cdot10^{-7}$	83,2
4	$1{,}093\cdot10^{-5}$	0,620	0,380	(0,255 0,179 0,079 0,488 0)	$7{,}649\cdot10^{-7}$	70,0
5	$1{,}366\cdot10^{-5}$	0,550	0,450	(0,276 0,226 0,141 0,055 0,302)	$7{,}872\cdot10^{-7}$	57,6

В таблицах 2 и 3 принято $\rho_i = (\lambda_{cpi} / \lambda_i)\cdot 100\%$ – процентное отношение между указанными интенсивностями, причем λ_i определяется из (1).

По результатам расчетов построен график зависимости процентного уменьшения интенсивности отказов участка при разных значениях критической интенсивности отказов.

На рис. 2 представлены графики трех вариантов процесса деградации: I – отказ устраняется путем ремонта на интервале времени, на котором он возник, без замены кабеля; II – замена кабеля после отказа при $\Lambda_{кр}$ = 1 1/год; III – замена кабеля после отказа при $\Lambda_{кр}$ = 1 1/мес.

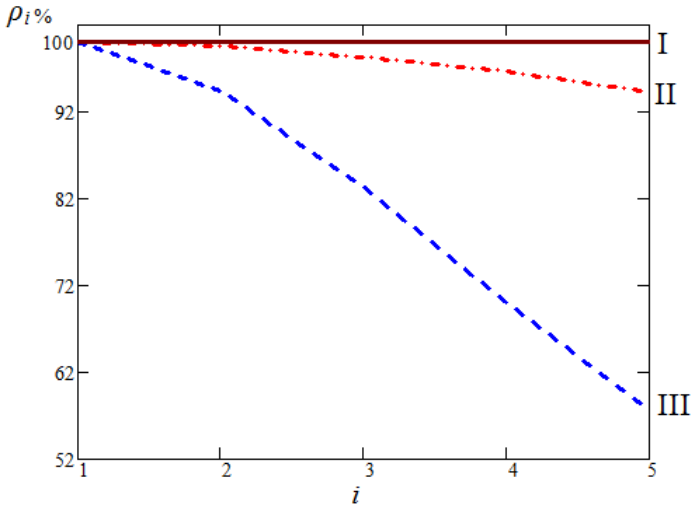


Рис.2. Процентное уменьшение интенсивности отказов участка при разных значениях критической интенсивности отказов

Из приведенной модели следует, что при любом конечном значении критической интенсивности отказов ОК имеет место снижение интенсивности глобальных отказов. При этом, чем больше критическая интенсивность отказов, тем сильнее проявляется это снижение. При определенном значении критической интенсивности отказов снижение может быть существенным. Так, при критической интенсивности отказов 1 1/мес снижение достигает 57,6%. Это явление можно назвать замедлением роста суммарной интенсивность отказов ОК, обусловленная применяемым методом технического обслуживания с заменой отказавшего элементарного участка ОК.

Фактор замедления роста суммарной интенсивности отказов ОК можно учитывать при проектировании ОК и при планировании его эксплуатации, в частности, такой подход позволяет обоснованно повысить гарантийный срок эксплуатации ОК.

В данной работе рассмотрена упрощенная модель процесса деградации с заменой после отказов элементарных участков одинаковой длины. Возможны более сложные варианты условий, например, участки могут быть разной длины, они могут находиться в разных условиях эксплуатации и т.д.

СПИСОК ЛИТЕРАТУРЫ:

1. Paris P.C., Erdogan F. A critical analysis of crack propagation laws. // Journal of Basic engineering, 1963. - Vol. 8. - P. 528-533.
2. Сценарии прогноза срока службы оптического волокна в КЛС / В. Андреев, В. Бурдин, А. Нижегородов // Первая миля, 2020. - № 4. - С. 34-42.
3. Цым А.Ю. Сроки службы оптических кабелей. Анализы. Риски // Кабели и провода, 2020. – № 2 (382). - С. 20-26.
4. Овчинникова И.А. Исследование и разработка оптических кабелей специального назначения. Диссертация на соискание ученой степени доктора технических наук. - Москва, ВНИИКП, 2021.
5. Matthewson M.J., Strength probability time diagrams using power law and exponential kinetics models for fatigue. // Proceedings of SPIE, 2006. – Vol. 6193. – P. 619301 - 11.
6. Bogdanoff J.L. A new cumulative damage model, part 1. // Journal of applied mechanics, 1978. – Vol. 45. – P. 246-250.

7. Рахман П. А. Марковская цепь гибели и размножения в моделях надежности технических систем. / П.А. Рахман, А. И. Каяшев, М.И. Шарипов // Вестник УГАТУ. - 2015. - Т. 19. - №1 (67). - С.140-154.
8. ГОСТ 27.102-2021. Надежность в технике: надежность объекта. Термины и определения. - М.: Российский институт стандартизации, 2021. - 36 с.
9. Aging and degradation of optical fiber parameters in a 16-year-long period of usage / A. Maslo, M. Hodzic, E. Skaljo, A. Mujcic // Fiber and Integrated Optics. - Feb., 2020. - Vol. 39. - № 1. - P. 39-52.
10. Initial Probability Distribution in Markov Chain Model for Fatigue Crack Growth Problem / S.S. Januri, Z.M. Nopiah, A.K. Ariffin Mohd Ihsan, N. Masseran, S. Abdullah. // International Journal of Engineering & Technology. – September, 2018. - Vol.7. - №. 3. - P. 136-139
11. Зеленцов Б.П. Матричные методы моделирования однородных марковских процессов. – Palmarium Academic Publishing, 2017. – 133 с.

И.В. Шульга

РАЗВИТИЕ СЕТИ СВЯЗИ НА ПРИМЕРЕ ОБОРУДОВАНИЯ АО «ИСКРАУРАЛТЕЛ»

ОА «ИскраУралТЕЛ», г. Екатеринбург, Россия

Ключевые слова: ICP, IMS, 5G, построение сети

В статье рассматривает основные тенденции развития сети связи на примере реализованных проектов компании ОА «ИскраУралТЕЛ». Приводится описание решений, которые используется для построения телекоммуникационных сетей и сервисов, предоставления широкополосного абонентского доступа, решений для предприятий и ведомств, цифровые сервисы городского управления.

I.V. Shulga

DEVELOPMENT OF THE COMMUNICATION NETWORK ON THE EXAMPLE OF THE EQUIPMENT OF JSC «ISKRAURALTEL»

OA "IskraUralTEL", Yekaterinburg, Russia

Keywords: ICP, IMS, 5G, network building

The article examines the main trends in the development of a communication network on the example of implemented projects of the company OA "IskraUralTEL". A description of the solutions that are used to build telecommunication networks and services, provide broadband subscriber access, solutions for enterprises and departments, digital services for city government is given.

Для классификации основных решений и тенденций в области связи определим основные направления, в рамках которых осуществляется модернизация сетевой инфраструктуры:

– телекоммуникации;
– абонентский широкополосный доступ;
– решения для ведомственных сетей и предприятий;
–сервисы городского управления.

Рисунок 1 – Голосовые коммуникации на базе NGN и IMS технологий

В области телекоммуникаций в настоящее время происходят самые значительные изменения на сети общего пользования. В последние годы голосовое ядро сети строится на базе технологии IMS (IP Multimedia Subsystem), постепенно вытесняя технологию NGN (New Generation Networks). Важно отметить, что обе технологии, IMS и NGN, являются технологиями VoIP, таким образом сеть связи переходит на пакетную передачу данных. Несмотря на это, на сети еще много оборудования, которое поддерживает еще более старые технологи, базирующееся на плезиохронной цифровой иерархии. Таким образом, решения IMS и NGN поддерживают возможность совместной работы с существующими сетями через сигнальные шлюзы, постепенно осуществляя переход к сетям пакетной коммутации (стек протоколов TCP/IP) [1].

Следующим важным моментом при построении голосового ядра является переход от решений на базе аппаратного обеспечения (hardware) на платформы виртуализации и, далее, на облачные решения. В настоящее время на базе облачных решений реализуется не только голосовое ядро оператора, а практически вся инфраструктура. Частное облако включает себя телефонию, диспетчерскую связь, системы управления бизнес-процессами и бухгалтерского учета, сервера почты, баз данных и любые другие цифровые решения.

Переход к технологии IMS позволяет реализовать одну из востребованных услуг для телефонии – FMC (Fixed Mobile Convergence). Технология позволяет объединить фиксированных и мобильных абонентов, что позволит предоставить им единых номер и позволит управлять устройствами и услугами абонента через единый портал администратора [2].

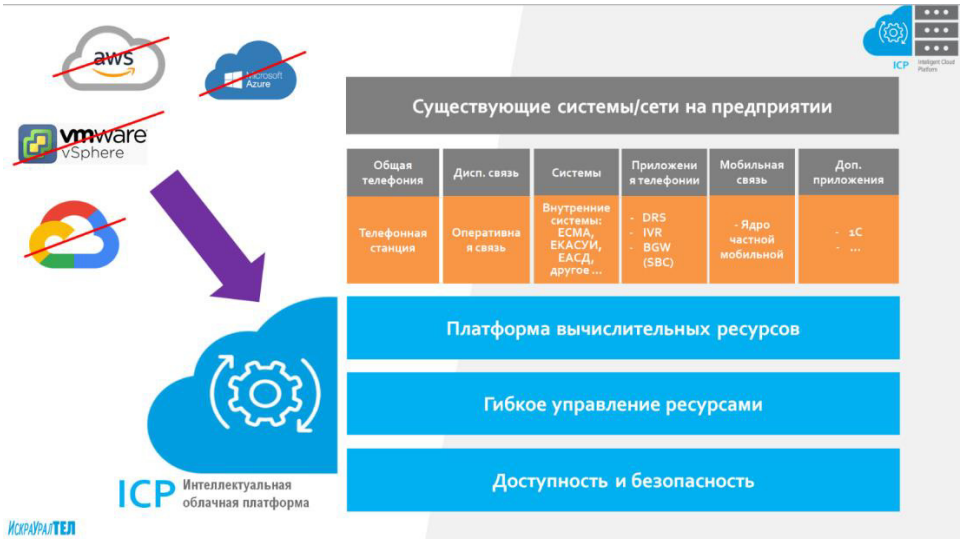


Рисунок 2 – Интеллектуальная облачная платформа

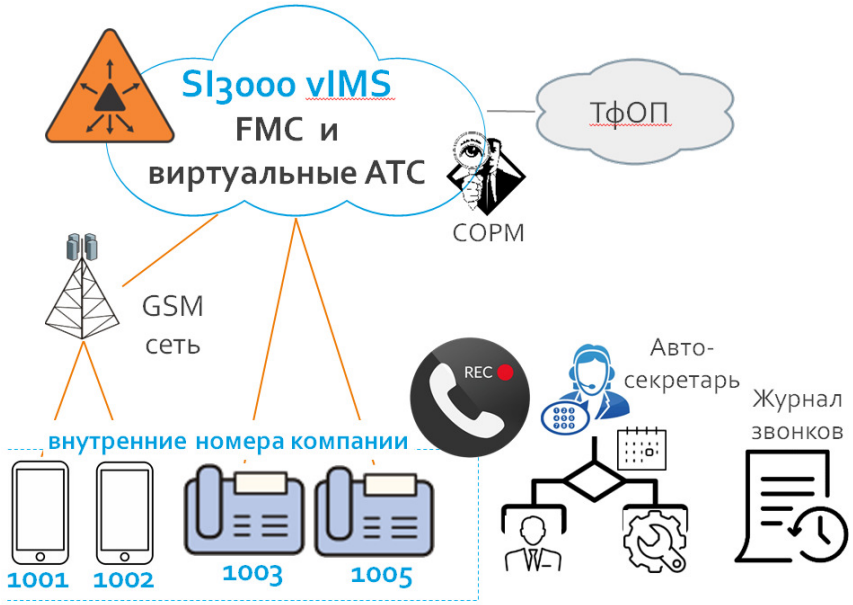


Рисунок 3 – Корпоративная связь и FMC

Следующее направление – это широкополосный абонентский доступ. Современная абонентская сеть стоится на базе технологии пассивной оптической сети GPON. Оператор устанавливает блок OLT (Optical Line Terminal), на стороне абонента устанавливаются оптические оконечные модемы (ONT, Optical Network Terminal). Технология поддерживает ветвления сети через оптические сплиттеры, что делает ее выгодной для провайдера услуг.

Рисунок 4 – Пример секции OLT Lumia SI3000

Далее рассмотрим решения для ведомственных сетей и предприятий. Особенность этих сетей в том, что они сохранили свою существующую архитектуру сети и оборудования, таким образом решения в этой области должны поддерживать ряд специфических, как правило аналоговых, протоколов и ведомственных сигнализаций. Кроме того, в такие сети часто интегрировано оборудования конференций, диспетчерской связи, оповещений и другого специфического оборудования. Практически любая модернизация оборудования должна поддерживать уже имеющуюся архитектуру.

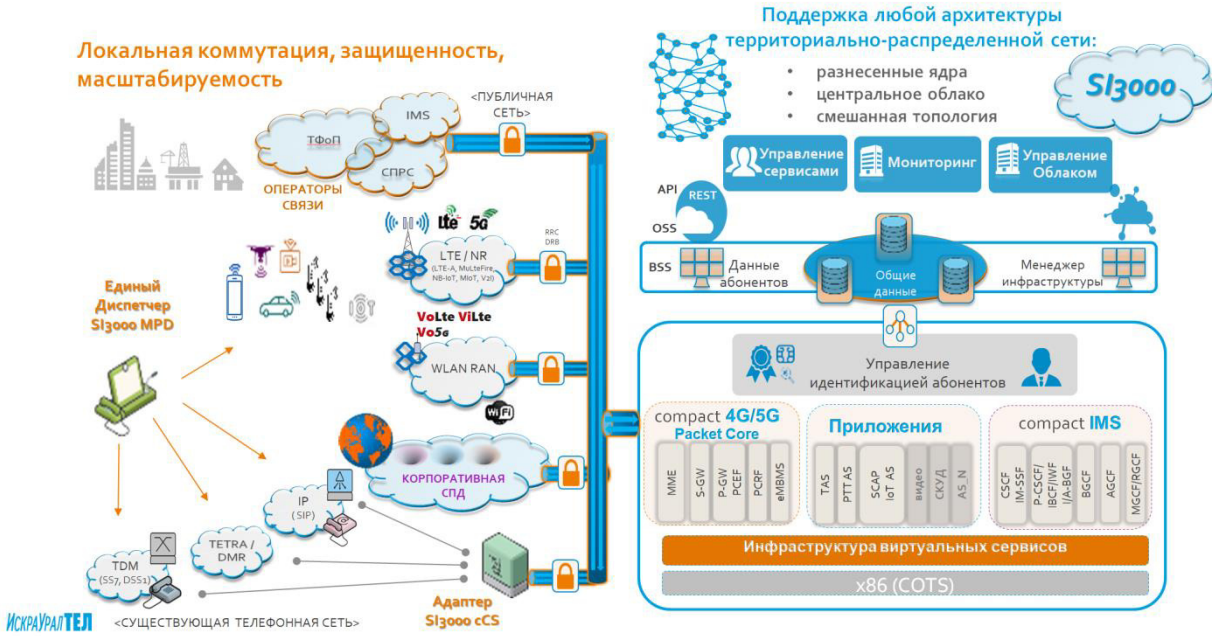


Рисунок 5 – Единая технологическая сеть предприятия

Кроме абонентских услуг важным направлением являются продукты и решения построения Умного города (Smart City). В это решение входит организация единых номеров 112 (единый номер вызова экстренных оперативных служб) и 122 (единый номер для всех регионов РФ по вопросам COVID-19 и вызова врача на дом) на базе сети общего пользования, а также ряд функциональных сервисов городских услуг [3].

Рисунок 6 – Продукты и решения Умного города

СПИСОК ЛИТЕРАТУРЫ:

1. Rebecca Copeland Converging NGN Wireline and Mobile 3G Networks with IMS. - 1 изд. - Taylor & Francis Group, LLC, 2009. - 511 с.
2. Arun Handa System Engineering for IMS Networks. - 1 изд. - USA: Elsevier Inc, 2009. - 340 с.
3. Gonzalo Camarillo, Miguel A. Garc´ıa-Mart´ın The 3G IP Multimedia Subsystem (IMS). - 3-е изд. - UK: A John Wiley and Sons, 2009. - 655 с.

Секция 2. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Е.В. Агаркова, Д.В. Мирошниченко, О.А. Сафарьян

GRPC: СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМЫ УДАЛЕННОГО ВЫЗОВА ПРОЦЕДУР

Донской государственный технический университет в г. Ростов-на-Дону (ДГТУ), Россия

Ключевые слова: gRPC, REST, RESTful API, клиент-серверное приложение, система удаленного вызова процедур.

В статье приведены архитектуры построения API, описан сетевой протокол gRPC, выделены достоинства и недостатки использования выбранных технологий для реализации модели клиент-сервер. Цель работы заключается в проведении сравнительного анализа система удаленного вызова процедур gRPC и возможностями, предоставляемыми интерфейсом прикладного программирования (API).

E.V. Agarkova, D.V. Miroshnichenko, O.A. Safaryan

GRPC: COMPARATIVE ANALYSIS OF THE REMOTE PROCEDURE CALL SYSTEM

Don State Technical University in Rostov-on-Don (DSTU), Russia

Keywords: gRPC, REST, RESTful API, client-server application, remote procedure call system.

The article presents the architecture of API construction, describes the gRPC network protocol, highlights the advantages and disadvantages of using the selected technologies to implement the client-server model. The purpose of the work is to conduct a comparative analysis of the gRPC remote procedure call system and the capabilities provided by the application programming interface (API).

В современном мире связь между приложениями важна как никогда. В связи с быстрым развитием микросервисов и распределенных систем идет постоянный поиск эффективных, надежных и масштабируемых способов взаимодействия приложений друг с другом.

Application Programming Interface (API) — это интерфейсы прикладного программирования. Эти интерфейсы служат программным посредником, который устанавливает определенные определения и правила для приложений, чтобы взаимодействовать и общаться друг с другом. API отвечает за доставку ответа от пользователя в систему, который, в свою очередь, отправляется обратно из системы пользователю.

API определяет типы запросов, которые одно приложение (веб-страница или мобильное приложение) может отправлять другому, а также устанавливает: как делать эти запросы, какие форматы данных использовать, и практики, которым должны следовать пользователи.

С одной стороны, в монолитном приложении все функциональные возможности проекта включены в единый блок, точнее, в единую кодовую базу. С другой стороны, микросервисная архитектура включает в себя несколько небольших сервисов, которые взаимодействуют друг с другом с помощью таких протоколов, как HTTP. Службы-компоненты, являющиеся частью архитектуры микрослужб, взаимодействуют друг с другом через API. Другими словами, API-интерфейсы позволяют всем службам, интегрированным в микросервисное приложение, подключаться и обмениваться данными.

Наиболее часто используемый архитектурный стиль — REST API. Однако при построении API есть три основные модели: RPC (удаленный вызов процедур), REST (передача репрезентативного состояния) и GraphQL . В этой статье мы остановимся на первых двух.

RPC использует модель клиент-сервер. Запрашивающий сервер (другими словами, клиент) запрашивает сообщение, которое преобразуется RPC и отправляется на другой сервер. Как только сервер получает запрос, он отправляет ответ обратно клиенту. Пока сервер обрабатывает этот вызов, клиент блокируется, а внутреннее сообщение, проходящее внутри серверов, скрыто.

Кроме того, RPC позволяет клиенту запрашивать функцию в определенном формате и получать ответ в точно таком же формате. Тем не менее, метод отправки вызова с помощью RPC API находится в URL-адресе. RPC поддерживает удаленные вызовы процедур как в локальной, так и в распределенной среде.

gRPC был разработан Google как высокопроизводительная среда удаленного вызова процедур (RPC). Он основан на более раннем проекте Stubby, который представлял собой внутреннюю систему RPC Google. gRPC был открыт в 2015 году и с тех пор завоевал значительную популярность в сообществе разработчиков программного обеспечения.

gRPC означает удаленный вызов процедур Google и представляет собой вариант, основанный на архитектуре RPC. Эта технология соответствует реализации API RPC, использующей протокол HTTP 2.0, но HTTP не предоставляется ни разработчику API, ни серверу. Следовательно, нет необходимости беспокоиться о том, как концепции RPC сопоставляются с HTTP, что снижает сложность.

В целом gRPC направлен на ускорение передачи данных между микросервисами. Он основан на подходе к определению службы, установлению методов и соответствующих параметров для обеспечения удаленного вызова и типов возврата.

Более того, он выражает модель API RPC на языке IDL (язык описания интерфейса), который предлагает более прямое определение удаленных процедур. По умолчанию IDL использует буферы протоколов (но также доступны и другие альтернативы) для описания интерфейса службы, а также структуры сообщений полезной нагрузки.

RESTful API был представлен Роем Филдингом в его докторской диссертации 2000 года и стал стандартом де-факто для веб-API. REST, что означает Representational State Transfer, представляет собой архитектурный стиль, предоставляющий рекомендации по проектированию сетевых приложений.

gRPC использует HTTP/2 в качестве транспортного протокола, что обеспечивает эффективную передачу двоичных данных, сжатие заголовков и мультиплексирование нескольких вызовов по одному соединению. gRPC использует протокольные буферы в качестве языка определения интерфейса (IDL) и формата сериализации, обеспечивая строго типизированный, эффективный и компактный обмен сообщениями.

RESTful API использует HTTP/1.1, хотя можно использовать и HTTP/2. REST использует стандартные методы HTTP (GET, POST, PUT, DELETE) для связи, а данные можно обменивать в различных форматах, таких как JSON, XML или обычный текст. Выбор формата данных зависит от конкретной реализации и требований клиента.

Рассмотрим основные различия между gRPC и REST.

API-интерфейсы REST следуют модели связи запрос-ответ, которая обычно построена на HTTP 1.1. Это означает, что, если микросервис получает несколько запросов от нескольких клиентов, модель должна обрабатывать каждый запрос за раз, что, следовательно, замедляет работу всей системы. Однако API REST также могут быть построены на HTTP 2, но модель связи запрос-ответ остается прежней, что не позволяет API REST максимально использовать преимущества HTTP 2, такие как потоковая связь и двунаправленная поддержка.

gRPC не сталкивается с подобным препятствием. Он основан на HTTP 2 и вместо этого следует модели связи «клиент-ответ». Эти условия поддерживают двустороннюю связь и потоковую передачу благодаря способности gRPC получать несколько запросов от нескольких клиентов и обрабатывать эти запросы одновременно, постоянно передавая информацию. Кроме того, gRPC также может обрабатывать «унарные» взаимодействия, подобные тем, которые построены на HTTP 1.1.

Таким образом, gRPC может обрабатывать унарные взаимодействия и различные типы потоковой передачи:

1. Унарный: когда клиент отправляет один запрос и получает один ответ.

2. Server-streaming: когда сервер отвечает потоком сообщений на запрос клиента. После отправки всех данных сервер дополнительно отправляет сообщение о состоянии для завершения процесса.

3. Клиентская потоковая передача: когда клиент отправляет поток сообщений и, в свою очередь, получает одно ответное сообщение от сервера.

4. Двунаправленная потоковая передача: два потока (клиент и сервер) независимы, что означает, что они оба могут передавать сообщения в любом порядке. Клиент — это тот, кто инициирует и завершает двунаправленную потоковую передачу.

Поддержка браузером является одним из основных преимуществ REST API по сравнению с gRPC. С одной стороны, REST полностью поддерживается всеми браузерами. С другой стороны, gRPC по-прежнему весьма ограничен, когда речь идет о поддержке браузеров. К сожалению, для выполнения преобразований между HTTP 1.1 и HTTP 2 требуется gRPC-web и прокси-уровень. Таким образом, gRPC в основном используется для внутренних/частных систем (программы API в рамках серверных данных конкретной организации и функциональности приложений).

gRPC по умолчанию использует протокольный буфер для сериализации данных полезной нагрузки. Это решение легче, так как оно обеспечивает сильно сжатый формат и уменьшает размер сообщений. Кроме того, Protobuf (или Protocol Buffer) является двоичным. Ттаким образом, он сериализует и десериализует структурированные данные для их связи и передачи. Другими словами, строго типизированные сообщения могут быть автоматически преобразованы из Protobuf в язык программирования клиента и сервера.

Напротив, REST в основном использует форматы JSON или XML для отправки и получения данных. На самом деле, даже несмотря на то, что он не требует какой-либо структуры, JSON является наиболее популярным форматом из-за его гибкости и способности отправлять динамические данные без обязательного следования строгой структуре. Еще одним значительным преимуществом использования JSON является уровень удобочитаемости, с которым Protobuf пока не может конкурировать.

Тем не менее, JSON не такой легкий и быстрый, когда речь идет о передаче данных. Причина этого заключается в том, что при использовании REST JSON (или другие форматы) необходимо сериализовать и превратить в язык программирования, используемый как на стороне клиента, так и на стороне сервера. Это добавляет дополнительный шаг к процессу передачи данных, который, следовательно, может снизить производительность и открыть возможность для ошибок.

В отличие от gRPC, REST API не предоставляет встроенных функций генерации кода, а это означает, что разработчики должны использовать сторонний инструмент, такой как Swagger или Postman, для создания кода для запросов API.

Напротив, gRPC имеет собственные функции генерации кода благодаря компилятору protoc, который совместим с несколькими языками программирования. Это особенно полезно для систем микросервисов , которые интегрируют различные сервисы, разработанные на разных языках и платформах. В целом, встроенный генератор кода также облегчает создание SDK (Software Development Kit).

Также рассмотрим варианты использования данных технологий, чтобы понять, насколько универсальной является каждая из них.

Преимущества использования gRPC:

1. Высокопроизводительная связь: двоичный протокол gRPC и поддержка HTTP/2 делают его отличным выбором для связи между службами с малой задержкой и высокой пропускной способностью. gRPC может обрабатывать тысячи одновременных подключений и обеспечивает быструю сериализацию и десериализацию.

2. Контракты со строгой типизацией. С помощью gRPC вы определяете интерфейсы служб и структуры сообщений с помощью буферов протоколов. Это обеспечивает соблюдение строгих контрактов между клиентом и сервером, снижая вероятность ошибок из-за недопонимания или изменения формата данных.

3. Поддержка потоковой передачи: gRPC изначально поддерживает двунаправленную потоковую передачу, что обеспечивает связь и обработку данных между службами в режиме реального времени.

4. Независимость от языка: gRPC поддерживает генерацию кода для множества языков программирования, что упрощает интеграцию с различными службами и платформами.

Преимущества использования RESTful API:

1. Совместимость с веб-клиентом: веб-браузеры изначально поддерживают RESTful API, что делает их идеальным выбором для взаимодействия клиент-сервер в веб-приложениях.

2. Удобочитаемые форматы данных: API-интерфейсы RESTful часто используют JSON или XML в качестве форматов данных, которые более удобочитаемы, чем двоичные форматы, такие как протокольные буферы.

3. Кэширование: API-интерфейсы RESTful могут использовать механизмы кэширования HTTP, которые могут помочь снизить нагрузку на серверы и улучшить время отклика.

4. Упрощение отладки и тестирования: RESTful API, как правило, легче отлаживать и тестировать из-за их простоты, широкой поддержки инструментов и возможности использовать стандартные инструменты, такие как curl или Postman, для взаимодействия с API.

Подводя итог можно сказать, что gRPC, также как и RESTful API имеет свои уникальные преимущества и подходит для разных сценариев. gRPC отличается высокой производительностью, строгой типизацией и взаимодействием между службами в режиме реального времени, в то время как RESTful API больше подходит для взаимодействия между веб-клиентом и сервером, кэширования и удобочитаемых форматов данных.

При выборе между API gRPC и RESTful важно оценить ваш конкретный вариант использования и требования. Имейте в виду, что вы можете использовать обе технологии в одном проекте для удовлетворения различных потребностей. Например, вы можете использовать gRPC для эффективной связи между микросервисами и RESTful API для интерфейсов веб-приложений.

Таким образом, API-интерфейсы gRPC и RESTful — это мощные инструменты в арсенале разработчика, каждый из которых предлагает уникальные преимущества. Понимая их сильные стороны, ограничения и соответствующие варианты использования, можно принимать обоснованные решения и создавать масштабируемые, эффективные и удобные в сопровождении приложения, отвечающие вашим конкретным потребностям.

СПИСОК ЛИТЕРАТУРЫ:

1. Индрасири, К. gRPC: запуск и эксплуатация облачных приложений. Go и Java для Docker и Kubernetes : практическое руководство / К. Индрасири, Д. Курупу. - Санкт-Петербург : Питер, 2021. - 224 с. - (Серия «Бестселлеры O’Reilly»). - ISBN 978-5-4461-1737-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1733695.
2. Официальная документация gRPC [Электронный ресурс]. – Режим доступа: https://grpc.io/docs/what-is-grpc/.
3. Аквино, К. Front-end. Клиентская разработка для профессионалов. Node.js, ES6, REST : практическое руководство / К. Аквино, Т. Ганди. - Санкт-Петербург : Питер, 2017. - 512 с. - (Серия «Для профессионалов»). - ISBN 978-5-496-02930-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1739586.
4. gRPC и REST: как gRPC сравнивается с традиционными REST API [Электронный ресурс]. – Режим доступа: https://blog.dreamfactory.com/grpc-vs-rest-how-does-grpc-compare-with-traditional-rest-apis/.

Е.А. Фаляева, К.Ф. Мубаракшина

АНАЛИЗ НОВЫХ СИСТЕМ ОБНАРУЖЕНИЯ МЕСТОПОЛОЖЕНИЯ ПОЕЗДА. ТЕНДЕНЦИИ И РАЗВИТИЕ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный университет путей сообщения», г. Екатеринбург, Россия

Научный руководитель:
ассистент кафедры «Автоматика, телемеханика и связь на ж. д. транспорте» Ю. В. Могильников

Ключевые слова: системы обнаружения местоположения поезда, базовые станции, системы глобального позиционирования, система радиоориентации, использование искусственного интеллекта.

В данной научной статье рассмотрены системы для обеспечения безопасности движения поездов, проанализированы системы обнаружения местоположения поезда, базовые станции, системы глобального позиционирования, система радиоориентации, использование искусственного интеллекта. В результате сравнения выделена необходимость развития современных систем обнаружения местоположения поезда, их интеграция и использование искусственного интеллекта для обработки и анализа данных.

E.A. Falyaeva, K.F. Mubarakshina

ANALYSIS OF NEW TRAIN LOCATION DETECTION SYSTEMS. TRENDS AND DEVELOPMENT

Federal State Budgetary Educational Institution of Higher Education "Ural State University of Railway Transport", Yekaterinburg, Russia

Scientific director:
assistant of the department “Automation, telemechanics and communication on the railway transport"
Yu. V. Mogilnikov

Keywords: train location detection systems, base stations, global positioning systems, radio orientation system, use of artificial intelligence.

In this scientific article, systems for ensuring the safety and efficiency of train traffic are considered, train location detection systems, base stations, global positioning systems, a radio orientation system, and the use of artificial intelligence are analyzed. As a result of the comparison, the need for the development of modern train location detection systems, their integration and the use of artificial intelligence for data processing and analysis is highlighted.

Обеспечение безопасности движения поездов, максимально быстрое формирование составов, осуществление перевозок и своевременность доставки пассажиров и грузов – это ключевые задачи транспортных компаний и железнодорожных операторов. Разработка технологических инноваций, повышение точности и надежности оценки местоположения поездов – это главные перспективные направления развития железнодорожного транспорта. В последние годы наблюдается бурное развитие новых систем, ориентированных на повышения точности определения местоположения поезда в режиме реального времени. Цель данной статьи – проанализировать особенности новых систем обнаружения местоположения поезда и определить тенденции их развития.

На железнодорожном транспорте применяют различные способы обнаружения местоположения поезда [1]. Один из наиболее распространенных методов – использование базовых станций, которые закреплены на железнодорожных путях. Базовые станции получают данные о положении поезда из спутниковых систем и передают эти данные в центр управления движением. Однако, системы на основе базовых станций требуют больших затрат на установку и эксплуатацию. Кроме того, они не обеспечивают доступность данных по местоположению поезда в режиме реального времени, особенно в местах с плохой связью.

В настоящее время широко распространены новые системы глобального позиционирования (GPS), которые обеспечивают точное определение местоположения поезда. Системы на основе GPS позволяют получить информацию о местоположении поезда в режиме реального времени и даже в местах с плохой связью [2]. Также, существуют такие технологии позиционирования объекта «ГЛОНАСС», имеющие возможность довольно точно определять местоположение, но в этом случае стоит вопрос киберзащищенности, существуют технологии определения местоположения поезда на основе датчиков счета осей, но возникает проблема отсутствия контроля целостности рельсов (не выполняется контрольный режим) [3].

Также, в последние годы были разработаны новые методы и технологии по обработке и анализу данных, что позволяет существенно улучшить точность и надежность измерения местоположения поезда [4].

Одним из новых подходов является использование системы инерционной навигации (INS). Система INS основана на использовании акселерометров и гироскопов для определения ускорения и угловых скоростей транспортного средства [5]. Эта информация затем используется для определения местоположения поезда. Система INS является более точной и надежной, чем системы на основе базовых станций или GPS, и может обеспечивать высокую точность в режиме реального времени. Однако, система INS требует большой частоты обновления параметров и может иметь ограниченную доступность данных в некоторых местах.

Другой новой системой является система радиоориентации (RFID), которая использует радио-трансмиттеры для отправки информации о местоположении поезда. Высокочастотные RFID трансмиттеры устанавливаются на поездах и на железнодорожных путях. Автоматические системы идентификации поездов (АТС) используют данные из трансмиттеров для определения местоположения поезда и контроля за его движением. Преимуществом системы RFID является высокая точность и надежность измерения местоположения поезда, а также возможность обеспечить доступность данных в режиме реального времени.

С каждым днём увеличивается тенденция развития систем обнаружения местоположения поезда, а также контроля занятости и свободности участков. Связано это с тем, что существующие системы обнаружения местоположения поезда на основе рельсовых цепей морально устарели и имеют ряд недостатков, связанных с их обслуживанием. Более того, они подвержены влиянию асимметрии тягового тока, особенно при тяжеловесном движении поездов и подвергаются тяжелым климатическим условиям [6]. Для корректной работы необходим постоянный контроль РЦ на наличие явных, а также скрытых дефектов [7].

Развитие систем обнаружения местоположения поезда ориентировано на повышение точности и надежности измерения местоположения поезда, а также на обеспечение доступности данных в режиме реального времени. Одной из направляющих тенденций является интеграция различных систем, таких как GPS, INS, RFID и базовые станции. Такая интеграция может обеспечить высокую точность и доступность данных в режиме реального времени, поскольку стремительное развитие высокоскоростного движения требует увеличения частоты (уменьшение времени) обновления информации о местоположении поезда [8].

Другой тенденцией развития систем обнаружения местоположения поезда является использование искусственного интеллекта и автоматического обучения для обработки и анализа больших объемов данных. Использование алгоритмов машинного обучения может позволить автоматически анализировать данные о перемещении поездов, чтобы улучшить точность и надежность измерения местоположения. Мониторинг позволит облегчить внедрение системы беспилотных технологий, что является ещё одним актуальным направлением развития железнодорожного транспорта.

В заключении, можно сделать вывод, что новые системы обнаружения местоположения поезда, такие как INS, RFID и интеграция с GPS и базовыми станциями, становятся все более актуальными в железнодорожной отрасли. Эти системы обеспечивают высокую точность и надежность определения местоположения поезда, а также доступность данных в режиме реального времени. Тенденцией развития таких систем является интеграция различных систем определения местоположения поезда и использование искусственного интеллекта для обработки и анализа данных.

СПИСОК ЛИТЕРАТУРЫ:

1. О развитии возможностей RFID-систем [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/o-razvitii-vozmozhnostey-rfid-sistem.
2. Направления развития спутникового мониторинга железнодорожного транспорта [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/napravleniya-razvitiya-sputnikovogo-monitoringa-zheleznodorozhnogo-transporta
3. Вершинин И. Д., Миклин С. А., Могильников Ю. В. Внедрение беспилотных технологий на железнодорожном транспорте, как фактор повышения безопасности перевозочного процесса// Сборник научных трудов VII Всероссийской научно-практической конференции: Информационные технологии и когнитивная электросвязь. Екатеринбург, 2021. с. 74-78
4. Способ определения местоположения поезда по инфраструктуре железнодорожного пути в режиме реального времени, Головин В. И., Наговицын В. С., Калмыков А. А.
5. Селиванова Л.М., Шевцова Е.В. Инерциальные навигационные системы: учеб. пособие. – Ч. 1: Одноканальные инерциальные навигационные системы – М.: Издательство МГТУ им. Н.Э. Баумана, 2012. – 46 с.
6. Патент на изобретение № RU 2747818, 13.04.2023. Заявка № 2020121646 от 25.06.2020.
7. Могильников Ю. В. Влияние тяжеловесных поездов на работу рельсовых цепей и аппаратуры АЛСН //Транспорт Урала – 2014. - № 2(41) – с. 109-113
8. Могильников Ю. В. Оценка эффективности рельсовых цепей и средств дефектоскопии при выявлении изломов и дефектов рельс //Транспорт Урала – 2019. - № 3(62) – с.64-67
9. Регистрация и определение местоположения или опознавания подвижного состава или поезда, или состояния путевых устройств [Электронный ресурс]. – Режим доступа: https://findpatent.ru/catalog/2/50/336/3092/

Р.В. Фаткуллин, Е.В. Кислицын

ГРАФОВЫЕ БАЗЫ ДАННЫХ: ОСНОВНЫЕ ПОДХОДЫ К ПРОЕКТИРОВАНИЮ

Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ), Россия

Ключевые слова: база данных, граф, графовая база данных, NoSQL

Аннотация. В настоящем исследовании авторами представлен сравнительный анализ подходов к проектированию графовых баз данных. Выделено три основных подхода – построение ориентированных графовых БД, неориентированных графовых БД и графовых БД с множественными графами. По каждому подходу представлены основные принципы проектирования баз данных, а также инструментарий реализации. Данное исследование может быть интересно специалистам в области системного анализа и проектирования информационных систем, а также в области анализа данных.

R.V. Fatkulin, E.V. Kislitsyn

Graph databases: basic design approaches

Ural Technical Institute of Communications and Informatics (branch) in Yekaterinburg
(UrTISI SibGUTI), Russia

Keywords: database, graph, graph database, NoSQL

Annotation. In this study, the authors present a comparative analysis of approaches to the design of graph databases. Three main approaches are identified – the construction of oriented graph databases, undirected graph databases and graph databases with multiple graphs. For each approach, the basic principles of database design are presented, as well as the implementation tools. This study may be of interest to specialists in the field of system analysis and design of information systems, as well as in the field of data analysis.

Графовые базы данных – это современный тип NpSQL баз данных, который представляет и хранит информацию в виде графов, состоящих из узлов (вершин) и связей между ними (ребер). Этот тип баз данных получил большую популярность в последние годы благодаря своей способности эффективно моделировать и обрабатывать связанные данные.

В отличие от реляционных баз данных, где данные хранятся в таблицах, графовые базы данных позволяют представлять сложные связи между данными. Это особенно полезно для обработки данных, связанных с социальными сетями, географическими картами, биологическими и медицинскими данными, и многими другими приложениями.

Графовые базы данных также обладают рядом преимуществ по сравнению с традиционными реляционными базами данных, включая более быстрый доступ к данным, более простую масштабируемость и более гибкие запросы. На текущий момент существует разделение графовых баз данных в зависимости от предметной области и поставленной задачи перед разработчиками баз данных.[1]

1. Ориентированные графовые базы данных

Ориентированные графовые базы данных (Directed Graph Databases) хранят данные в виде ориентированных графов. Они предназначены для хранения информации о направлении связей между узлами и обеспечивают быстрый доступ к смежным узлам. Это позволяет моделировать отношения и зависимости между узлами в более точном формате. Такие базы данных наиболее подходят для решения задач, связанных с анализом социальных сетей, маркетинговым исследованиям и управлению проектами.

Основные принципы ориентированных графовых баз данных:

1. Направленность ребер: в ориентированном графе каждое ребро имеет направление, которое указывает на то, какие вершины связаны друг с другом. Это позволяет эффективно моделировать сложные взаимодействия между объектами.

2. Связность вершин: в ориентированном графе каждая вершина может быть связана с другими вершинами через направленные ребра. Это позволяет эффективно моделировать зависимости между объектами.

3. Алгоритмы обхода графа: ориентированные графовые базы данных используются для эффективного выполнения запросов к данным, используя различные алгоритмы обхода графа, такие как обход в глубину и обход в ширину. Эти алгоритмы позволяют быстро находить и обрабатывать связанные данные.

Применение ориентированных графовых баз данных:

1. Генеалогические деревья: ориентированные графовые базы данных используются для моделирования генеалогических деревьев, где каждый узел представляет собой человека, а каждое ребро указывает на отношения между людьми (родство, брак и т.д.).

2. Транспортные сети: ориентированные графовые базы данных используются для моделирования транспортных сетей, где каждый узел представляет собой город или точку на маршруте, а каждое ребро указывает на маршрут или дорогу между городами.

3. Социальные сети: ориентированные графовые базы данных используются для моделирования социальных сетей, где каждый узел представляет человека или сущность, а каждое ребро указывает на связь между ними. В ориентированных графовых базах данных социальных сетей можно хранить информацию о профилях пользователей, их друзьях, сообществах, подписчиках и т.д. Такие базы данных могут использоваться для рекомендации контента, анализа социальных связей, предсказания поведения пользователей и т.д.

Примеры ориентированных графовых баз данных:

1. Neo4j - это одна из самых популярных ориентированных графовых баз данных. Она предоставляет широкий спектр возможностей для работы с графовыми данными, таких как быстрый доступ к данным, обработка запросов и транзакций, а также инструменты для визуализации и анализа данных.

2. OrientDB - это многомодельная база данных, которая поддерживает ориентированные графы, документы и ключ-значение. Она обладает многими функциями, включая поддержку запросов SQL и многопоточность, что делает ее очень гибкой и масштабируемой.

3. ArangoDB - это многомодельная база данных, которая поддерживает графы, документы и ключ-значение. Она предоставляет удобный интерфейс для работы с графовыми данными и имеет мощные инструменты для обработки запросов и анализа данных.

2. Неориентированные графовые базы данных

Неориентированные графовые базы данных (Undirected Graph Databases) хранят данные в виде неориентированных графов. Они предназначены для хранения информации о связях между узлами без указания направления. Такие базы данных обычно используются для решения задач, связанных с анализом сетей взаимодействия, например, в биологии и социологии.

В неориентированных графовых базах данных каждый узел может содержать множество атрибутов или свойств, а ребро может содержать дополнительные данные, такие как вес, метку или тип связи. Неориентированные графовые базы данных часто используются в различных областях, таких как биология, социология, география и информационные системы, где сети взаимодействия не имеют определенного направления.

Одним из примеров неориентированных графовых баз данных является Neo4j. Он предоставляет инструменты для хранения и анализа неориентированных графовых данных, такие как язык запросов Cypher, алгоритмы машинного обучения и визуализацию данных. Еще одним примером является OrientDB, который также поддерживает язык запросов SQL и имеет множество функций для работы с данными.

Неориентированные графовые базы данных могут использоваться для решения различных задач, связанных с анализом и моделированием неориентированных графов. Они могут быть использованы для анализа социальных сетей, поиска сообществ или выявления центральных

узлов. Они также могут быть использованы для моделирования биологических сетей, например, для анализа связей между генами или белками.

В целом, неориентированные графовые базы данных являются мощным инструментом для хранения, обработки и анализа неориентированных графовых данных. Они позволяют эффективно работать с большими объемами данных и применять различные алгоритмы для анализа структуры графов и выявления закономерностей в данных.

3. Графовые базы данных с множественными графами

Графовые базы данных с множественными графами (Multi-Graph Databases) предназначены для хранения и обработки нескольких графов в одной базе данных. Они позволяют эффективно решать задачи, связанные с анализом нескольких сетей взаимодействия, например, в области биоинформатики и машинного обучения.

Такие базы данных могут быть полезными для различных приложений, где данные могут иметь несколько аспектов или контекстов, которые могут быть лучше представлены в виде отдельных графов. Например, в социальных сетях каждый граф может представлять профиль пользователя, его связи и активность в сети.

Одним из примеров графовых баз данных с множественными графами является база данных Amazon Neptune. Она позволяет создавать и управлять несколькими графами внутри одной базы данных и предоставляет возможности для выполнения сложных запросов на многих графах одновременно.[4]

Также существуют другие графовые базы данных с поддержкой множественных графов, такие как ArangoDB и OrientDB.

Neo4j, OrientDB и ArangoDB - это наиболее популярные графовые базы данных, которые предоставляют мощные инструменты для хранения, обработки и анализа графовых данных. Они имеют различные преимущества и недостатки, которые могут определять, какую базу данных следует использовать в конкретном случае.

Ниже приведены основные сравнительные характеристики Neo4j, OrientDB и ArangoDB:

1. Язык запросов:

- Neo4j использует язык запросов Cypher, который легко читаем и интуитивно понятен.
- OrientDB использует SQL для графовых баз данных, а также имеет собственный язык запросов Gremlin.
- ArangoDB использует AQL (ArangoDB Query Language), который сочетает в себе SQL, Cypher и Gremlin, позволяя использовать различные языки для запросов.

2. Модель данных:

- Neo4j использует проприетарную модель данных, которая состоит из узлов и связей.
- OrientDB и ArangoDB используют гибридные модели данных, которые могут быть использованы как для графовых, так и для документных баз данных.

3. Распределенность:

- Neo4j поддерживает только мастер-слейв репликацию, а шардинг[2] реализуется через дополнительное программное обеспечение.
- OrientDB поддерживает как мастер-слейв репликацию, так и шардинг данных.
- ArangoDB имеет встроенную поддержку для мастер-слейв репликации и шардинга данных.

4. Масштабируемость:

- Neo4j имеет ограничения на горизонтальную масштабируемость из-за своей модели данных и реализации репликации.
- OrientDB и ArangoDB лучше масштабируются горизонтально, так как они поддерживают распределенные вычисления и шардинг данных.

5. Производительность:

[2] Шардинг - метод разделения и хранения единого логического набора данных в виде множества баз данных

- Neo4j обычно считается наиболее производительной графовой базой данных из-за своей проприетарной модели данных и многих оптимизаций.
- OrientDB и ArangoDB обеспечивают хорошую производительность благодаря своей гибридной модели данных и возможности распределенных вычислений.[3]

При выборе между Neo4j, OrientDB и ArangoDB следует учитывать их сильные и слабые стороны, а также требования к проекту, чтобы определить, какая база данных лучше всего подходит для конкретной задачи.

Если проект требует полностью графовой базы данных с поддержкой ACID-транзакций и сильным фокусом на графовых алгоритмах, то Neo4j может быть наилучшим выбором. Neo4j имеет богатый набор инструментов для работы с графами, таких как Cypher Query Language, и широко используется в областях, таких как социальные сети, рекомендательные системы и биоинформатика.

Однако, если проект требует более гибкой базы данных, которая может хранить как графовые, так и неструктурированные данные, OrientDB и ArangoDB могут быть лучшими выборами. OrientDB имеет документо-графовую модель данных, что позволяет хранить данные как графы, так и документы в одной базе данных. ArangoDB имеет многомодельную архитектуру, что позволяет хранить данные как графы, документы и ключ-значение.

Кроме того, ArangoDB поддерживает асинхронные запросы, что может быть важно для приложений с высокой нагрузкой, а OrientDB имеет встроенную поддержку SQL, что может быть полезным для проектов, которые уже используют SQL-запросы.

Выбор между Neo4j, OrientDB и ArangoDB зависит от конкретных потребностей проекта. При выборе следует учитывать требования к модели данных, требования к производительности и доступности, а также требования к гибкости и расширяемости.

Графовые базы данных являются мощным инструментом для хранения и анализа сложных связанных данных. Они позволяют легко хранить и исследовать связи между различными элементами данных, что делает их особенно полезными в областях, таких как социальные сети, биоинформатика, телекоммуникации и т.д.

Однако, при выборе графовой базы данных необходимо учитывать множество факторов, таких как требования к производительности, доступности и гибкости, а также требования к модели данных и поддержке запросов.

В настоящее время на рынке существует множество графовых баз данных, каждая из которых имеет свои особенности и преимущества. Поэтому, выбор графовой базы данных зависит от конкретных требований проекта и необходимо проводить тщательное сравнение и анализ перед принятием решения.

СПИСОК ЛИТЕРАТУРЫ

1. Ёсу М. Т., Вальдуриес П. Принципы организации распределенных баз данных / М.Т. Ёсу, П. Вальдуриес, пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2021. – 672 с.:
2. Bruggen R. V. Learning Neo4j / R. V. Bruggen. – United Kingdom Livery Place: Birmingham B3 2PB, Published by Packt Publishing Ltd. 2014. – 222 p.
3. Редмонд Э. Семь баз данных за семь недель. Введение в современные базы данных и идеологию NoSQL / Э. Редмонд, пер. с англ. Слинкин А. А. – М.: ДМК Пресс, 2018. – 384 с.: ил.
4. Робинсон Я. Графовые базы данных / Я. Робинсон, Д. Вебнер, Э. Эифрем. пер. с англ. Р. Н. Рагимова; науч. ред. А. Н. Киселев. – 2-е изд. – М.: ДМК Пресс, 2016. – 256 с.: ил.
5. Сьоре Э. Проектирование и реализация систем управления базами данных / Э. Сьоре, пер. с англ. А. Н. Киселева; науч. ред. Е. В. Рогов. – М.: ДМК Пресс, 2021. – 466 с.: ил.
6. Салибекян С.М., Петрова С.Б. Объектно-атрибутная модель представления пространственно-временных отношений между объектами // Прикладная информатика. 2016. Т. 11. № 3 (63). С. 103-115.
7. Franks B. Taming big data: how to extract knowledge from arrays of information using deep analytics / B. Franks; trans. from English. Andrey Baranov. – M.: Mann, Ivanov and Ferber, 2014. – 352 p.

8. Bruggen R. V. Learning Neo4j / R. V. Bruggen. – United Kingdom Livery Place: Birmingham B3 2PB, Published by Packt Publishing Ltd. 2014. – 222 p.
9. Harrison G. Next Generation Databases / G. Harrison – United States, CA, Published by Apress, 2015. – 244 p.

АВТОРЫ СТАТЕЙ

АРЕФЬЕВА Елизавета Алексеевна — курсант Уральского института Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, г. Екатеринбург, Россия, arefyeva2001@mail.ru

АРТЕМЬЕВ Павел Игоревич — студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

АГАРКОВА Екатерина Владимировна — студентка Донского государственного технического университета, г. Ростов – на Дону, Россия, agarkat@yandex.ru

АГАПИТОВ Денис Вадимович — студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, koshkidadanet@gmail.com

БАИМОВ Роман Ирекович — студент ФГАОУ ВО «Южно-Уральский государственный университет (Национальный исследовательский университет)» (ФГАОУ ВО ЮУрГУ (НИУ)), г. Челябинск, Россия, baimov.roman@internet.ru

БАТЕНКОВ Кирилл Александрович — доктор технических наук, профессор РТУ МИРЭА, г. Москва, Россия, pustur@yandex.ru

БАРБИН Николай Михайлович — доктор технических наук, профессор Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, nmbarbin@mail.ru

БЕНЦЕЛЬ Валерий Владимирович — студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, val.ben.2016@yandex.ru

БРАГИН Кирилл Игоревич — аспирант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, braga.k.urtisi@gmail.com

БУДЫЛДИНА Надежда Вениаминовна — кандидат технических наук, доцент, и.о. зав. кафедрой инфокоммуникационных технологий и мобильной связи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, bnv@urtisi.ru

БУРУМБАЕВ Даниль Ильмирович — аспирант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, bdi@urtisi.ru

ДЕНИСОВ Дмитрий Вадимович — кандидат технических наук, доцент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет

	телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, ddv@urtisi.ru
ГАНЧЕНКО Дарья Денисовна	студентка Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, zhora.gorod1@mail.ru
ГАНЧЕНКО Егор Евгеньевич	студент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, zhora.gorod1@mail.ru
ГЛАДНЕВ Виталий Викторович	студент магистратуры Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru
ГЛЕБЕЦ Алексей Леонидович	студент ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск, Россия, Lexa.glebec@yandex.ru
ГНИЛОМЕДОВ Ефим Иванович	доцент кафедры многоканальной электросвязи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, mec@urtisi.ru
ГОЛОВЛЕВ Максим Олегович	студент ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск, Россия, golowlev.maksim@yandex.ru
ГОРЛОВ Николай Ильич	доктор технических наук, профессор ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ), г. Новосибирск, Россия, gorlovnik@yandex.ru
ЗЕМСКОВ Александр Васильевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, zemsckov.alexander2016@yandex.ru
ЗЫСКИНА Дина Вениаминовна	студентка Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, mec@urtisi.ru
КАЗАНЦЕВ Семён Сергеевич	студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, alexnodov635@gmail.com
КАЙГОРОДОВ Алексей Евгеньевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия
КАМЕНСКОВ Александр Евгеньевич	студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, sashakamenskov@mail.ru

КВИТКОВА Ирина Геннадьевна — старший преподаватель кафедры инфокоммуникационных систем и сетей ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики», г. Новосибирск, Россия, irin.creme@yandex.ru

КИСЛИЦЫН Евгений Витальевич — кандидат экономических наук, доцент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, kev@usue.ru

КОБЕЛЕВ Антон Михайлович — кандидат технических наук, доцент кафедры автоматизированных систем и противопожарной защиты Уральского института Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, г. Екатеринбург, Россия, antonkobelev85@mail.ru

КОЗЛОВСКИЙ Андрей Тадеушевич — кандидат технических наук, доцент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, katroick@gmail.com

КОЛТАШЕВ Ярослав Андреевич — студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, y.koltashev@mail.ru

КОРОБИЦЫН Иван Владимирович — студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, kiv@urtisi.ru

КОНОВАЛОВ Иван Сергеевич — студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, mec@urtisi.ru

КРЫСИН Дмитрий Сергеевич — студент магистратуры Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru

КУМАЧЕВ Даниил Леонидович — студент магистратуры Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru

КУСАЙКИН Дмитрий Вячеславович — кандидат технических наук, доцент кафедры многоканальной электросвязи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, Kusaykin@mail.ru

ЛЕВИКОВ Артём Андреевич — студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и

	информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, gurulevikov@yandex.ru
ЛОБУНЕЦ Олег Дементьевич	доктор технических наук, профессор Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, lod@urtisi.ru
МАЛКОВА Ирина Андреевна	старший преподаватель кафедры инфокоммуникационных технологий и мобильной связи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, mia@urtisi.ru
МАЛЫЙ Максим Владимирович	студент магистратуры Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru
МИРОШНИЧЕНКО Дарья Вячеславовна	студентка Донского государственного технического университета, г. Ростов – на Дону, Россия, miros.dasha@gmail.com
МИХАЙЛЕНКО Максим Владимирович	ассистент Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru
МИХАЙЛЕНКО Оксана Леонидовна	ассистент Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru
МУБАРАКШИНА Кристина Фирдаусовна	студентка Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, mubarakshina.christina@yandex.ru
НИКИТИН Алексей Степанович	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, Biveralexey@yandex.ru
ОВЧИННИКОВ Данил Юрьевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, mec@urtisi.ru
ОСИПОВА Ирина Александровна	кандидат технических наук, доцент кафедры информационных систем и технологий Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, oia@urtisi.ru
ПЕТРОВ Аркадий Сергеевич	студент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, pietrov_arkadii@mail.ru
ПЛЕХАНОВ Савелий Михайлович	преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский

	государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, psm@urtisi.ru
ПЯТКОВ Никита Аркадьевич	кандидат философских наук, студент Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, violetwolf@mail.ru
РАГОЗИН Андрей Николаевич	кандидат технических наук, доцент ФГАОУ ВО «Южно-Уральский государственный университет (Национальный исследовательский университет)» (ФГАОУ ВО ЮУрГУ (НИУ)), г. Челябинск, Россия, ragozinan@susu.ru
САФАРЬЯН Ольга Александровна	кандидат технических наук, доцент Донского государственного технического университета, г. Ростов – на Дону, Россия, safari_2006@mail.ru
СВАЛУХИН Константин Владимирович	аспирант Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, skv@urtisi.ru
СЕРГЕЕВ Алексей Анатольевич	ассистент Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, ek.sergeev134@yandex.ru
СЕНАЧИН Никита Михайлович	студент Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, senachin-nikita@mail.ru
СТОЙЧИН Красимир Людмилов	старший преподаватель Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru
СТОЙЧИНА Елена Владиславовна	ассистент Уральского федерального университета, Института радиоэлектроники и информационных технологий - РТФ (ИРИТ-РТФ), г. Екатеринбург, Россия, K001kk96@mail.ru
СТУПНИКОВА Александра Алексеевна	студентка магистратуры Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ), г. Новосибирск, Россия, sanya.sano1.1@gmail.com
ТАРАСОВ Евгений Сергеевич	доцент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, tes@urtisi.ru
ТИТОВ Станислав Андреевич	научный сотрудник научно-исследовательского отделения учебно-научного комплекса пожаротушения и проведения аварийно-спасательных работ Уральского института Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, г. Екатеринбург, Россия, tsa-nhl@mail.ru
ФАЛЯЕВА Елена Анатольевна	студентка Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург, Россия, elena.fa@inbox.ru

ФАСТОВ Даниил Алексеевич — системный инженер 3-ей категории Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, fastov-2000@mail.ru

ФАТКУЛЛИН Руслан Владиславович — студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, buddhaeye13@gmail.com

ШЕСТАКОВ Иван Игоревич — старший преподаватель кафедры многоканальной электрической связи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, ivansche2007@rambler.ru

ШУВАЛОВ Вячеслав Петрович — доктор технических наук, профессор ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики», г. Новосибирск, Россия, shvp04@mail.ru

ШУЛЬГА Игорь Викторович — директор учебного центра ОА «ИскраУралТЕЛ», г. Екатеринбург, Россия, shulga@iskrauraltel.ru

ЮРЧЕНКО Евгения Владимировна — старший преподаватель кафедры многоканальной электросвязи Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, jena23@mail.ru

АВТОРСКИЙ УКАЗАТЕЛЬ
THE AUTHOR·S INDEX