



СибГУТИ

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

# **ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОГНИТИВНАЯ ЭЛЕКТРОСВЯЗЬ**

**Сборник научных трудов X Всероссийской научно-  
практической конференции**

Екатеринбург  
2024



Уральский технический  
институт связи  
и информатики

**X Всероссийская научно-практическая  
конференция «Информационные технологии и  
когнитивная электросвязь»**  
»

### **Научные направления конференции:**

- Инфокоммуникационные технологии и системы связи
- Системы электросвязи специального назначения
- Современные технологии передачи информации

### **Партнёры:**



**СибГУТИ**

СИБИРСКИЙ  
ГОСУДАРСТВЕННЫЙ  
УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ  
И ИНФОРМАТИКИ

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



УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ  
(УРГУПС), Г. ЕКАТЕРИНБУРГ

УДК 378+621.391  
ББК 74.58 + 32.88-01

Информационные технологии и когнитивная электросвязь. X Всероссийская научно-практическая конференция;  
Сб. науч. ст. в 1 т. / Под ред. Шувалова В.П.;  
Сост.: М.П. Карачарова  
УрТИСИ СибГУТИ, 2024. 137 с.

#### ПРОГРАММНЫЙ КОМИТЕТ

**Председатель:**

*Минина Е. А.*, кандидат технических наук, директор УрТИСИ СибГУТИ (г. Екатеринбург, Россия);

**Заместитель председателя:**

*Будылдина Н. В.*, кандидат технических наук, доцент, зав. кафедрой инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

**Члены программного комитета:**

*Овчинников Д. А.*, старший преподаватель кафедры инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

*Вольнская А. В.*, кандидат технических наук, доцент, начальник Управления обеспечения образовательного процесса УрГУПС.

#### ОРГАНИЗАЦИОННЫЙ КОМИТЕТ УрТИСИ СибГУТИ

**Председатель:**

*Поршнев С. В.*, доктор технических наук, профессор, профессор кафедры инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

**Члены организационного комитета:**

*Будылдина Н. В.*, кандидат технических наук, доцент, зав. кафедрой инфокоммуникационных технологий и мобильной связи УрТИСИ СибГУТИ;

*Гниломёдов Е. И.*, доцент кафедры МЭС, и.о. зав. кафедрой многоканальной электрической связи УрТИСИ СибГУТИ;

*Куаньшиев В. Т.*, кандидат физико-математических наук, доцент, зав. кафедрой высшей математики и физики УрТИСИ СибГУТИ

*Карачарова М. П.*, начальник методического отдела УрТИСИ СибГУТИ

В сборник включены доклады, выполненные в рамках X 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 13.05.2024.

Вышло в свет 20.05.2024.

620109, Россия, г Екатеринбург, ул. Репина, д. 15

© УрТИСИ СибГУТИ, 2024

# СОДЕРЖАНИЕ

№ п/п	Авторы и названия статей	Стр.
	<b>ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ</b>	
1	<b>Р.И. Баимов, А.Н. Рагозин.</b> Многопозиционный посадочный радиолокатор для обеспечения надёжной посадки БПЛА в условиях постановщиков помех на подготовленную посадочную площадку.....	6
2	<b>Н.А. Байтяков, С.В. Мухачев.</b> Распознавание текстов, сгенерированных искусственным интеллектом.....	11
3	<b>Н.А. Байтяков, К.Л. Костюченко.</b> Безопасность инфокоммуникационных систем: угрозы, способы и средства обеспечения.....	14
4	<b>К.А. Батенков.</b> Характеристики предельных значений частоты для цифровых систем передач.....	18
5	<b>Д.И. Бурумбаев, Н.М. Барбин.</b> Анализ исследований в области изучения свойств жидкости оптическим излучением.....	20
6	<b>А.А. Воробьев, И.И. Шестаков.</b> Исследование влияния FBT и PLC разветвителей на диаграммы уровней сигналов в сети GPON.....	23
7	<b>В.П. Шувалов, Б.П. Зеленцов, И.Г. Квиткова.</b> О совместном распределении времени до отказа и времени восстановления.....	28
8	<b>А.В. Земсков, И.А. Малкова.</b> 3D-симулятор для демонстрации процесса управления системами связи.....	31
9	<b>М.Ю. Казанцев.</b> Блокчейн: революция в финансах, здравоохранении и не только.....	37
10	<b>В.С. Сидоров, Н.В. Будылдина.</b> Организация OpenSource зонтичной системы мониторинга для сбора и систематизации параметров сервера MariaDB.....	40
11	<b>И.В. Ташкинов, Н.В. Будылдина.</b> Анализ существующих решений и протоколов SD-WAN.....	44
12	<b>О.Г. Мелентьев, Д.А. Гончаров, И.М. Куликов.</b> Алгоритм многооконной символьной синхронизации по отсчетам комплексной огибающей.....	48
13	<b>К.Н. Кудрявцева, А.В. Волынская.</b> Микросервисная архитектура: эффективное решение для автоматизированного управления перевозками.....	53
14	<b>С.В. Михеева, Е.А. Минина, И.И. Шестаков.</b> Исследование влияния пиковой мощности и фазы смежных солитонов, распространяющихся в TDM режиме.....	58
15	<b>В.П. Шувалов, И.Г. Квиткова.</b> К расчету показателей надежности волоконно - оптической линии связи сети доступа.....	62
16	<b>Н.И. Горлов.</b> Оптоволоконные датчики и сенсорные сети.....	67
17	<b>С.Ю. Красных, Н.М. Барбин, В.Т. Куанышев.</b> Обзор методов и способов измерения электрических характеристик жидких диэлектриков.....	71
18	<b>Е.С. Тарасов, Н.В. Будылдина, А.С. Никитин.</b> Анализ экономической эффективности внедрения аппаратно-программной системы передачи данных с обработкой реального трафика.....	77
19	<b>О.Д. Лобунец.</b> Определение эпюр сигналов совмещенного канала питания и передачи информации.....	82
20	<b>Е.В. Юрченко, А.Е. Каменсков.</b> Разработка искусственной нейронной сети для прогнозирования энергопотребления сети интернета вещей.....	86
21	<b>Е.В. Юрченко, Д.В. Чадаев.</b> Анализ применения нейронных сетей в концепции сетей интернета вещей.....	91
22	<b>А.С. Яковлев.</b> К вопросу о механической надежности оптоволоконных линий связи.....	96
23	<b>Д.А. Овчинников, С.А. Баранов, Н.М. Барбин, В.Т. Куанышев.</b> Исследование коэффициента отражения радиоволн в зависимости от геометрических размеров емкости.....	100
	<b>СИСТЕМЫ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ</b>	

24	<b>В.Н. Коваленко.</b> Системы управления поездами на базе радиоканала и с использованием спутниковых технологий.....	103
	<b>СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ИНФОРМАЦИИ</b>	
25	<b>И.С. Коновалов, Д.В. Кусайкин.</b> О применении автокодировщиков в волоконно-оптических системах передачи.....	108
26	<b>И.В. Коробицын, О.Е. Каранин, С.М. Плеханов.</b> Проект IoT системы – «Автономный умный дом».....	112
27	<b>И.И. Нуруллин, А.В. Волынская.</b> Использование нейронных сетей в ветеринарии....	118
28	<b>А.В. Румянцева, Е.С. Богданова.</b> Применение протоколов FTP, WebDAV для реализации в информационных системах в ОАО «РЖД».....	121
29	<b>К.Л. Костюченко, М.А. Серeda.</b> Инновации в области цифровой передачи данных: квантовые технологии.....	125
30	<b>К.М. Тупицын.</b> Стеганография в современных кибератаках.....	129
	<b>АВТОРЫ СТАТЕЙ</b> .....	133
	<b>АВТОРСКИЙ УКАЗАТЕЛЬ</b> .....	137

# Секция 1. ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ

Р.И. Баимов, А.Н. Рагозин

## МНОГОПОЗИЦИОННЫЙ ПОСАДОЧНЫЙ РАДИОЛОКАТОР ДЛЯ ОБЕСПЕЧЕНИЯ НАДЁЖНОЙ ПОСАДКИ БПЛА В УСЛОВИЯХ ПОСТАНОВЩИКОВ ПОМЕХ НА ПОДГОТОВЛЕННУЮ ПОСАДОЧНУЮ ПЛОЩАДКУ

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.

Исследована структура и состав радиоугломерной системы посадки беспилотного летательного аппарата (БПЛА) в виде многопозиционного посадочного радиолокационного комплекса, что позволяет обрабатывать информацию на нескольких пространственно-разнесённых участках поля от источника радиоизлучения (ИРИ). Совместная обработка принятого сигнала значительно повышает помехозащищённость и информативность. Исследуется применение адаптивной фазированной антенной решетки (АФАР) радиопеленгатора в составе радиоугломерной системы посадки БПЛА, а также новых оптимальных амплитудных распределений на элементах АФАР. Это позволяет повысить точность определения угловых координат источника радиоизлучения в радиоугломерной системе посадки.

R.I. Baimov, A.N. Ragozin

## MULTI-POSITION LANDING RADAR TO ENSURE A RELIABLE LANDING OF THE UAV IN THE CONDITIONS OF JAMMERS ON A PREPARED LANDING SITE

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

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

The structure and composition of the radiocarbon landing system of an unmanned aerial vehicle (UAV) in the form of a multi-position landing radar complex has been studied, which allows processing information on several spatially spaced sections of the field from a radio emission source (IRI). Joint processing of the received signal significantly increases noise immunity and information content. The use of an adaptive phased array antenna array (AFAR) of a radio direction finder as part of a radio node-dimensional UAV landing system, as well as new optimal amplitude distributions on AFAR elements, is being investigated. This makes it possible to increase the accuracy of determining the angular coordinates of the radio emission source in the radio angle-measuring landing system.

### Введение:

В настоящее время актуальной задачей является пеленгация (измерение угловых координат) источников радиоизлучения (ИРИ), реализуемая в радиотехнических системах.

Задача измерения угловых координат ИРИ в пассивной радионавигации возникает при реализации радиоугломерной системы (РС) для целей наведения и автоматической посадки беспилотного летательного аппарата (БПЛА). Например, при размещении ИРИ на борту БПЛА для определения координат ИРИ применяются методы пассивной триангуляции [1,2].

Для решения задачи помехозащиты при реализации радиоугломерной системы необходимо путем обработки исследуемого сигнала определить количество источников излучения и

определить их угловые координаты. В условиях нестационарной помеховой обстановки методы помехозащиты могут быть реализованы, если предварительно определены угловые координаты постановщиков помех и их число [3].

## 2. Пример построения радиоугломерной системы посадки БПЛА.

На рис. 1 представлена радиоугломерная система посадки БПЛА на стационарную посадочную подготовленную площадку

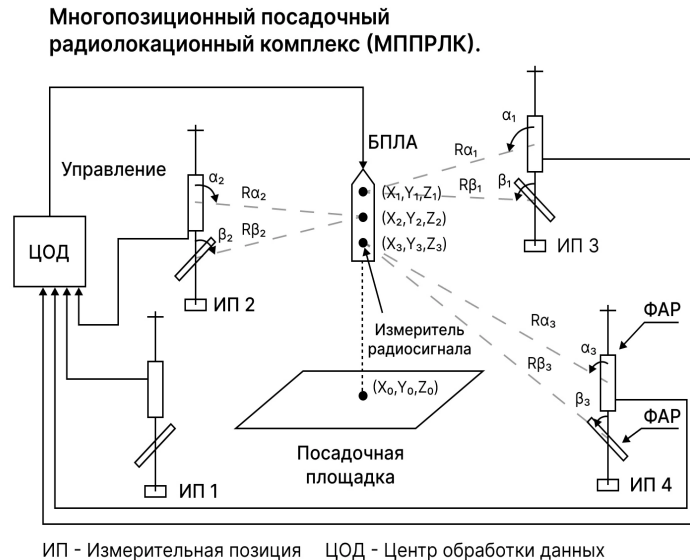


Рис. 1. Радиоугломерная система посадки БПЛА на стационарную посадочную подготовленную площадку

Радиоугломерная система посадки БПЛА на стационарную посадочную площадку представляет собой стационарный наземный многопозиционный посадочный радиолокационный комплекс (МППРЛК).

МППРЛК (рис.1) состоит из нескольких измерительных позиций (ИП), центра обработки данных (ЦОД), посадочной площадки (ПП) и беспилотного летательного аппарата (БПЛА).

ИП МППРЛК – фазированные антенные решётки (ФАР), ориентированные в азимутальной и угломестной плоскостях, размещённые на определённой высоте на мачте. ИП МППРЛК – формирует первичные угловые координаты БПЛА в ходе процесса автоматической посадки.

ЦОД – объединяет первичные координаты всех ИП и формирует конечные координаты БПЛА для реализации автоматической посадки БПЛА на посадочную площадку.

На БПЛА установлены источники радиосигнала (ИР), и их первичные координаты определяются с помощью наземных измерительных позиций (ИП) в режиме пассивной радиотехнической системы.

## 3. Пример построения измерительной позиции радиоугломерной системы посадки БПЛА.

На рис. 2, в качестве примера отображена структура ИП МППРЛК, содержащая два яруса (этажа) линейных ФАР, размещённых на мачте, две азимутальные линейные ФАР (ФАР1, ФАР3), две угломестные линейные ФАР (ФАР2, ФАР4).

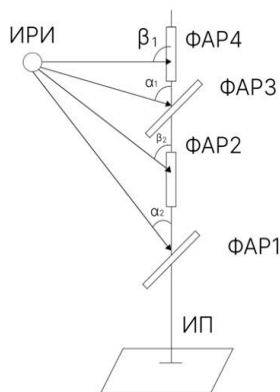


Рис. 2. Двухуровневая ИП МППРЛК, содержащая в своём составе четыре линейных ФАР, две азимутальные линейные ФАР (ФАР1, ФАР3), две угломестные линейные ФАР (ФАР2, ФАР4).

Применение в составе ИП МППРЛК АФАР позволит существенно повысить точность определения координат, а также помехоустойчивость в условиях активного радиопротиводействия.

АФАР – антенная система, которая включает в себя массив из нескольких антенн (элементов АФАР) и алгоритма адаптивной обработки сигналов, позволяющий динамически изменять диаграмму направленности (ДН) или направление луча, в ответ на изменение условий окружающей среды или помеховой обстановки. Формирование глубоких нулей или широких провалов в заданных направлениях ДН ЛФАР позволяет эффективно подавлять воздействия постановщиков помех [4].

Задача выбора весового окна амплитудного распределения на элементах ЛФАР по критерию ширина луча – уровень боковых лепестков ДН рассмотрена в работе [5]. При моноимпульсном методе пеленгования ИРИ требуется формировать суммарную и разностную ДН ЛФАР [6,7]. В публикациях рассмотрен алгоритм построения ДН и критерии оценки для точной пеленгации ИРИ. В работе [8] проведено исследование определения угловой координаты на фоне помех многоточечного ИРИ, находящегося в зоне Френеля линейной ФАР.

Формирование нулей (рис. 3) и провалов (рис. 4) в ДН:

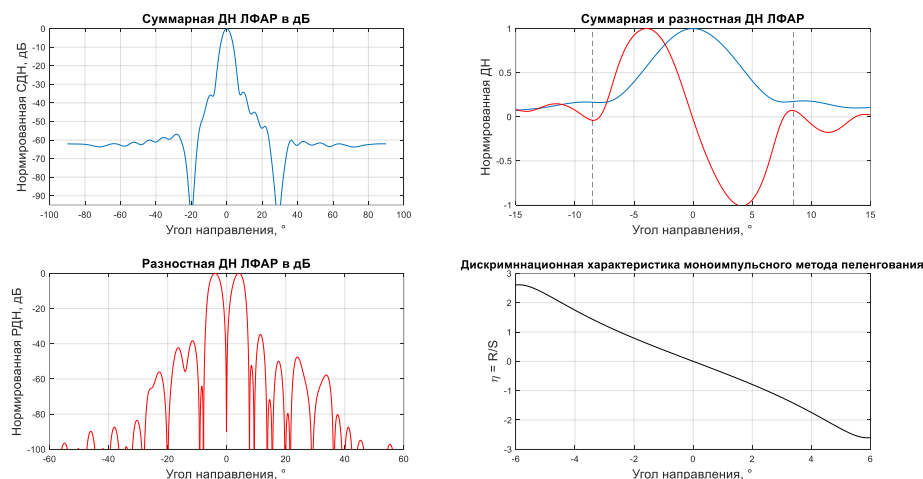


Рис. 3. Результаты расчётов СДН с нулями в направлении помех, РДН, дискриминационной характеристики моноимпульсного радиопеленгатора для оптимального амплитудного распределения с общей шириной лепестков



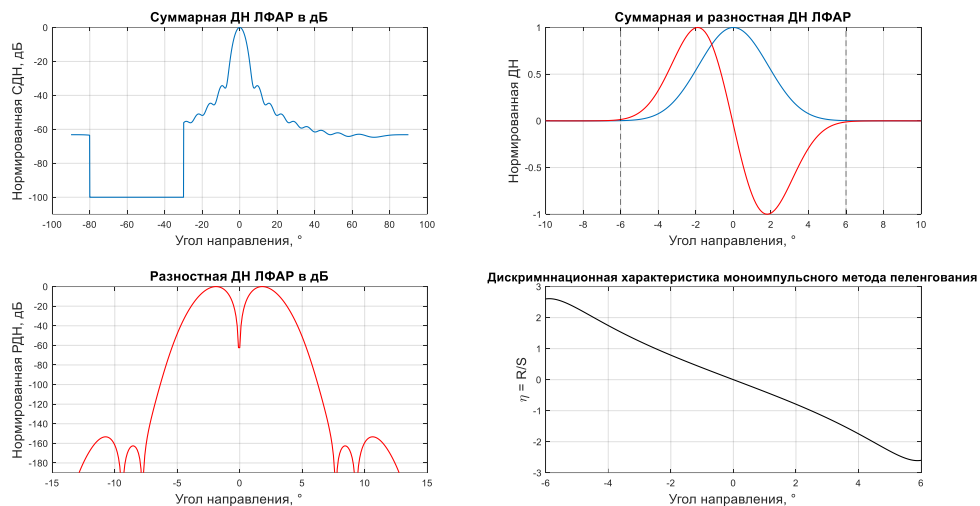


Рис. 4. Результаты расчётов СДН с широкими провалами в направлении помех, РДН, дискриминационной характеристики моноимпульсного радиопеленгатора для оптимального амплитудного распределения с общей шириной лепестков

Результаты исследование объединены в таблицу 1:

Таблица 1. Сравнение амплитудных распределений весовых коэффициентов с учётом формирования нулевых значений и провалов в направлении помех.

Оптимальные амплитудные распределения	Ширина главного лепестка, град.		Уровень боковых лепестков СДН, дБ		Уровень боковых лепестков РДН, дБ		Крутизна	
	Форм. нулей	Форм. провалов	Форм. нулей	Форм. провалов	Форм. нулей	Форм. провалов	Форм. нулей	Форм. провалов
Оптимальное с общей шириной лепестков	7,1	7,1	-34,7	-34,70	-35,01	-153,53	0,46	0,46
Оптимальное с минимальной боковой лепестковой энергией	5,6	5,6	-28,77	-28,77	-21,68	-119,41	0,54	0,54
Оптимальное с минимальной суммой квадратов пьедесталов	6,3	6,3	-31,38	-31,38	-34,88	-142,27	0,4	0,4
Оптимальное с минимальной площадью под кривой диаграммы направленности	7,2	7,2	-36,17	-36,17	-35,18	-155,21	0,58	0,58
Оптимальное с минимальным количеством несовпадений фаз	6,8	6,8	-34,75	-34,75	-35,31	-155,2	0,44	0,44
Оптимальное с наименьшей мощностью на пьедестале	6	6	-35,35	-35,35	-35,41	-157,2	0,58	0,58

**Заключение:** Рассмотрена структура и состав радиоугломерной системы посадки БПЛА в виде многопозиционного посадочного радиолокационного комплекса, что позволяет обрабатывать информацию на нескольких пространственно-разнесённых участках поля от ИРИ,

при этом совместная обработка принятого сигнала позволяет значительно повысить помехозащищённость и информативность радиотехнических систем.

В ходе проведённого исследования по результатам анализа данных, приведённых в таблице 1 и по результатам анализа графиков (рис. 3-4) можно сделать вывод, что метод формирования нулей и широких провалов в ДН ЛФАР с оптимальным весовым амплитудным распределением на элементах в виде распределения с наименьшей мощностью на пьедестале на элементах ЛФАР реализует критерии для точной пеленгации ИРИ в условиях высокой помеховой нагрузки в заданном угловом секторе. Это обусловлено тем, что уровень боковых лепестков РДН направленности, ответственных за помехозащищённость, является минимальным.

Метод формирования широких провалов в ДН ЛФАР позволяет эффективно одновременно подавить несколько источников помех, действующих с различных угловых направлений.

Результаты исследования могут быть использованы для оптимизации и улучшения работы радиопеленгатора в составе радиоугломерной посадочной системы БПЛА, также при разработке радиопеленгатора с высокой степенью помехозащищённости для решения различных задач радиомониторинга.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Булычев Ю.Г., Таран В.Н. Инвариантно-групповой метод отождествления пеленгов в триангуляционных многопозиционных системах пассивной локации // Радиотехника и электроника. – 1987. – Т. 32. – № 4.
2. Middlebrook D.L. Bearings-only tracking automation for a single unmanned underwater vehicle: Thesis (S.M.) Massachusetts Institute of Technology, Dept. of Mechanical Engineering, 2007.
3. Чистяков В.А. Определение угловых координат радиоизлучения в антенных решетках космических аппаратов // Universum: Технические науки: электрон. научн. журн. 2017. № 12(45). URL: <http://7universum.com/ru/tech/archive/item/5373>
4. Григорьев В.А., Щесняк С.С., Гулюшин В.Л., Распаев Ю.А., Лагутенко О.И., Щесняк А.С. //Адаптивные антенные решетки. Учебное пособие в 2-ух частях. Часть 1. Санкт-Петербург: СПб: Университет ИТМО, 2016. С. 45 – 46.
5. Баимов Р. И., Рагозин А. Н. Выбор весового окна амплитудного распределения на элементах линейной фазированной антенной решетки по критерию ширина луча - уровень боковых лепестков диаграммы направленности// 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.
6. Баимов Р. И., Рагозин А. Н. Повышение точности пеленгования источника радиоизлучения за счёт выбора весового амплитудного распределения на элементах линейной фазированной решетки радиопеленгатора в составе радиоугломерной системы посадки// Материалы 10-й научной выставки-конференции научно-технических и творческих работ студентов. Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет, 2023. С. 90 – 93.
7. Баимов Р. И., Рагозин А. Н. Оптимизация амплитудного распределения на элементах линейной фазированной антенной решетки в составе радиопеленгатора источника радиоизлучения// Сборник научных трудов IX Всероссийской научно-практической конференции. Екатеринбург, 2023. С. 14 – 18.
8. Errors in Measuring the Angular Coordinate of Extended Targets by the Monopulse Method in the Fresnel Zone of the Linear Antenna Array / A.N. Ragozin, S.N. Darovskich, V.F. Telezhkin, A.D. Pletenkova //Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2020. – Т. 20, № 2. – С. 67–76. DOI:10.14529/ctcr200207.

## РАСПОЗНАНИЕ ТЕКСТОВ, СГЕНЕРИРОВАННЫХ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

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

Ключевые слова: искусственный интеллект, нейронные сети, ChatGPT, машинное обучение, генерация текстов.

В статье рассматривается проблема роста количества генерируемого текста с помощью искусственного интеллекта, а также влияние чат-ботов на электронные ресурсы, аудиторию и уровень успеваемости студентов и учеников. Мы анализируем методы опознавания сгенерированного текста и его признаки.

N.A. Baytyakov, S.V. Mukhachev

## RECOGNITION OF TEXTS GENERATED BY ARTIFICIAL INTELLIGENCE.

Ural State University of Railways and Transport (USURT), Yekaterinburg, Russia

Key words: Artificial intelligence, neural networks, ChatGPT, machine learning, text generation.

The article considers the problem of the growth of the amount of generated text with the help of artificial intelligence, as well as the impact of chat bots on electronic resources, the audience and the level of academic achievement of students and students. We're analyzing methods to identify the generated text and its signs.

Количество материалов, сгенерированных искусственным интеллектом, стремительно растет. Многие школьники и студенты пользуются услугами искусственного интеллекта для выполнения различных заданий: написание рефератов и сочинений, подготовка программного кода, перевод текстов, создание иллюстраций, обработка фото, в качестве шпаргалок [1].

Различные модули искусственного интеллекта, основанные на нейронных сетях, не идеальны и пока не могут создавать тексты, сравнимые с произведениями человека. Однако они совершенствуются, и уже сегодня такие модули иногда способны вызвать иллюзию того, что текстовый материал создан человеком.

Использование искусственного интеллекта для подготовки текста, кроме очевидных удобств, влечет и некоторые негативные последствия: возможность искажения фактов, возможность «плагиата» – когда текст написан с использованием искусственного интеллекта, падение качества обучения.

В настоящее время появляется и публикуется все большее количество текстов, подготовленных с использованием искусственного интеллекта. В 2022 году появилась и стала доступна для широкого круга пользователей нейронная сеть ChatGPT. Она в состоянии поддерживать диалог, исправлять ошибки в тексте, отвечать более верно стилистически и грамматически, чем ее предыдущие версии.

Такой результат был получен путем модернизации версии ChatGPT 3.0. На основе этой модели компания, наняв штат, принялась обучать нейросеть прикладным путем. Первоначально сеть сама генерировала ответ на вопрос сотрудника, после чего сотрудник вручную корректировал неверный или смежный ответ и натаскивал сеть отвечать четко и не отходя от первоначальной темы. На другой стадии людей просили ранжировать выданные предыдущей версией модели ответы на те или иные входные тексты: от самого релевантного до полного несоответствия. [2].

Нередко возникает вопрос о том, как отличить текст, написанный нейросетью, от текста, полностью созданного человеком. Необходимо определить признаки, указывающие на использование нейросети.

Один из важных признаков – выполнение закона Ципфа. Закон Ципфа («ранг–частотность») – эмпирическая закономерность распределения частотности слов естественного языка. Смысл этого закона состоит в том, что если все достаточно длинного текста упорядочить по убыванию частотности их использования, то частотность  $n$ -го слова в таком списке окажется приблизительно обратно пропорциональной его порядковому номеру  $n$  (рангу этого слова) [3].

Например, второе по используемости слово встречается примерно в два раза реже, чем первое, третье – в три раза реже, чем первое, и так далее. Или, другими словами, произведение ранга на частоту есть величина постоянная. Согласно закону Ципфа, в тексте, написанном естественным языком, имеются предсказуемые пропорции. Отклонения от этих пропорций можно достаточно легко обнаружить. Поэтому для выявления текста, созданного с помощью нейросети, можно использовать закон Ципфа. Машинный текст не подобен по частотным свойствам сложным естественным языкам.

Однако с развитием нейронных сетей данный закон утрачивает диагностическую силу, так как современные чат-боты способны генерировать тексты, для которых закон Ципфа выполняется. Также значительно уменьшилась значимость такого признака, как связность текста.

Следующий признак – тематическая избыточность. Нейронная сеть, в отличие от человека, генерирует слишком длинный текст там, где можно обойтись лаконичным сообщением.

Еще один признак – наличие в тексте такой структуры, как список, а также частота его использования. Например, ChatGPT стремится построить весь текст в виде нескольких списков, которые следуют друг за другом. Люди же, как правило, используют списки не так часто. Для описания сложных идей формат списка неприемлем, и даже если такой формат подходит, люди редко его используют.

Также важный признак – орфография и пунктуация: если в тексте нет никаких ошибок, то текст, возможно, подготовлен нейросетью.

В основном для поиска машинного текста используется машина, в Интернете имеется много сервисов, которые предлагают определить написан ли текст человеком или использовался искусственный интеллект. Но любой из них не лишен недостатков.

В русскоязычном сегменте наиболее продвигаемым детектором использования искусственного интеллекта для генерирования текста стал «Антиплагиат». С 2023 года в программу внедрен модуль определения сгенерированного текста, который указывает на текст, возможно сгенерированный нейронной сетью. Результаты детектора имеют лишь характер предположения, поэтому нет гарантии безошибочного определения текста, сгенерированного нейронной сетью[4].

Еще один пример таких сервисов – GPTZero Classic. Он, в том числе, анализирует параметр Perplexity – предсказуемость текста. Смысл анализа состоит в том, чтобы оценивает структуру и длину предложений. А затем сравнить полученные данные с типовыми для текста, написанного человеком. Особенность в том, что люди пишут сложнее и используют менее очевидные словосочетания.

Для идентификации сгенерированных текстов предлагается использовать вотермарки (водяные знаки), которые позволят определить авторство. Эту технологию уже разрабатывают в OpenAI.

Сегодня нейросети обучаются на постоянно увеличивающемся количестве текстов из интернет-источников, задействуют обучение с подкреплением и фидбэк пользователей. Это позволяет создавать тексты, очень похожие на те, что создает человек, так как чат-боты обучаются на тысячах текстов совместно с живыми людьми, корректирующими их структуру и глубину ответа. Детекторы также совершенствуются. с каждым годом это будет все труднее, ведь. Получается, что между ними идет состязание: генеративная модель пытается запутать детектирующую, а та, в свою очередь, учится верно различать сгенерированные и написанные человеком тексты.

## СПИСОК ЛИТЕРАТУРЫ:

1. В России половина студентов использует ИИ в учебе // URL: <https://rg.ru/2023/08/25/v-rossii-polovina-studentov-ispolzuet-ii-v-uchebe.html> (дата обращения: 11.04.2024).
2. За кулисами интеллекта ChatGPT: рассказ о том, как определяют тексты, созданные ИИ // URL: <https://habr.com/ru/companies/antiplagiat/articles/728112/> (дата обращения: 10.04.2024).
3. Закон Ципфа // URL: <https://ru.megaindex.com/support/faq/zakon-zipfa> (дата обращения: 10.04.2024).
4. Антиплагиат выявляет текст, созданный ChatGPT // URL: <https://antiplagiat.ru/news/text-chatgpt/?ysclid=luzj6oz1gc143206311> (дата обращения: 09.04.2024).

## БЕЗОПАСНОСТЬ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ: УГРОЗЫ, СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИ

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

Ключевые слова: инфокоммуникационная система, защита информации, информационная сеть, техническая защита информации, физическая защита, квантовые технологии, квантовый интернет.

Стремительный рост технологий и развитие информационных систем приводят к увеличению числа угроз безопасности информации. В статье рассматриваются основные проблемы, связанные с обеспечением информационной безопасности в инфокоммуникационных сетях.

N.A. Baytyakov, K.L. Kostyuchenko

## INFOCOMMUNICATION SYSTEM SECURITY: THREATS, METHODS AND MEANS

Ural State University of Railways and Transport (USURT), Yekaterinburg, Russia

Keywords: infocommunication system, information protection, information network, technical information protection

Constant growth of technologies and development of information systems lead to increase of number of threats of information security. The article considers main problems related to information security in infocommunication networks.

Стремительный рост количества техники и быстрое развитие информационных технологий во всех сферах жизнедеятельности человека, заставляют все больше внимания уделять проблеме защиты информации. При передаче информации путем использования инфокоммуникационной сети (ИКС), пользователь сталкивается с множеством подводных камней и опасностей, обусловленных недоработками системы защиты ИКС.

Инфокоммуникационная сеть – совокупность вычислительных ресурсов, программно-аппаратных комплексов, методов передачи и хранения информации, благодаря инфокоммуникационным технологиям.

Информационная безопасность ИКС представляет собой способность системы противостоять воздействиям из вне. Для комплексного подхода в обеспечение сетевой безопасности, необходимо реализовать мониторинг сети, приближенный к реальному времени, распределение устройств контроля в пространстве, централизовать систему управления сетевой безопасностью. Благодаря данным мерам можно построить общую схему атак на ИКС, для дальнейшего обеспечения защиты.

При разработке конкретной системы требуется выявление всех возможных воздействий на объект информатизации. С усложнением архитектуры информационных систем, следует увеличение количества угроз. Основными угрозами являются: уничтожение, искажение или модификация информации и акты мошенничества. Таким образом для комплексной защиты определенного объекта требуется модель угроз безопасности ИКС. Данная схема включает в себя описание ресурсов ИКС, описание воздействий и их потенциальные возможности, жизненный цикл ИКС. В приложении к модели идет полный перечень угроз и база данных выявленных нарушений.

Одними из основных частей модели угроз являются объекты воздействия, способы воздействия и описание нарушителей. Нарушителями безопасности могут быть:

террористические организации, конкурирующие организации, спец службы иностранных государств, хакеры, бывшие сотрудники, авторизованные пользователи, поставщики/разработчики ПО. Действия нарушителей чаще всего настроены на ухудшение качественных характеристик функционирования ИКС, благодаря использованию эксплуатационных и технологических уязвимостей.

Цифровое развитие информационных технологий и увеличение количества техники приводят к необходимости усиления защиты информации в инфокоммуникационных сетях. Так, к примеру уже существующие воздействия на сети инфокоммуникации такие как несанкционированный доступ, побочные электромагнитные излучения и наводки, технические каналы утечки информации. Все вышеперечисленные методы воздействия хорошо изучены и для каждого из них существует множество тактик и методик для предотвращения. Относительно новыми видами воздействия можно назвать компьютерные атаки и программно-аппаратные воздействия, которые могут использовать разные стратегии получения информации.

Существует несколько направлений обеспечения защиты информации: правовая, техническая, криптографическая и физическая защита информации. Правовая защита информации подразумевает разработку и использование нормативно-правовых документов, регулирующих отношения субъектов. Техническая защита представляет собой обеспечение целостности ИКС не криптографическими методами. Криптографическая защита использует криптографические преобразования. Физическая защита производится путем применения ряда организационных мероприятий, направленных на защиту контролируемой зоны или препятствия злоумышленникам [1].

Новым открытием в инфокоммуникационных сетях стало использование квантовых технологий в передаче информации. Квантовый интернет — это сеть квантовых компьютеров, которые когда-нибудь будут отправлять, вычислять и получать информацию, закодированную в квантовых состояниях. Квантовый интернет не заменит современный или "классический" интернет; вместо этого он обеспечит новые функции, такие как квантовая криптография и квантовые облачные вычисления.

В обычных телекоммуникациях, таких как Интернет или телефонные линии, информация может быть потеряна на больших расстояниях. Чтобы бороться с этим, эти системы используют «ретрансляторы» в обычных точках, которые считывают и повторно усиливают сигнал, гарантируя, что он дойдет до места назначения в целостности и сохранности.

Классические ретрансляторы, однако, не могут быть использованы с квантовой информацией, так как любая попытка прочитать и скопировать информацию уничтожит ее. С одной стороны, это преимущество, так как квантовые соединения не могут быть «прослушены», не уничтожив информацию и не предупредив пользователей. Тем не менее, это проблема, которую необходимо решить для квантовых сетей на больших расстояниях.

Одним из способов преодоления этой проблемы является обмен квантовой информацией в виде запутанных частиц света или фотонов. Запутанные фотоны обладают такими свойствами, что вы не можете понять одно без другого. Чтобы разделить запутанность на больших расстояниях в квантовой сети, вам нужны два устройства: одно для создания запутанных фотонов, а другое для их хранения и последующего извлечения[2].

Существует несколько устройств, используемых для создания квантовой информации в виде запутанных фотонов и ее хранения, но и генерация этих фотонов по требованию, и наличие совместимой квантовой памяти для их хранения долгое время ускользали от исследователей.

Фотоны имеют определенные длины волн (которые в видимом свете создают разные цвета), но устройства для их создания и хранения часто настроены на работу с разными длинами волн, препятствуя их сопряжению.

Чтобы сделать устройства взаимосвязанными, команда создала систему, в которой оба устройства использовали одну и ту же длину волны. «Квантовая точка» производила (незапутанные) фотоны, которые затем передавались в систему квантовой памяти, которая хранила фотоны в облаке атомов рубидия. Лазер включал и выключал память, позволяя сохранять фотоны и высвобождать их по требованию.

Во-вторых, «квантовая угроза», исходящая от квантовых вычислений. Как упоминалось в предыдущем разделе, разложение целых чисел на множители — это один из типов задач, которые

квантовые компьютеры могут решать особенно эффективно. Большая часть нашей цифровой инфраструктуры и практически все, что мы делаем в Интернете — будь то видеоконференции, отправка электронных писем или доступ к нашему банковскому счету в Интернете — шифруется с помощью криптографических протоколов, основанных на сложности решения такого рода задач разложения целых чисел на множители (например, алгоритм RSA).

Первые квантовые датчики уже коммерчески доступны, что делает их наиболее зрелыми технологиями в области сенсорики, связи и вычислений. Более того, что касается квантовых коммуникаций и вычислений, ожидается, что гражданский сектор будет двигать вперед разработки, учитывая огромную потенциальную ценность, которую они имеют для гражданской промышленности.

Китай продемонстрировал стабильную коммуникационную сеть на основе квантового распределения ключей (QKD), охватывающую более 4600 км — крупнейшую и самую передовую сеть QKD в мире на сегодняшний день. Квантовая коммуникация использует фотоны для безопасного распространения «секретного ключа», позволяющего обмениваться зашифрованными сообщениями.

Сеть QKD соединяет четыре района — Пекин, Цзинань, Хэфэй и Шанхай — называемые Quantum Metropolitan Area Networks. Система имеет оптоволоконную линию протяженностью 2000 км между четырьмя городами и спутниковую линию протяженностью 2600 км между двумя обсерваториями — одна на востоке Пекина, а другая на границе Китая с Казахстаном.

Интегрированная квантовая сеть включает в себя 700 оптоволоконных линий связи и две линии связи «земля-спутник» с более чем 150 пользователями. Сеть подключается к спутнику квантовой связи Micius. Китай запустил Micius в 2016 году, который использовался для установления соединения QKD на расстоянии 7400 км между Пекином и Веней.

Оптоволоконные линии используют 32 релейных узла для передачи квантовой информации. Каждый из четырех QMAN имеет несколько релейных узлов, а также пользовательские узлы и оптические коммутаторы. Jinan QMAN, который поддерживает 95 пользовательских узлов, является самым большим из четырех QMAN.

В 2024 базовая ИТ-инфраструктура компании РЖД включает свыше 70 000 км магистральных волоконно-оптических линий связи. Для строительства квантовой сети нужны так называемые доверенные узлы. Их нужно ставить каждые 100 км, поскольку передаваемый сигнал затухает и его нужно расшифровывать и зашифровывать заново. Эксперты говорят, что у РЖД такие доверенные узлы есть.

Доверенный узел состоит из квантового приемника, связанного с квантовым передатчиком, который размещен на защищенной границе, предназначенной для предотвращения несанкционированного доступа. Они были спроектированы таким образом, чтобы компоненты квантовой системы — контроллер квантового ключа (QKC) и квантовый ключевой механизм (QKE) — помещались в стандартную плату или блейд-модуль ATCA (усовершенствованная архитектура телекоммуникационных вычислений) — стандартный телекоммуникационный форм-фактор, который защищен от вторжений и сертифицирован в соответствии со стандартом FIPS 140-2, уровень 3.

При питании и включении QKC QKE непрерывно генерирует поток кубитов, измеряет частоту ошибок и выполняет операции по исправлению ошибок и усилению конфиденциальности для поддержания хранилища кубитов, которые можно использовать для генерации ключей шифрования. Эти кубиты передаются в QKC, где они используются в качестве источника энтропии, общего для двух узлов.

Новые достижения в области исследований и разработок в области инфокоммуникационных сетей и квантовых технологий могут принести военным новые захватывающие возможности. Учитывая значительный интерес и финансирование квантовых технологий как со стороны гражданской промышленности, так и со стороны правительств, ожидается, что технология будет развиваться и что новые квантовые приложения станут доступны в ближайшие пять-десять лет.

Список литературы:



1. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // URL: <https://cyberleninka.ru/article/n/voprosy-bezopasnosti-infokommunikatsionnyh-sistem-i-setey-spetsialnogo-naznacheniya-osnovnye-ugrozy-sposoby-i-sredstva-obespecheniya?ysclid=lv22aqd56g137736207> (дата обращения: 10.04.2024).
2. Quantum Goes the Distance // URL: <https://www.bnl.gov/newsroom/news.php?a=214491> (дата обращения: 11.04.2024).

## ХАРАКТЕРИСТИКИ ПРЕДЕЛЬНЫХ ЗНАЧЕНИЙ ЧАСТОТЫ ДЛЯ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧ

РТУ МИРЭА, Россия

Ключевые слова: функция погрешности времени, относительное отклонение частоты, фазовая автоматическая подстройка частоты, погрешность частоты, цифровая система передач.

Показано, что предельные значения частоты для систем с фазовой автоматической подстройкой частоты описываются четырьмя основными характеристиками: полоса статического слежения, полоса динамического слежения, полоса синхронизации, полоса захвата.

К.А. Batenkov

## CHARACTERISTICS OF FREQUENCY LIMITS FOR DIGITAL TRANSMISSION SYSTEMS

RTU MIREA, Russia

Keywords: time error function, relative frequency deviation, phase automatic frequency adjustment, frequency error, digital transmission system.

It is shown that the frequency limits for systems with phase automatic frequency tuning are described by four main characteristics: the static tracking band, the dynamic tracking band, the synchronization band, and the capture band.

Функция погрешности времени  $x(t)$  (time error function) – разница между временами исследуемого тактового генератора  $T(t)$  и эталонного  $T_r(t)$  (рис. 1)

$$x(t) = T(t) - T_r(t).$$

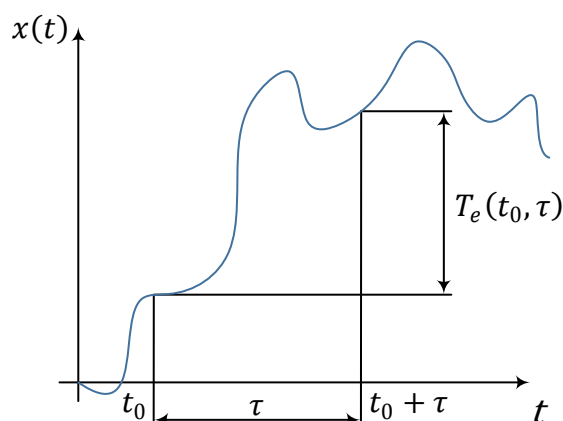


Рис. 1. Пример графика функций погрешности времени

Поскольку непрерывное значение функции погрешности времени  $x(t)$  практически неизмеримо, то рассматривают последовательность эквидистантных отсчетов

$$x_i = x[t_0 + (i - 1)\tau_0], i = 1, 2, \dots, N,$$

где  $t_0$  – момент начала измерений,  $\tau_0$  – временной интервал между соседними отсчетами (дискретизации).

Так как производной в непрерывном времени соответствует оператор разности в дискретном [1], то отсчеты относительного отклонения частоты

$$y_i = \frac{|x_{i+1} - x_i|}{\tau_0}, i = 1, 2, \dots, N - 1.$$

Соответственно период измерений  $\tau$  содержит целое число  $n$  отсчетов, то есть  $\tau = n\tau_0$  [2, 3].

Тогда погрешность частоты

$$y_m = \max_i y_i, i = 1, 2, \dots, N - 1.$$

Предельные значения частоты для систем с фазовой автоматической подстройкой частоты описываются четырьмя основными характеристиками: полоса статического слежения, полоса динамического слежения, полоса синхронизации, полоса захвата [1, 4].

Взаимосвязь отсчетов функции времени  $T_i$ , полной (обобщенной) мгновенной фазы  $\Phi_i$ , времени эталонного генератора  $T_{r,i}$  и погрешности времени  $x_i$  имеют вид:

$$T_i = \frac{\Phi_i}{2\pi\nu_0} \\ x_i = T_i - T_{r,i}.$$

*Полоса статического слежения (hold-in range)* – наибольшее смещение частоты входного опорного сигнала от номинальной частоты, в пределах которого ведомое устройство продолжает оставаться в режиме синхронизации при медленном изменении частоты во всем диапазоне частот. Таким образом в полосе статического слежения устройство способно отслеживать медленные (квазистационарные) вариации частоты синхросигнала [5].

*Полоса динамического слежения (pull-out range)* – наибольшее смещение частоты входного опорного сигнала от номинальной частоты, в пределах которого ведомое устройство продолжает оставаться в режиме синхронизации, а за пределами которой нет, независимо от скорости изменения частоты. Таким образом в полосе динамического слежения устройство способно отслеживать быстрые скачки частоты синхросигнала.

*Полоса асинхронизации (lock-in range)* – наибольшее смещение частоты входного опорного сигнала от номинальной частоты, в пределах которого ведомое устройство быстро переходит на новую частоту синхронизации.

*Полоса захвата (pull-in range)* – наибольшее смещение частоты входного опорного сигнала от номинальной частоты, в пределах которого ведомое устройство переходит в режим синхронизации независимо от скорости захвата входного сигнала.

Все четыре вышеприведенные характеристики описываются на основе параметра погрешности частоты  $y_m$ , то есть в относительных единицах, не смотря на то, что определения даны в абсолютных.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Брени С. Синхронизация цифровых сетей связи / Стефано Брени ; Пер. с англ. Н. Л. Бирюкова, С. Я. Несвитской, Н. Р. Триски ; Под ред. А. В. Рыжкова. – М. : Мир, 2003. – 417 с.
2. Jitter and Wander Test Solutions. Synchronization – Jitter – Wander: Basic Principles and Test Equipment. – 32 p.
3. Сообщение по применению 1264-1. Синхронизация телекоммуникационных сетей: основные понятия. – Hewlett-Packard, 1995. – 26 p.
4. Батенков К.А. Моделирование непрерывных каналов связи в форме операторов преобразования некоторых пространств // Труды СПИИРАН. 2014. № 1 (32). С. 171-198.
5. Rec. G.810. Definitions and terminology for synchronization networks. – 1996–08. – Geneva : ITU-T, 1996. – 27 p.

## АНАЛИЗ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИЗУЧЕНИЯ СВОЙСТВ ЖИДКОСТИ ОПТИЧЕСКИМ ИЗЛУЧЕНИЕМ

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

Ключевые слова: измерения, свойства жидкости, оптическое излучения, оптико-электронный приборы, анализ свойств.

В статье проведен литературный обзор исследований в области изучения свойств жидкости при помощи оптического излучения. Сделаны выводы о необходимости дальнейших исследований в данном направлении, а также в направлении передачи информации через различные среды распространения.

D.I. Burumbaev, N.M. Barbin

## ANALYSIS OF RESEARCH IN THE FIELD OF STUDYING THE PROPERTIES OF LIQUIDS BY OPTICAL RADIATION

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

Keywords: measurements, liquid properties, optical radiation, optoelectronic devices, property analysis.

The article provides a literary review of research in the field of studying the properties of a liquid using optical radiation. Conclusions are drawn about the need for further research in this direction, as well as in the direction of information transmission through various distribution media.

На данный момент уже существует множество публикаций или патентов, связанных с изучением свойств воды и водных растворов. Также вызывает интерес и области, в которых применяются исследование жидкостей при помощи оптического излучения.

В работе «Оптическое волокно как основа для создания датчиков идентификации жидкостей и определения концентрации растворов» рассматривается вопрос использования оптического волокна как основы датчиков. Предложено использовать в качестве информационного параметра величину пика рефлектограммы для идентификации жидкостей, имеющих разные показатели преломления, а также определения концентрации растворенных в воде веществ [1].

Также, в другой работе авторов А. О. Зеневич и другие, установили, что волоконно-оптический датчик может работать на любой длине волны оптического излучения, соответствующей окнам прозрачности спектра оптических потерь волокна. Исследовали влияние длины оптического волокна между регистрирующим устройством и местом определения концентрации раствора жидкости с помощью волоконно-оптического датчика [2].

В статье «Волоконно-оптические датчики для контроля параметров состояния объектов и окружающей среды в задачах мониторинга» авторы исследуют возможность применение волоконно-оптических датчиков для мониторинга природно-технических систем. В исследовании рассматривают возможность применения датчиков на различных принципах: на рессеянии, интерференционные, на основе внутриволоконных решеток, на основе рамановской спектроскопии. Авторы отдельно подчеркивают, что для исследования свойств водных растворов, наиболее оптимальным способом является рамановская спектроскопия [3].

В работе авторов Н.Р. Рахимов, Е.Ю. Кутенкова, Д.Д. Исломов, Ш.И. Мадумаров предлагается математическая модель оптоэлектронного фотоколориметра для автоматического контроля оптических параметров жидких сред, особенностью которого является двукратное прохождение светового потока через исследуемую полупрозрачную жидкость. Рассмотрена зависимость оптического и электрического сигналов от свойств жидкостей [4].

В другой статье этих же авторов, анализируются существующие средства мониторинга жидких сред. Также, уточняется, что в зависимости от химического состава вещества и количественного соотношения составляющих его элементов изменяется интенсивность светопоглощения, угол отражения и другие характеристики взаимодействия светового излучения и вещества [5].

В работе «Возможности методов оптической спектроскопии для исследования воды и водных растворов с нанопузырьковой газовой фазой», группа авторов проводит анализ спектров ультрафиолетовой, инфракрасной и терагерцовой спектроскопии артезианской воды и водных растворов NaCl с нанопузырьковой фазой газов разной природы (азот, аргон, кислород, воздух). В результате эксперимента были сделаны следующие выводы: ИК-спектры нечувствительны к изменениям состояния водных систем, связанным с формированием нанопузырьковой газовой фазы; изменения интенсивности УФ-спектров коррелируют с изменениями величины pH и параметрами нанопузырьковой газовой фазы. Терагерцовые спектры позволяют оценить изменение количества водородных связей в водном растворе [6].

В работе А.П. Маркова «Анализ оптико-электронных приборов технологического контроля жидких сред» рассмотрены методы и средства оптического контроля жидкостных сред. Приведены схемы одноканального и двухканального датчиков для измерения свойств жидкости. Но для данных способов выделяют явные недостатки: влияния на процесс измерения нестабильности источника излучения, наличие внешней засветки, загрязнение торцов световодов [7].

В статье «Оптический способ регистрации параметров жидкостных потоков» авторы приходят к выводу, что для измерения необходимых параметров (давления, объема, расхода, скорости, силы) различных типов жидкостей в разных узлах, предпочтительно использовать оптические методы. По сравнению с механическими способами измерения, предлагаемые более надежны, чувствительны и точны [8].

В работе авторов А.А. Семёнов, В.Я. Савицкий «Перспективные системы анализа жидкости» проведен анализ устройств для оптического контроля жидкостей и газов. Например, бензин, масла, технические жидкости нуждаются в измерении количественных и качественных параметров непосредственно в процессе эксплуатации для поддержания работоспособности различных устройств. В качестве устройства для измерения предлагается использовать оптический спектрометр [9].

В статье «Связь между оптическими и теплофизическими свойствами жидкостей» Джафарова А.Н. рассматривает теоретическую задачу, возникающую при взаимодействии лазерных лучей с жидкостью на основе решения уравнения сохранения энергии установлена связь между теплофизическими и оптическими свойствами жидкостей. Полученные формулы позволяют вычислить значения теплофизических параметров, зная оптические параметры [10].

Таким образом, исходя из проведенного анализа литературы, можно сделать вывод, что:

- 1) Исследования в области применения оптического излучения для изучения свойств жидкостей остаются актуальными;
- 2) Исследуемые направления могут применяться в различных сферах жизнедеятельности человека;
- 3) Малое количество исследований направлено на изучение зависимостей оптических параметров от типа жидкости;
- 4) Также, небольшое количество литературы направлено на изучение свойств передачи данных в зависимости от типа жидкости, в которой передается сигнал.

#### Список литературы:

1. Оптическое волокно как основа для создания датчиков идентификации жидкостей и определения концентрации растворов / А. О. Зеневич, Т. М. Мансуров, Т. Г. Коваленко [и др.]

- // Известия высших учебных заведений. Приборостроение. – 2022. – Т. 65, № 12. – С. 895-901. – DOI 10.17586/0021-3454-2022-65-12-895-901. – EDN HYDZUM
2. Волоконно-оптический датчик идентификации жидкостей и определения концентрации растворов / А. О. Зеневич [и др.] // Доклады БГУИР. 2023. Т. 21, № 6. С. 14–20. <http://dx.doi.org/10.35596/1729-7648-2023-21-6-14-20>.
  3. Волоконно-оптические датчики для контроля параметров состояния объектов и окружающей среды в задачах мониторинга / А. И. Вялышев, В. М. Добров, А. А. Долгов [и др.] // Природообустройство. – 2014. – № 3. – С. 32-37. – EDN STHXBL.
  4. Математическая модель оптоэлектронного преобразователя для мониторинга жидких сред / Н. Р. Рахимов, Е. Ю. Кутенкова, Д. Д. Исломов, Ш. И. Мадумаров // Автоматика и программная инженерия. – 2012. – № 2(2). – С. 36-40. – EDN VJNNSZ
  5. Кутенкова Елена Юрьевна, Рахимов Бахтиержон Нематович, Ларина Татьяна Вячеславовна, Мадумаров Шерзод Ильхомович Исследование оптоэлектронного метода и разработка устройств для мониторинга жидких сред // Автоматика и программная инженерия. 2012. №1 (1). URL: <https://cyberleninka.ru/article/n/issledovanie-optoelektronnogo-metoda-i-razrabotka-ustroystv-dlya-monitoringa-zhidkih-sred>
  6. Канунникова Ольга Михайловна, Аксенова Валерия Викторовна, Трубачев Алексей Владиславович, Назаров Максим Михайлович, Кропачева Татьяна Николаевна, Кожевников Владимир Изосимович Возможности методов оптической спектроскопии для исследования воды и водных растворов с нанопузырьковой газовой фазой // Химическая физика и мезоскопия. 2018. №2. URL: <https://cyberleninka.ru/article/n/vozmozhnosti-metodov-opticheskoy-spektroskopii-dlya-issledovaniya-vody-i-vodnyh-rastvorov-s-nanopuzyrkovoy-gazovoy-fazoy>
  7. Марков А. П. Анализ оптико-электронных приборов технологического контроля жидких сред // Вестник Белорусско-Российского университета. 2006. №2. URL: <https://cyberleninka.ru/article/n/analiz-optiko-elektronnyh-priborov-tehnologicheskogo-kontrolya-zhidkih-sred>
  8. Оптический способ регистрации параметров жидкостных потоков / Т. И. Мурашкина, Е. А. Бадеева, Д. И. Серебряков [и др.] // Инновационные, информационные и коммуникационные технологии. – 2019. – № 1. – С. 295-299. – EDN MFQCCO.
  9. Семенов, А. А. Перспективные системы анализа жидкости / А. А. Семенов, В. Я. Савицкий // Военное обозрение. – 2022. – № 1(11). – С. 7-10. – EDN XZBJQQ.
  10. Джафарова А.Н. Связь между оптическими и теплофизическими свойствами жидкостей // Актуальные проблемы гуманитарных и естественных наук. 2017. №1-3. URL: <https://cyberleninka.ru/article/n/svyaz-mezhdu-opticheskimi-i-teplofizicheskimi-svoystvami-zhidkostey>

## ИССЛЕДОВАНИЕ ВЛИЯНИЯ FBT И PLC РАЗВЕТВИТЕЛЕЙ НА ДИАГРАММЫ УРОВНЕЙ СИГНАЛОВ В СЕТИ GPON

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

Ключевые слова: оптический, разветвитель, PLC, FBT, GPON, PON

В статье приведены структурные схемы сети PON с использованием двух различных типов разветвителей FBT и PLC, таблица с реальными характеристиками оптических разветвителей, сравнительные графики и графики зависимости разветвителей в зависимости от типа и числа деления по оптическим каналам, также произведен анализ по графикам и подведен вывод об зависимости вносимых потерь от типа разветвителя и числа делений по каналам.

A.A. Vorobyev, I.I. Shestakov

## STUDY OF THE INFLUENCE OF FBT AND PLC SPLITTERS ON SIGNAL LEVEL DIAGRAMS IN GPON NETWORK

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

Keywords: optical, splitter, PLC, FBT, GPON, PON

The article contains structural schemes of PON network using two different types of splitters FBT and PLC, a table with real characteristics of optical splitters, comparative graphs and graphs of the dependence of splitters depending on the type and number of divisions on optical channels, also analyzed the graphs and summarized the dependence of insertion loss on the type of splitter and the number of divisions on the channels.

В современных сетях передачи данных, таких как сети GPON (Gigabit Passive Optical Network), использование разветвителей сигнала играет ключевую роль в обеспечении эффективной передачи информации. В данной статье рассматривается влияние двух основных типов разветвителей - FBT (Fused Biconic Taper) и PLC (Planar Lightwave Circuit) на диаграммы уровней сигналов в сетях GPON. Исследование проводится с целью определения оптимального выбора разветвителя для обеспечения стабильной и качественной передачи данных в сетях GPON.

PLC (Planar Lightwave Circuit) — планарные разветвители. Производятся по технологии, использующей вытравливание волноводов на кристалле кремния в соответствии с необходимой конфигурацией каналов. Возможен выбор моделей с различным количеством ответвлений: 1:2, 1:4, 1:8, 1:16, 1:24, 1:32 (до 2:64). [1]

Преимущества PLC сплиттеров:

1. высокая стабильность и точность параметров;
2. меньшая вероятность появления сбоев;
3. равномерность деления оптического потока;
4. компактность;
5. работа в широком волновом диапазоне (1260–1650 нм).

Недостаток: деление принимаемой мощности лишь в соотношении 50 на 50, без возможности изменения этой пропорции.

Основная область применения:

• сети, по которым транслируется кабельное телевидение, и пассивные сети GPON/GEPON. Сплиттеры устанавливаются у абонентов, позволяя выделить индивидуальный канал из группового. [2]

FBT (Fused Biconical Taper) — сплавные разветвители. Изготавливаются по технологии сплавления боковых поверхностей или торцов стандартного одномодового и многомодового стекловолокна. Число ответвлений может выполняться в разных вариантах:  $1 \times 2 \dots 32 \times 32$ . Мощность излучения делится по портам в необходимом процентном соотношении с интервалом 1 %. [3]

Преимущества FBT сплиттеров:

1. малые вносимые потери;
2. большой коэффициент направленности;
3. минимальные отклонения от заданного коэффициента ответвления;
4. сохранение заявленных параметров в зависимости от ширины волнового спектра вводимого излучения;
5. распределение мощности между выходными полюсами: равномерное и заданное заказчиком;
6. рабочая длина волны: 1310, 1490, 1550 нм;
7. низкий уровень поляризационных потерь;
8. высокая температурная стабильность.

Главное преимущество FBT сплиттеров — достижение нужного коэффициента деления канала (10%/90%, 15%/85% и т. д.). Это свойство особенно полезно при построении сети, где нужно сделать ответвления для абонентов, которые от точки деления находятся на разном расстоянии.

Недостатки FBT сплиттеров: потери, которые зависят от длины волны света; невысокая однородность светового потока; значительное различие в мощности между выходами; сильная зависимость потерь от температуры; большие размеры.

FBT разветвители применяются в следующих областях:

• Сети передачи кабельного телевидения (CATV). В этом случае сплиттеры используются в качестве ADM (add drop module) — меньшая часть оптического сигнала выделяется, а большая передаётся далее по трассе.

• Пассивные оптические сети (PON, GPON). В этом случае сплиттеры устанавливаются по трассе между оптическим линейным терминалом (OLT), расположенным в центральном узле связи, и абонентским оптическим сетевым терминалом (ONT).

В работе была рассмотрена двухкаскадная схема оптической распределительной сети PON с применением двух типов разветвителей PLC и FBT. [4]

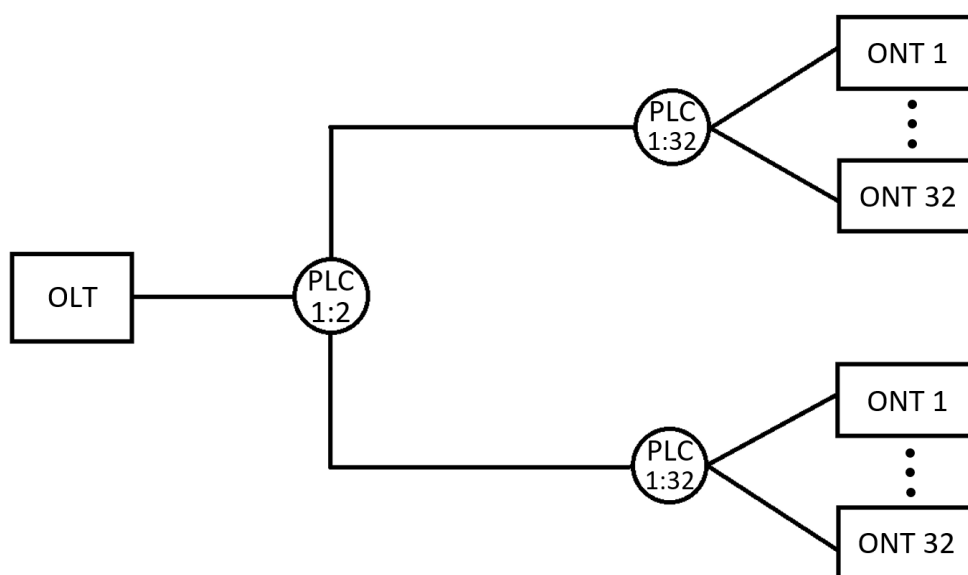


Рис. 1 – Двухкаскадная структурная схема сети GPON с применением разветвителей типа PLC 1:2 и разветвителей типа PLC 1:32



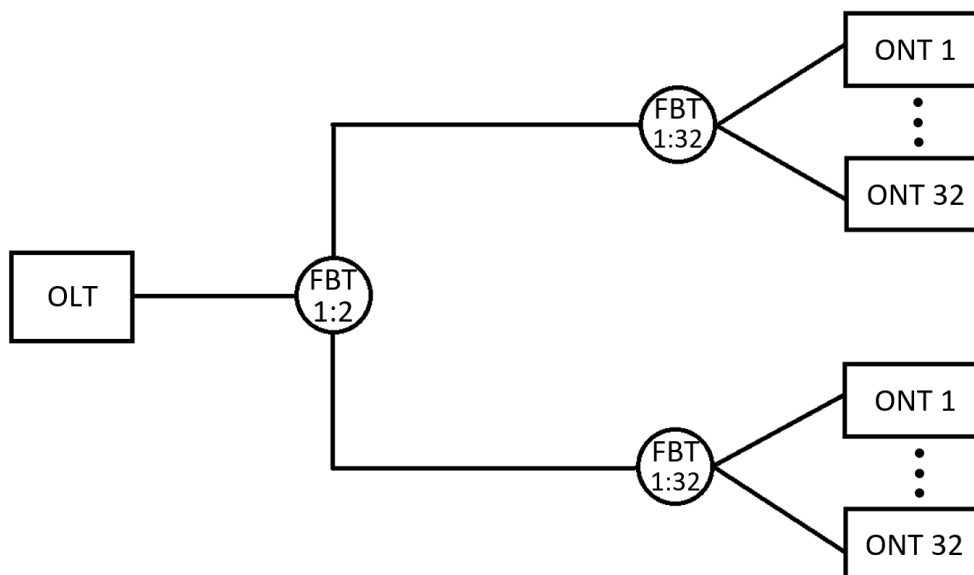


Рис. 2 – Двухкаскадная структурная схема сети GPON с применением разветвителей типа FBT 1:2 и разветвителей типа FBT 1:32

Ниже, представлена таблица, описывающая реальные характеристики оптических разветвителей в зависимости от числа делений по каналам, а также в зависимости от типа разветвителя.

Таблица 1 – Реальные характеристики оптических разветвителей типа PLC и FBT с числом делений по каналам 1:2 и 1:32 [5], [6], [7], [8]

Тип разветвителя	PLC 1:2	PLC 1:32	FBT 1:2	FBT 1:32
Габаритные размеры, мм	4x12x60	6x20x80	100x80x10	140x115x18
Диапазон рабочих длин волн, нм	1260...1650	1260...1650	1310/1550	1310/1550
Вносимые оптические потери, дБ	3.9	16.6	3.6	16,4
Поляризационные потери, дБ	0.2-0.4	0.2-0.4	≤0.15	≤0.5
Направленность, дБ	55	55	55	55
Обратные потери, дБ	55	55	55	55
Тип волокна	G.657	G.657	G.657	G.657
Стандартная длина кабельных отводов, м	1	1	1	1
Рабочая температура,	-40 ~ +85	-20 ~ +50	-20 ~ +50	-20 ~ +50
Температура хранения	-40 ~ +85	-40 ~ +85	-40 ~ +85	-40 ~ +85
Производитель	Component	Component	Component	Component

Диаграммы сравнения вносимых оптических потерь, строились на основе данных из таблицы 1, а именно из суммы вносимых и поляризационных потерь, для наглядности.

Ниже, на рисунках 3, 4 и 5 представлены диаграммы сравнения изменения оптических потерь в зависимости от типа разветвителя и числа деления по каналам связи.

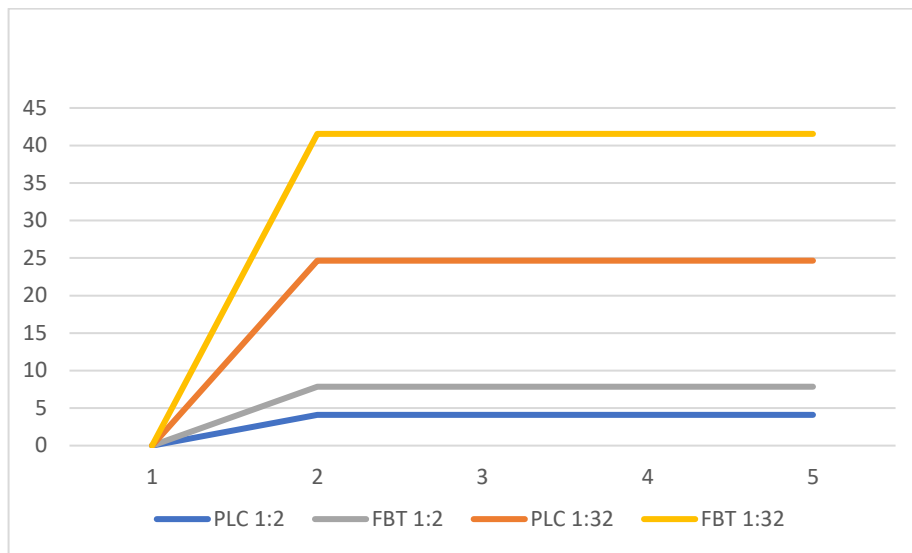


Рис. 3 – Сравнительный график оптических потерь для разных типов разветвителей

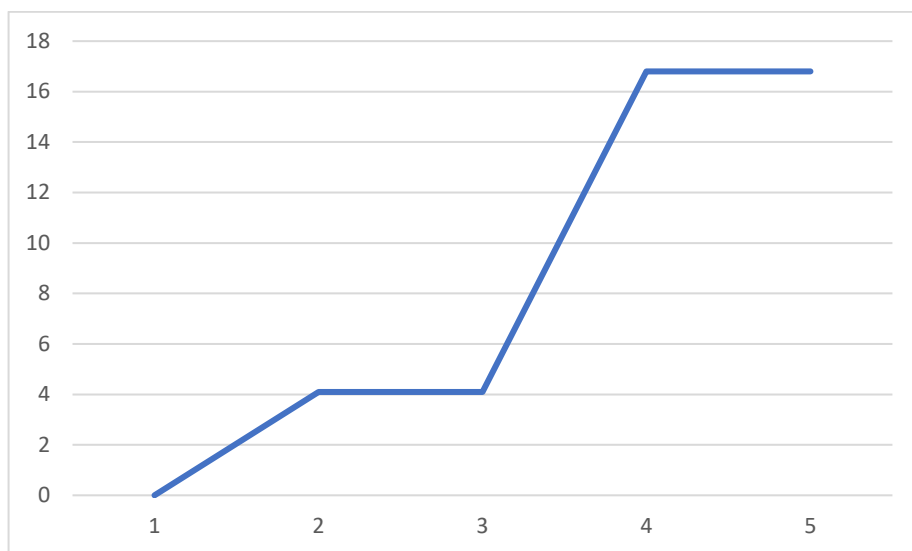


Рис. 4 – График зависимости вносимых потерь, для двухкаскадной схемы PON, от числа разветвлений в разветвителях типа PLC

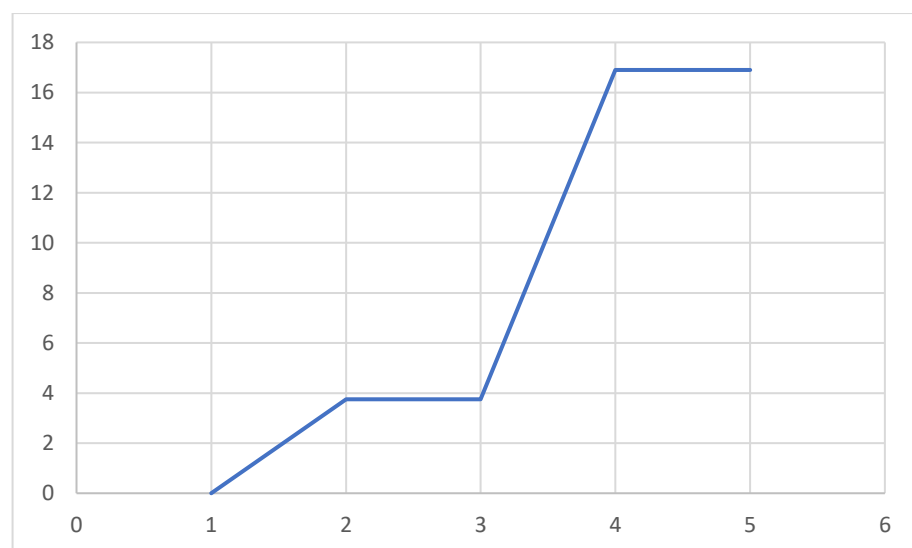


Рис. 5 – График зависимости вносимых потерь, для двухкаскадной схемы PON, от числа делений в разветвителях типа FBT

Рассмотрев на примере графиков изменения оптических потерь в зависимости от числа ответвлений в разветвителях PLC и FBT, можно судить о том, что оптические потери отличаются для двух типов разветвителей на небольшое число, приблизительно равное 0,3 дБ. В данном случае не учитывались другие потери, вносимые в оптический канал, а брались только потери, возникающие при прохождении сигналом оптического разветвителя. С уверенностью можно сказать, что разветвители PLC вносят меньше оптических потерь в канал связи, по причине того, что FBT сплиттеры, более чувствительны к длине волны света и предоставляют возможность неравномерного разделения мощности по каналам.

Подводя итог, можно судить о том, что теоретически разветвители типа FBT должны вносить меньше потерь в оптический канал, но при применении их на реальных сетях связи, стало понятно, что факторы, влияющие на изменения вносимых потерь, оказывают сильное влияние на конечное число. Можно заключить, что при увеличении числа деления в оптическом разветвителе, увеличиваются и оптические потери, которые данный разветвитель вносит в канал оптической связи. Причиной этому являются: потери на отражении, из-за увеличения количества сварных соединений, избыточное рассеяние из-за оптических неоднородностей в волокне, изгибные потери, загрязнение волокна, температурные изменения и неравномерное распределение оптической мощности по каналам, с увеличением числа каскадов падает и равномерность распределения оптической мощности по каналам.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Савин Е.З. Волоконно-оптические кабели и пассивные элементы ВОЛП: учебное пособие для вузов: 2021. 184с.
2. В. И. Ефанов Проектирование, строительство и эксплуатация ВОЛС: учебное пособие для вузов: 2012. 22 с.
3. В.И. Ефанов Проектирование волоконно - оптических линий связи: учебное пособие для вузов: 2007. 87 с.
4. Горлов Н.И. Оптические линии связи и пассивные компоненты ВОСП: учебное пособие для вузов: 2033. 58 с.
5. Официальный сайт интернет - магазина Компонент, разветвитель PLC 1:2 [Электронный ресурс]. URL: <https://componentltd.ru/catalog/razvetviteli-planarnye-plc/opticheskiy-splitter-plc-1-2-0-9mm-3sc-apc/>
6. Официальный сайт интернет - магазина Компонент, разветвитель PLC 1:32 [Электронный ресурс]. URL: <https://componentltd.ru/catalog/razvetviteli-planarnye-plc/opticheskiy-splitter-plc-1x32-0-9mm-33sc-apc/>
7. Официальный сайт интернет - магазина Компонент, разветвитель FBT 1:2 [Электронный ресурс]. URL: <https://componentltd.ru/catalog/splavnye-razvetviteli/opticheskiy-splitter-fbt-1-2-50-50-3-0-mm/>
8. Официальный сайт интернет - магазина Компонент, разветвитель FBT 1:32 [Электронный ресурс]. URL: <https://componentltd.ru/catalog/splavnye-razvetviteli/opticheskiy-splitter-fbt-1-32-3-0-mm/>

## О СОВМЕШНОМ РАСПРЕДЕЛЕНИИ ВРЕМЕНИ ДО ОТКАЗА И ВРЕМЕНИ ВОССТАНОВЛЕНИЯ

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

Ключевые слова: техническое состояние объекта, интенсивность отказа, интенсивность восстановления, показательный закон распределения, равномерный закон распределения, полумарковский процесс, марковская модель.

В статье рассматривается совместное распределение времени до отказа технического объекта, описываемого показательным распределением и времени восстановления, описываемого равномерным распределением. Приведены варианты диаграмм состояний-переходов технического объекта при различных вариантах распределения интенсивностей переходов, а также получены вероятностные и временные характеристики для описанных диаграмм.

V.P. Shuvalov, B.P. Zelentsov, I.G. Kvitkova

## ON THE COMBINED DISTRIBUTION OF TIME TO FAILURE AND RECOVERY TIME

Siberian State University of Telecommunications and Information Science (SibSUTIS),  
Novosibirsk, Russia

Keywords: technical condition of the object, failure rate, recovery rate, exponential distribution law, uniform distribution law, semi-Markov process, Markov model.

The article considers the combined distribution of the time to failure of a technical object, described by an exponential distribution, and the recovery time, described by a uniform distribution. Variants of diagrams of state transitions of a technical object are given for different variants of the distribution of transition rates, as well as probabilistic and temporal characteristics for the described diagrams are obtained.

Согласно ГОСТ 18322-2016 [1] техническое состояние (ТС) объекта – это совокупность свойств объекта, подверженных изменению в процессе его производства, эксплуатации, транспортировки и хранения, характеризуемых значениями параметров и/или качественными признаками, установленными в документации. Такими состояниями являются: исправное состояние, неисправное состояние, неработоспособное состояние и предельное состояние. Под предельным состоянием при эксплуатации объекта обычно понимается отказ. Рассматриваются два состояния – исправное и отказ. Соответствующие переходы из состояния в состояние условно показаны на рис. 1. Здесь состояние 1 – это исправное состояние, а состояние 2 – отказ. В результате ремонта имеет место переход из состояния 2 в состояние 1.

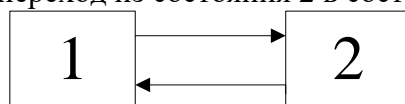


Рис. 1. Переходы объекта из состояния в состояние

Для характеристики переходов  $1 \rightarrow 2$ ,  $2 \rightarrow 1$  используются различные распределения.

Показательное распределение используется в математических моделях для описания случайных величин, в частности:

- времени до отказа;
- времени завершения восстановления;

- продолжительности ремонта оборудования;
- времени между проверками технического состояния оборудования.

Постоянная интенсивность восстановления заложена в стандартах ГОСТ Р 27.102-2021 [2], ГОСТ Р МЭК 61165-2019 [3]. Интенсивность ремонта заложена в ГОСТ Р МЭК 61165-2019 [3].

Показательное распределение времени до отказа обосновано вероятностными и статистическими методами. Однако использование показательного распределения для времени восстановления приводится, как правило, без обоснования.

В большинстве математических моделей время до отказа и время восстановления распределены по показательному (экспоненциальному) закону. Это позволяет использовать марковскую модель в непрерывном времени.

Рассмотрим случай, когда время до отказа распределено по показательному закону, а время восстановления – равномерно [4].

В таблице 1 приведены характеристики показательного и равномерного распределений, при этом время отсчитывается от момента попадания в состояние ( $t = 0$ ).

Таблица 1. Характеристики показательного и равномерного распределений

Характеристика	Событие	
	Отказ	Завершение восстановления
Плотность распределения	$f(t) = \lambda \cdot e^{-\lambda t}, t \geq 0$	$f(t) = \frac{1}{T}, 0 \leq t \leq T$
Интенсивность $\lambda(t) = f(t) / p(t)$	$\lambda(t) = \lambda$	$\lambda(t) = \frac{1}{T-t}$
Вероятность того, что событие не произойдет на интервале $[0; t]$	$P(t) = e^{-\lambda t}$	$P(t) = \frac{T-t}{T}$
Вероятность того, что событие произойдет на интервале $[0; t]$	$F(t) = 1 - e^{-\lambda t}$	$P(t) = \frac{t}{T}$

На рис. 2 приведена диаграмма состояний-переходов системы при различных распределениях интенсивностей переходов. В состоянии  $S_0$ , начиная с момента  $t = 0$ , имеет место совместное распределение показательного и равномерного распределений.

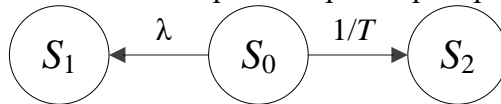


Рис. 2. Диаграмма состояний-переходов при различных распределениях интенсивностей переходов

Вероятность того, что в течение времени  $t$  состояние  $S_0$  не изменится:

$$p_{00}(t) = \frac{T-t}{T} \cdot e^{-\lambda t}, t \in [0; T].$$

Вероятность перехода  $S_0 \rightarrow S_1$  на интервале  $[t; t+dt]$ :

$$p_{01}(t; t+dt) = \frac{T-t}{T} \cdot \lambda \cdot e^{-\lambda t} \cdot dt, t \in [0; T].$$

Вероятность перехода  $S_0 \rightarrow S_1$  на интервале  $[0; t]$ :

$$p_{01}(t) = \int_0^t \frac{T-\tau}{T} \cdot \lambda \cdot e^{-\lambda \tau} \cdot d\tau = \frac{1}{\lambda \cdot T} \cdot [\lambda \cdot t \cdot e^{-\lambda t} - (1 - \lambda \cdot T) \cdot (1 - e^{-\lambda t})].$$

Вероятность перехода  $S_0 \rightarrow S_2$  на интервале  $[t; t+dt]$ :

$$p_{02}(t; t+dt) = e^{-\lambda t} \cdot \frac{dt}{T}.$$

Вероятность перехода  $S_0 \rightarrow S_2$  на интервале  $[0; t]$ :

$$p_{02}(t) = \int_0^t e^{-\lambda \tau} \cdot \frac{d\tau}{T} = \frac{1 - e^{-\lambda t}}{\lambda \cdot T}.$$

Проверка:

$$p_{00}(t) + p_{01}(t) + p_{02}(t) = 1.$$

Вероятности переходов при  $t = T$ :

$$p_{00}(T) = 0; \quad p_{01}(T) = 1 - \frac{1 - e^{-\lambda T}}{\lambda \cdot T}; \quad p_{02}(T) = \frac{1 - e^{-\lambda T}}{\lambda \cdot T}. \quad (1)$$

Проверка:

$$p_{00}(T) + p_{01}(T) + p_{02}(T) = 1.$$

Среднее время нахождения в состоянии  $S_0$  после попадания в него:

$$T_0 = \int_0^T p_{00}(t) \cdot dt = \frac{1}{\lambda} \cdot \left( 1 - \frac{1 - e^{-\lambda T}}{\lambda \cdot T} \right). \quad (2)$$

Вероятности  $p_{01}$  и  $p_{02}$  из (1), а также среднее время  $T_0$  из (2) могут быть использованы в модели на основе полумарковского процесса [5].

Если время до отказа и время восстановления распределены по показательному закону, то диаграмма состояний-переходов имеет вид, показанный на рис. 3.

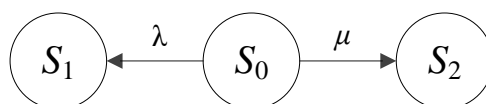


Рис. 3. Диаграмма состояний-переходов при показательном распределении интенсивностей переходов

Вероятности переходов между состояниями в непрерывном времени:

$$p_{00}(t) = e^{-(\lambda+\mu)t}; \quad p_{01}(t) = \frac{\lambda}{\lambda + \mu} \cdot [1 - e^{-(\lambda+\mu)t}]; \quad p_{02}(t) = \frac{\mu}{\lambda + \mu} \cdot [1 - e^{-(\lambda+\mu)t}].$$

Переходные вероятности полумарковского процесса (при  $t \rightarrow \infty$ ) определяются выражениями из (3):

$$p_{00} = 0; \quad p_{01} = \frac{\lambda}{\lambda + \mu}; \quad p_{02} = \frac{\mu}{\lambda + \mu}. \quad (3)$$

Среднее время нахождения в состоянии  $S_0$  после попадания в него в этом случае определяется выражением (4):

$$T_0 = \frac{1}{\lambda + \mu}. \quad (4)$$

В процессе эксплуатации технический объект из работоспособного состояния может перейти в неработоспособное состояние вследствие отказа. Восстановление приводит объект обратно в работоспособное состояние. Переходы из состояния в состояние могут быть описаны моделью марковского или полумарковского процесса в зависимости от характера распределения интенсивностей переходов (интенсивности отказа и восстановления). Вероятности переходов между состояниями и среднее время нахождения в том или ином состоянии являются характеристиками модели надежности объекта. Полученные выражения определить комплексные показатели надежности технического объекта или системы.

#### СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ 18322-2016. Система технического обслуживания и ремонта техники. Термины и определения [Текст]. – Введ. 2017-09-01. - М.: Стандартинформ, 2017. - 16 с.
2. ГОСТ Р 27.102-2021. Надежность в технике: надежность объекта. Термины и определения [Текст]. – Введ. 2022-01-01. - М.: Российский институт стандартизации, 2021. - 36 с.
3. ГОСТ Р МЭК 61165-2019. Надежность в технике. Применение марковских методов [Текст]. – Введ. 2019-12-01. - М.: Стандартинформ, 2019. - 31 с.
4. Проектирование и техническая эксплуатация цифровых телекоммуникационных сетей / Е.Б. Алексеев, В.Н. Гордиенко, В.В. Крухмалев и др. М.: Горячая линия – Телеком, 2008. 392 с.
5. Зеленцов Б.П. Матричные методы моделирования однородных марковских процессов. – Palmarium Academic Publishing, 2017. – 133 с.

## 3D-СИМУЛЯТОР ДЛЯ ДЕМОНСТРАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ СИСТЕМАМИ СВЯЗИ

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

Ключевые слова: 3d-моделирование, 3d-симулятор, 3ds Max, Unity3D, информационная система, программные коды, газовые краны, пульт оператора, служба технологической связи, телемеханика.

В настоящей работе описан инструментарий и разработка компьютерного 3d-симулятора для демонстрации процесса управления системами связи без отрыва от производства, который предназначен для отработки профессиональных знаний, умений и навыков в процессе работы с реальной системой.

Показано, что по итогам тестирования разработанный симулятор справляется с поставленной задачей.

A.V. Zemskov, I.A. Malkova

## 3D SIMULATOR FOR DEMONSTRATION THE PROCESS OF MANAGING COMMUNICATION SYSTEMS

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, program codes, gas valves, operator console, technological communication service, telemechanics.

At the presented paper describes the tools and development of a computer 3d simulator to demonstrate the process of managing communication systems on the job, which is designed to develop professional knowledge, skills and abilities in the process of working with a real system.

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

**Целью** настоящей работы является разработка 3D-симулятора для демонстрации процесса управления системами связи на предприятии.

### **Задачи:**

1. Создать диаграммы;
2. Выбор игрового движка;
3. Выбор системы связи проектирования;
4. Создание 3d-моделей;
5. Создание UV-разверток 3d-моделей;
6. Создание текстур 3d-моделей;
7. Разработка игровой логики;
8. Написание программных скриптов.

### **1. Создание диаграмм.**

На данном этапе создана диаграмма претендентов, диаграмма, отражающая отношения между акторами и прецедентами и являющаяся составной частью модели прецедентов, позволяющей описать систему на концептуальном уровне.

Прецедент — возможность моделируемой системы (часть её функциональности), благодаря которой пользователь может получить конкретный, измеримый и нужный ему результат. Прецедент соответствует отдельному сервису системы, определяет один из вариантов её использования и описывает типичный способ взаимодействия пользователя с системой. Варианты использования обычно применяются для спецификации внешних требований к системе. Основное назначение диаграммы — описание функциональности и поведения, позволяющее заказчику, конечному пользователю и разработчику совместно обсуждать проектируемую или существующую систему.

При моделировании прецедентов системный аналитик стремится:

- Конкретно отделить систему от её окружения;
- Определить язык или система программирования) при составлении модели прецедентов опускаются (для них составляется другой документ



Рис. 1. Диаграмма прецедентов

### 1.1 Создание диаграммы перспективы.

Она иллюстрирует структуру информационной системы, описывая классы, их атрибуты, методы и отношения между объектами.



Рис. 2. Диаграмма перспективы

## 2. Игровой движок.

Unity — это современный движок, который позволяет делать игры с современной графикой. Его преимущества можно перечислять очень долго. Пройдёмся по основным. При этом использование программных скриптов на относительно простом в освоении языке



программирования C# позволяет разработать логику любой сложности для игры любого жанра и масштаба. Для сравнения, порог вхождения в аналогичный игровой движок Unreal Engine значительно выше, ведь тот движок использует язык программирования C++, который труднее в освоении, чем C#. Игры, как правило, создаются путём постоянных доработок. Unity в этом смысле очень удобен, ведь позволяет запустить игру в редакторе уровней и опробовать её без создания отдельного билда, на который понадобится время.

Более того, пока игра запущена, имеется возможность что-нибудь изменить, чтобы сразу посмотреть, как изменение скажется на геймплее. Например, можно увеличить скорость игрового персонажа, поменять урон оружия, добавить ещё несколько противников, передвинуть объект и т.д.

Все объекты в Unity собираются из компонентов, которые очень легко удалять и добавлять. Это также облегчает создание прототипов, ведь всегда можно наделить любой объект уже проработанной логикой поведения, добавив готовый программный скрипт. Любой объект можно заставить летать, если добавить ему программный скрипт, написанный для другого объекта.



Рис. 3. Игровой движок

### 3. Система проектирования.

Телемеханика — это наука об управлении и контроле на расстоянии с передачей (по каналу связи) кодированных электрических или радиосигналов, несущих управляющую информацию или данные о состоянии контролируемого объекта. Объектами телемеханического управления и контроля могут служить технологические процессы, машины, устройства, биологические системы и др. А также отрасль техники, разрабатывающая, создающая и использующая средства кодирования, передачи и приёма информации по каналам проводной и радиосвязи. В системах телемеханики информация обычно передается в кодированном виде по одному каналу связи.

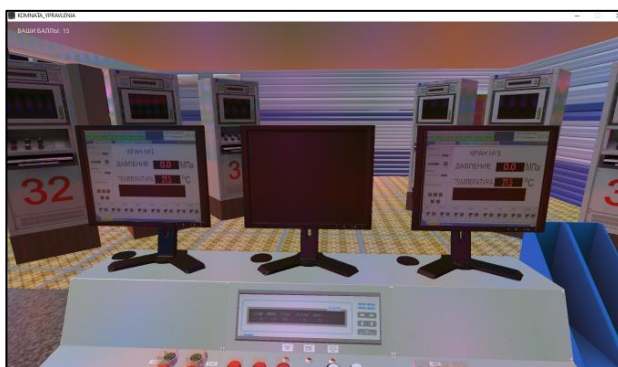


Рис. 4. Система телемеханики

### 4. Создание 3d-моделей

3D-моделирование — это процесс создания трехмерных объектов, которые могут быть использованы для различных целей, включая анимацию, видеоигры, фильмы и приложения виртуальной реальности. Будь вы художником, инженером или дизайнером, умение создавать 3D-модели может стать ценным навыком.

Существуют различные методы создания 3D-моделей, включая использование специализированного программного обеспечения, 3D-сканирование, фотограмметрию, игровые движки и 3D-печать. Каждый метод имеет свои преимущества и недостатки, и выбор будет зависеть от цели использования модели, доступных инструментов и уровня знаний создателя.

Независимо от метода, создание 3D-моделей требует творческого подхода, внимания к деталям и практики. Это навык, который можно освоить и улучшить со временем, проявив терпение и преданность делу. В этом руководстве мы рассмотрим некоторые из наиболее популярных методов создания 3D-моделей, а также советы и ресурсы, которые помогут вам начать работу.

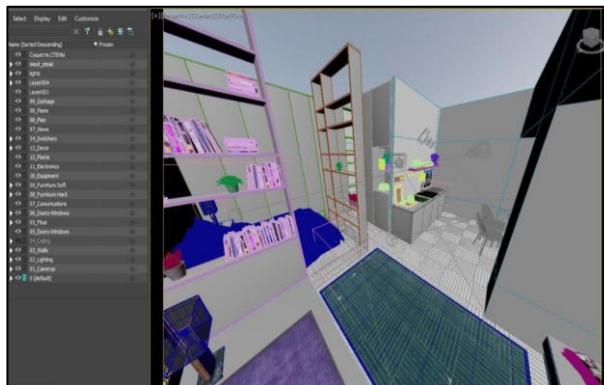


Рис. 5. Создание 3d-модели

## 5. Создание разверток

UV-развёртка — проецирование изображения на грани 3D-модели. От её расположения, вращения, масштабирования и формы зависит итоговый вид текстуры. Чтобы понять принцип развёртки, достаточно представить сборку моделей из бумаги, но в обратном порядке — объект разрезают и разворачивают на плоские детали.

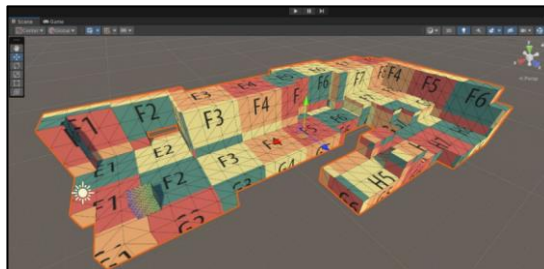


Рис. 6. Создание UV-развёртки

## 6. Создание текстур

За точную передачу геометрии 3D-объекта отвечает количество полигонов — тех самых векторных многоугольников, из которых состоит модель и с которыми работает дизайнер при её создании. Очевидно, что чем их больше, тем выше будет уровень детализации готовой модели.

Сделать цифровой образ реалистичным, сохранив минимальное количество полигонов, позволяют текстуры и материалы.

Текстура (иногда её называют картой) — это растровое изображение, накладываемое на поверхность модели для придания ей цвета, свойств окраски или иллюзии рельефа. Изображение будет наложено на модель, но геометрия останется неизменной. Так мы создадим видимость рельефа, не тратя много ресурсов на моделирование и компьютерную отрисовку.

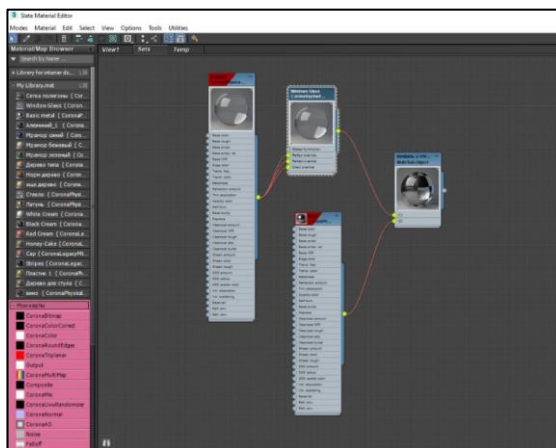


Рис. 7. Создание текстур

## 7. Разработка игровой логики

Игровая логика — это комплекс закономерностей, обеспечивающих единство геймплея, четкие связи между его элементами. Проще говоря - правила игры. Действие А приводит к событию В - например, выстрел в противника из плазменной пушки приводит к получению им 50 единиц урона.

Игровая механика - способ взаимодействия пользователя с игровыми объектами. Это конкретизация действий, из которых состоит игровой цикл. Основные механики, встречающиеся в большинстве проектов — это бой, экономика и прогресс.

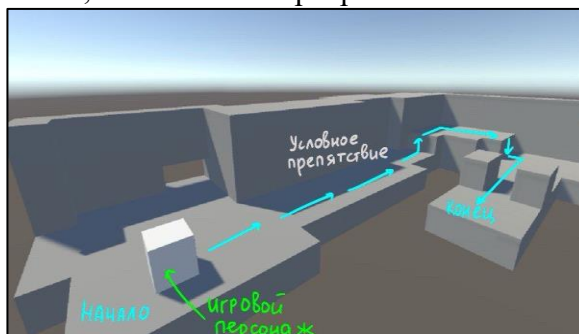


Рис. 8. Игровая логика

## 8. Написание программных скриптов

Скрипт — это четкая последовательность действий, обозначенная при помощи инструментов скриптового языка программирования. Его можно принимать за маленькую программу, которая встраивается в код базового приложения и автоматизирует выполнение конкретной задачи. Простота редактирования. Каждый скрипт — это самостоятельный элемент, который можно отредактировать, как угодно, никак не воздействуя на работоспособность остального года.

Оперативное решение задач. Если правильно писать и использовать скрипты, они работают не хуже, чем громоздкие участки кода, а то и достигают поставленной задачи еще быстрее.

```

1 procedure imgEngine_OnClick(ASender: TObject);
2 var
3   aValue: Byte;
4 begin
5   aValue := Random(2);
6   case aValue of
7     0: // меняем цвет текстуры в подкачку
8     begin
9       imgEngine.Color := $FF0000;
10      imgEngine.Hint := 'Этот двигатель, теперь, красного цвета';
11     end;
12   1:
13   begin
14     // меняем цвет текстуры
15     imgEngine.Color := $00FFFF;
16   end;
17   // разворачиваем изображение в противоположную
18   // сторону относительно X
19   imgEngine.FlipX := not imgEngine.FlipX;
20 end;
21 end;
22 end;
23 end;
24 end;
25 begin
26 end;
27 end;

```

Рис. 9. Программный скрипт

#### 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/>

## **БЛОКЧЕЙН: РЕВОЛЮЦИЯ В ФИНАНСАХ, ЗДРАВООХРАНЕНИИ И НЕ ТОЛЬКО**

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

Ключевые слова: блокчейн, децентрализация, инновации.

В статье рассмотрены ключевые аспекты блокчейна как технологической революции в области финансов, здравоохранения и других сфер, включая описание принципов децентрализации, применение криптовалют, инноваций и смарт-контрактов.

**M.Y. Kazantsev**

## **BLOCKCHAIN: A REVOLUTION IN FINANCE, HEALTHCARE AND MORE**

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

Keywords: blockchain, decentralization, innovation. The article examines the key aspects of blockchain as a technological revolution in finance, healthcare and other fields, including a description of the principles of decentralization, the use of cryptocurrencies, innovations and smart contracts.

Технология блокчейн стала одним из самых обсуждаемых и перспективных инновационных решений в современном мире. Ее применение охватывает различные отрасли, начиная от финансов и заканчивая здравоохранением. В данной статье мы рассмотрим основные аспекты блокчейн технологии и ее влияние на сферы финансов, здравоохранения, а также другие области.

Технология блокчейн представляет собой децентрализованную систему хранения данных, основанную на цепи блоков, где каждый блок содержит информацию о транзакциях. Основным принципом работы блокчейн является распределенный реестр, который обеспечивает прозрачность и надежность хранения информации. Каждое изменение в блокчейн системе подтверждается сетью участников, что исключает возможность подделки данных. Отличительной особенностью блокчейн технологии является ее невозможность изменения или удаления информации, что обеспечивает надежность и целостность данных.

Использование технологии блокчейн в различных сферах деятельности обладает рядом значительных преимуществ. Во-первых, блокчейн обеспечивает высокий уровень безопасности за счет криптографических методов шифрования данных и децентрализованной структуры хранения. Это позволяет предотвращать мошенничество и несанкционированный доступ к информации.

Во-вторых, блокчейн обеспечивает прозрачность и доступность данных для всех участников сети, что способствует повышению доверия между ними. Благодаря этому, возможно создание эффективных механизмов взаимодействия и сотрудничества.

Также следует отметить, что блокчейн позволяет сократить издержки и упростить процессы благодаря автоматизации выполнения соглашений и контрактов. Это способствует повышению эффективности бизнес-процессов и улучшению качества услуг.

Несмотря на множество преимуществ, технология блокчейн также сталкивается с рядом вызовов и ограничений, которые могут затруднить ее широкое внедрение.

Один из основных вызовов - масштабируемость. При увеличении количества транзакций в блокчейн сети возникают проблемы с производительностью и скоростью обработки данных. Это может привести к задержкам и увеличению комиссий за транзакции.

Другим вызовом является проблема конфиденциальности данных. Хотя блокчейн обеспечивает высокий уровень безопасности, но в некоторых случаях требуется сохранение конфиденциальности определенной информации, что может быть сложно реализовать в открытой децентрализованной сети.

Также следует отметить сложности с законодательством и регулированием в отношении использования блокчейн технологии. Некоторые страны имеют ограничения или запреты на использование криптовалют и смежных технологий, что создает негативное воздействие на их развитие.

И наконец, вопросы обеспечения безопасности и защиты от киберугроз также остаются актуальными. Хакеры могут пытаться атаковать блокчейн сети, что может привести к утечке данных или другим негативным последствиям.

Технология блокчейн имеет значительное влияние на финансовую сферу, предлагая различные инновационные решения и возможности для улучшения процессов.

Одним из ключевых аспектов блокчейн в финансах является возможность создания криптовалют и цифровых активов. Это открывает новые возможности для международных финансовых транзакций, обеспечивая быстрые и дешевые переводы с минимальными комиссиями.

Блокчейн также позволяет сократить издержки и упростить процессы ведения бухгалтерии и аудита благодаря автоматизации и цифровизации данных. Это способствует повышению эффективности работы финансовых учреждений и снижению рисков ошибок.

Также хотелось бы рассмотреть технологии блокчейн в сфере здравоохранения, которая открывает новые возможности для улучшения качества медицинского обслуживания, обеспечивая безопасное хранение и обмен медицинских данных.

Одним из главных преимуществ блокчейн в здравоохранении является безопасность и целостность информации. Благодаря шифрованию данных и децентрализованной структуре хранения, блокчейн обеспечивает защиту конфиденциальности пациентов и предотвращает несанкционированный доступ к медицинским данным.

Кроме того, блокчейн технология позволяет создавать единую базу данных медицинских записей, к которой имеют доступ врачи, пациенты и другие участники системы здравоохранения. Это способствует улучшению координации медицинского ухода, сокращению ошибок и оптимизации процессов диагностики и лечения.

Другим важным аспектом блокчейн в здравоохранении является возможность проведения исследований на основе анонимизированных медицинских данных. Это позволяет улучшить понимание заболеваний, разрабатывать новые методы диагностики и лечения, а также повысить эффективность медицинских исследований.

Технология блокчейн продолжает активно развиваться, открывая новые перспективы и возможности для различных отраслей и областей применения. Несмотря на вызовы и ограничения, блокчейн остается одним из самых перспективных инновационных инструментов современности.

Технология блокчейн уже сегодня меняет мир, предлагая новые возможности для развития бизнеса, улучшения качества жизни и содействия социальному прогрессу. С постоянным развитием и инновациями, блокчейн будет продолжать играть ключевую роль в цифровизации экономики, обеспечивая безопасность, прозрачность и эффективность в различных сферах деятельности.

Поэтому важно следить за новыми тенденциями, участвовать в развитии блокчейн проектов и использовать потенциал этой технологии для достижения новых высот в будущем.

#### Список литературы:

1. Антонопулос, А. Мастеринг биткойн: программирование блокчейна. — СПб.: Питер, 2018. — 416 с.
2. Иванов, Д. Блокчейн. Принципы. Технология. Применение. — М.: ДМК Пресс, 2017. — 352 с.

3. Сатоши, Н. Биткойн: электронная пиринговая платежная система. — 2008. [Электронный ресурс]. URL: <https://bitcoin.org/bitcoin.pdf> (дата обращения: 10.10.2021)
4. Глазьев, С. Цифровая экономика: как блокчейн изменит финансы и здравоохранение. — М.: Издательство "Эксмо", 2020. — 240 с.
5. Петров, И. Блокчейн технологии: от цифровой валюты до финансовых решений. — СПб.: БХВ-Петербург, 2019. — 288 с.

## ОРГАНИЗАЦИЯ OPENSOURCE ЗОНТИЧНОЙ СИСТЕМЫ МОНИТОРИНГА ДЛЯ СБОРА И СИСТЕМАТИЗАЦИИ ПАРАМЕТРОВ СЕРВЕРА MARIADB

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

Ключевые слова: мониторинг, SQL, OpenSource, Grafana, Zabbix, MariaDB.

В статье описывается процесс создания и внедрения зонтичной системы мониторинга на базе OpenSource решений для сбора, анализа и систематизации параметров серверов MariaDB. Рассматриваются ключевые компоненты системы, методы сбора данных и преимущества использования открытого программного обеспечения.

V.S. Sidorov, N.V. Budyldina

## ORGANIZATION OF AN OPENSOURCE UMBRELLA MONITORING SYSTEM FOR COLLECTING AND SYSTEMATIZING MARIADB SERVER PARAMETERS

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

Keywords: monitoring, SQL, OpenSource, Grafana, Zabbix, MariaDB.

The article describes the process of creating and implementing an umbrella monitoring system based on OpenSource solutions for collecting, analyzing, and systematizing MariaDB server parameters. Key components of the system, data collection methods, and the advantages of using open-source software are discussed.

### 1. Введение

В эпоху цифровизации и непрерывного роста объемов данных, эффективность и стабильность систем управления базами данных (СУБД) становятся критически важными для бизнеса и научных исследований. MariaDB, как один из лидеров среди открытых СУБД, зарекомендовала себя как надежное, производительное и гибкое решение. Однако, как и любая сложная система, MariaDB требует тщательного мониторинга для обеспечения оптимальной работы и быстрого реагирования на возможные проблемы.

Традиционные подходы к мониторингу часто ограничиваются узкоспециализированными решениями, которые не всегда способны предоставить полную картину состояния системы. В ответ на эти вызовы, сообщество OpenSource предлагает инновационные инструменты, способные интегрироваться с различными источниками данных и предоставлять глубокий анализ параметров работы СУБД.

В данной статье мы фокусируемся на создании зонтичной системы мониторинга, которая объединяет преимущества открытого программного обеспечения с передовыми методами сбора и анализа данных. Такая система позволяет не только отслеживать ключевые показатели работы серверов MariaDB, но и систематизировать данные для последующего анализа и принятия решений.

Основываясь на принципах открытости и доступности, мы стремимся разработать решение, которое будет полезно как крупным компаниям, так и индивидуальным разработчикам. Система мониторинга должна быть масштабируемой, легко настраиваемой и способной адаптироваться к изменяющимся условиям эксплуатации серверов.

Важной частью работы является анализ существующих решений мониторинга, выявление их недостатков и преимуществ, а также формирование требований к новой системе. Мы



рассмотрим такие аспекты, как производительность, безопасность, удобство использования и интеграцию с другими инструментами и сервисами.

В результате, статья предложит комплексный взгляд на процесс организации эффективной системы мониторинга для серверов MariaDB, обозначит ключевые этапы ее разработки и внедрения, и подчеркнет важность OpenSource подхода в создании устойчивых и гибких IT-решений.

## **2. Обзор технологий**

В основе эффективной системы мониторинга лежат мощные и гибкие технологии, способные обеспечить надежный сбор данных и их визуализацию. В данном разделе мы рассмотрим два ключевых инструмента, выбранных для нашей зонтичной системы мониторинга: Zabbix и Grafana.

Zabbix – это высокоинтегрированная OpenSource платформа для мониторинга сетей и приложений. Она предоставляет широкие возможности для сбора данных с серверов, сетевого оборудования, виртуальных машин и других компонентов инфраструктуры. Zabbix известен своей масштабируемостью и гибкостью, позволяя администраторам настраивать мониторинг под конкретные нужды бизнеса. Система поддерживает различные методы сбора данных, включая агенты, SNMP, JMX, IPMI и другие.

Grafana – это мощный инструмент для визуализации и анализа данных. Он позволяет создавать детализированные и интерактивные дашборды, которые могут отображать данные из множества источников, в том числе Zabbix. Grafana обладает интуитивно понятным интерфейсом и широким набором функций для настройки визуализаций, что делает её идеальным выбором для представления метрик серверов MariaDB.

Интеграция Zabbix с Grafana дает возможность не только собирать обширные данные о состоянии серверов, но и представлять их в удобной и информативной форме. Это обеспечивает администраторам быстрый доступ к актуальной информации и помогает в принятии обоснованных решений при управлении производительностью и безопасностью серверов.

В следующих разделах мы подробно рассмотрим процесс настройки Zabbix для сбора данных с серверов MariaDB и создание дашбордов в Grafana, которые будут отражать ключевые показатели работы и эффективности системы.

## **3. Сбор и анализ данных**

Сбор и анализ данных являются ключевыми аспектами любой системы мониторинга. В контексте нашей зонтичной системы мониторинга для серверов MariaDB, мы используем Zabbix для сбора данных и Grafana для их визуализации. Этот процесс включает в себя несколько этапов:

### **1) Настройка Zabbix для сбора данных:**

- Конфигурация агента Zabbix: на серверах MariaDB устанавливается агент Zabbix, который собирает информацию о состоянии сервера.

- Создание пользовательских параметров: в файле конфигурации агента (`template_db_mysql.conf`) указываются параметры для мониторинга MariaDB.

- Настройка прав доступа: создаётся специальный пользователь в MariaDB с правами, достаточными для сбора статистики, но ограниченными для обеспечения безопасности.

### **2) Сбор метрик:**

- Производительность сервера: загрузка CPU, использование памяти, объем свободного места на диске.

- Состояние базы данных: количество активных соединений, время отклика, частота транзакций.

- Репликация: статус репликации, задержки, количество реплицируемых данных.

### **3) Анализ данных в Grafana:**

- Создание дашбордов: используя данные, собранные Zabbix, в Grafana создаются дашборды, которые отображают ключевые показатели в удобной форме.

- Визуализация: графики, таблицы и счетчики на дашбордах позволяют быстро оценить текущее состояние серверов и историю их работы.

- Оповещения: на основе анализа данных настраиваются оповещения о критических состояниях или предупреждениях.

#### 4) Оптимизация и масштабирование:

- Анализ трендов: Долгосрочный анализ данных помогает выявлять тенденции и прогнозировать потребности в ресурсах.

- Масштабирование: на основе анализа данных принимаются решения о необходимости масштабирования инфраструктуры.

#### 5) Интеграция с другими системами:

- API: Zabbix и Grafana предоставляют API для интеграции с другими системами, что позволяет автоматизировать процессы и расширять функциональность.

Этот раздел статьи подчеркивает важность тщательного сбора и анализа данных для обеспечения стабильности и производительности серверов MariaDB. Он также иллюстрирует, как Zabbix и Grafana могут быть использованы для создания мощной системы мониторинга, способной адаптироваться к меняющимся условиям и потребностям бизнеса.

### 4. Тестирование и валидация системы

Тестирование и валидация системы мониторинга являются неотъемлемыми этапами разработки, позволяющими убедиться в её надежности и эффективности. Для системы мониторинга серверов MariaDB на базе Zabbix и Grafana, тестирование включает в себя следующие шаги:

#### 1. Функциональное тестирование:

- Проверка сбора данных: убедиться, что Zabbix корректно собирает все необходимые метрики с серверов MariaDB.

- Валидация дашбордов Grafana: проверить, что все панели корректно отображают данные, и визуализации соответствуют заданным параметрам.

#### 2. Нагрузочное тестирование:

- Имитация высокой нагрузки: с помощью инструментов для генерации трафика (например, mysqlslap) создать высокую нагрузку на сервера MariaDB и оценить способность системы мониторинга отслеживать изменения в реальном времени.

- Анализ производительности: оценить, как система справляется с большим объемом данных и как это влияет на производительность мониторинга.

#### 3. Тестирование отказоустойчивости:

- Имитация сбоев: провести тесты на отказоустойчивость, включая отключение серверов MariaDB, и проверить, насколько быстро система мониторинга реагирует на инциденты.

- Восстановление после сбоев: проверить механизмы восстановления и оповещения, чтобы убедиться, что система может эффективно управлять инцидентами.

#### 4. Тестирование безопасности:

- Проверка доступа: убедиться, что доступ к метрикам строго контролируется и предоставляется только авторизованным пользователям.

#### 5. Валидация данных:

- Сопоставление с реальными данными: сверить данные, собранные системой мониторинга, с реальными показателями работы серверов MariaDB, чтобы убедиться в точности мониторинга.

#### 6. Документирование:

- Создание документации: подготовить подробную документацию по процессу тестирования, включая описание тестовых сценариев, инструкции и результаты.

Этот раздел подчеркивает важность тщательного тестирования системы мониторинга перед её внедрением в производственную среду. Он также обеспечивает уверенность в том, что система будет работать корректно и эффективно в различных условиях эксплуатации.

### Заключение

В завершение, разработка OpenSource зонтичной системы мониторинга для серверов MariaDB представляет собой значительный шаг вперед в области управления и оптимизации баз данных. Использование таких инструментов, как Zabbix и Grafana, позволяет не только

эффективно собирать и анализировать данные, но и предоставлять их в удобной и наглядной форме для администраторов и специалистов по базам данных.

В ходе работы были рассмотрены ключевые аспекты настройки системы мониторинга, включая сбор метрик, визуализацию данных, настройку оповещений и интеграцию с другими системами. Тестирование и валидация системы позволяют подтвердить её надежность и готовность к эксплуатации в производственной среде.

Система мониторинга, основанная на OpenSource решениях, демонстрирует гибкость и масштабируемость, позволяя адаптироваться к различным условиям и требованиям бизнеса. Она способствует повышению производительности, устойчивости и безопасности серверов MariaDB, что в свою очередь влияет на общую эффективность IT-инфраструктуры.

В заключение, данная работа подчеркивает важность сообщества OpenSource и его вклада в развитие технологий мониторинга. Она служит примером успешного применения открытого программного обеспечения для решения сложных задач и предоставляет основу для дальнейших исследований и разработок в этой области.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Zabbix 6.4 Documentation. [Электронный ресурс]. – Режим доступа: <https://www.zabbix.com/documentation/current/>
2. Monitoring MariaDB with Zabbix. [Электронный ресурс]. – Режим доступа: <https://mariadb.com/kb/en/monitoring-mariadb-with-zabbix/>
3. Grafana: The open observability platform. [Электронный ресурс]. – Режим доступа: <https://grafana.com/docs/>
4. MySQL 8.0 Reference Manual. [Электронный ресурс]. – Режим доступа: <https://dev.mysql.com/doc/refman/8.0/en/>
5. Best Practices for Setting Up a Zabbix Environment. [Электронный ресурс]. – Режим доступа: [https://www.zabbix.com/best\\_practices](https://www.zabbix.com/best_practices)
6. MariaDB Knowledge Base.” MariaDB Corporation. [Электронный ресурс]. – Режим доступа: <https://mariadb.com/kb/en/>

## **АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ И ПРОТОКОЛОВ SD-WAN**

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

Ключевые слова: SD-WAN, программно-определяемая сеть, управление сетью, безопасность сети, глобальные сети, Cisco, Citrix, Kaspersky, МТС, производительность сети, оптимизация трафика, централизованное управление, отечественные решения, масштабируемость, адаптивность.

Статья рассматривает современные решения SD-WAN (Software-Defined Wide Area Network) от ведущих мировых компаний, а также их отечественных аналогов. Программно-определяемая глобальная сеть представляет собой технологию, которая упрощает управление и эксплуатацию глобальных сетей, повышая производительность, надежность и безопасность корпоративных сетей. Статья описывает основные принципы работы SD-WAN, технологии и функции различных решений, а также их преимущества для бизнеса.

**I.V. Tashkinov, N.V. Budyldina**

## **ANALYSIS OF EXISTING SD-WAN SOLUTIONS AND PROTOCOLS**

Ural Technical Institute of Communications and Informatics (Branch) of FSBEI VO "Siberian State University of Telecommunications and Informatics" in Ekaterinburg (UrTISI SibGUTI), Russia

Keywords: SD-WAN, software-defined network, network management, network security, global networks, Cisco, Citrix, Kaspersky, MTS, network performance, traffic optimization, centralized management, homegrown solutions, scalability, adaptability.

The article considers modern SD-WAN (Software-Defined Wide Area Network) solutions from the world's leading companies, as well as their domestic analogs. Software-Defined Wide Area Network is a technology that simplifies the management and operation of wide area networks, improving the performance, reliability and security of corporate networks. The article describes the basic principles of SD-WAN operation, technologies and functions of various solutions, as well as their business benefits.

SD - WAN, также известная как Software - Defined Wide Area Network, — это технология, которая упрощает управление и эксплуатацию глобальной сети (WAN), отделяя сетевое оборудование от механизма управления. [1] Вместо того чтобы зависеть только от конфигурации оборудования и ручного вмешательства, SD - WAN использует принципы программно-определяемой сети (SDN) для централизованного управления и динамической корректировки потока сетевого трафика. Основная цель SD - WAN - повысить производительность, надежность и безопасность корпоративных сетей, особенно если они разбросаны по разным точкам. Для этого используются различные типы соединений, такие как широкополосный интернет, MPLS и LTE, для создания единой сетевой инфраструктуры. SD - WAN разумно направляет трафик.[2]

Для начала рассмотрим готовые решения для организации сети SD - WAN от зарубежных компаний, а также и от отечественных.

Зарубежные решения:

1) Cisco SD - WAN, изначально известная как Viptela, представляет собой программно-определяемое сетевое решение, направленное на оптимизацию и обеспечение безопасности подключения к глобальной сети. Оно использует оверлейную архитектуру для отделения плоскости управления от плоскости данных, что позволяет централизованно управлять сетевыми политиками и эффективно пересылать трафик данных через глобальную сеть. Безопасное

подключение обеспечивается с помощью зашифрованных туннелей типа IPsec для защиты целостности и конфиденциальности данных. Cisco SD-WAN обеспечивает централизованное управление с помощью удобного графического интерфейса пользователя или CLI, что позволяет администраторам эффективно настраивать, контролировать и устранять неполадки в сети.[9]

Cisco SD - WAN поддерживает технологию "нулевого касания", позволяющую легко подключать и настраивать удаленные филиалы без ручного вмешательства. Это упрощает развертывание и снижает расходы.

2) Citrix SD - WAN, ранее Citrix NetScaler SD-WAN, - это сетевое решение, которое улучшает и защищает подключение к глобальной сети (WAN). В нем используются алгоритмы динамического выбора пути для интеллектуального направления трафика через WAN. Вместо статических конфигураций Citrix SD - WAN постоянно наблюдает за состоянием сети и мгновенно выбирает оптимальный путь для каждого потока приложений. Этот адаптируемый метод гарантирует высочайшую производительность и надежность даже при изменении сетевой среды.[10]

Citrix SD - WAN использует технологию, называемую FEC на уровне пакетов, для решения проблем потери пакетов и задержки, характерных для WAN-каналов. Кодировая дополнительную информацию в пакетах, Citrix SD - WAN может восстановить потерянные или поврежденные данные на принимающей стороне без необходимости повторной отправки информации. Эта технология повышает производительность приложений и удобство работы пользователей, особенно в ненадежных сетях, таких как Интернет.

Citrix SD - WAN устанавливает приоритет критически важного трафика приложений над менее важными потоками данных с помощью политик QoS. Это гарантирует, что чувствительные к задержкам приложения, такие как видеоконференции, получают достаточную пропускную способность и минимальную задержку даже при перегрузке сети. Такой механизм приоритизации повышает производительность приложений и удовлетворенность пользователей. Citrix SD - WAN обеспечивает инновационную технологию безопасности. Она включает в себя брандмауэр с учетом приложений. Он проверяет трафик и фильтрует его на основе характеристик приложений. В отличие от обычных брандмауэров, которые проверяют только заголовки пакетов, это решение может идентифицировать приложения. Оно отслеживает их независимо от номеров портов и используемых протоколов. Такой подробный обзор и контроль повышает безопасность и соответствие нормативным требованиям.

3) VMware SD - WAN Orchestrator - это облачный портал. Он управляет, контролирует и диагностирует сеть SD - WAN. С его помощью можно легко запускать виртуальные сетевые службы в филиалах, облаках или корпоративных центрах обработки данных одним щелчком мыши. Этот веб-портал для управления сетью SD - WAN доступен как услуга (SaaS). Также его можно развернуть в локальном центре обработки данных[8].

Архитектура оркестратора позволяет масштабировать сеть от нескольких узлов до тысяч. Управление на основе политик и шаблоны профилей обеспечивают мгновенное развертывание изменений в сети. Это лишь некоторые из возможностей оркестратора. Он также предоставляет мониторинг состояния узлов сети, SLA по каналам, сетевую активность по приложениям и клиентам, а также продвинутую систему отчетности.

Функция Zero - Touch Provisioning (ZTP) позволяет активировать устройства в филиалах без необходимости выезда специалиста. Процесс активации сводится к нескольким простым шагам, и устройство автоматически получает связь с оркестратором.

С помощью оркестратора также доступна диагностика сети, включая состояние протоколов маршрутизации, портов, таблиц ARP и NAT, а также инструменты Ping и Traceroute, все без необходимости подключения к устройствам через CLI/SSH.

Также журнал событий позволяет отслеживать изменения и уведомления со всех устройств, доступные для поиска и просмотра прямо на SD - WAN Orchestrator.

Стоит уделить внимание и некоторым отечественным решениям:

1) Kaspersky SD - WAN - это программное обеспечение для защиты глобальных сетей. Оно разработано экспертами по кибербезопасности из компании Kaspersky. Решение нацелено на обеспечение безопасности сетей SD - WAN. В нем используются навыки Касперского в области

киберзащиты. Специальные функции предотвращают такие угрозы, как хакеры, вирусы и вредоносные веб-сайты. Эти средства защиты защищают инфраструктуру SD - WAN[7].

Как и другие продукты SD - WAN, Kaspersky оптимизирует поток интернет-трафика. Он выбирает оптимальный путь, основываясь на потребностях приложений, состоянии сети и правилах безопасности. Это обеспечивает хорошую работу жизненно важных приложений. В то же время он эффективно использует сетевые ресурсы. Интеллектуальная маршрутизация повышает производительность, оставаясь при этом безопасной.

Kaspersky SD - WAN имеет единую панель управления. Из нее администраторы видят всю сеть. Они устанавливают политики, следят за производительностью, быстро реагируют на проблемы безопасности. Это централизует управление сетью, упрощает задачи и устранение неполадок.

SD - WAN легко интегрируется с другими защитными решениями Касперского. Такая интеграция обеспечивает единое обнаружение угроз и скоординированную защиту на всех уровнях. Обмен данными об угрозах также происходит беспрепятственно. Все это значительно повышает общий уровень безопасности.

2) МТС SD - WAN - это предложение от МТС, крупной телекоммуникационной компании. МТС SD - WAN создан для малых или средних предприятий. Компании могут быстро менять конфигурацию своей сети, используя гибкие возможности развертывания. Услуга оптимизирует производительность сети за счет интеллектуальной передачи данных по различным каналам связи, таким как MPLS, широкополосный доступ и LTE. При этом учитываются такие факторы, как потребности приложений, состояние сети и затраты. Оптимизация повышает удобство работы пользователей и производительность приложений за счет эффективного использования полосы пропускания. Кроме того, она включает в себя функции безопасности, которые защищают сообщество и его пользователей от киберугроз. Они могут включать в себя брандмауэр, средства обнаружения и предотвращения вторжений (IDPS), а также шифрование для защиты передаваемых данных. Интегрируя функции безопасности в решения SD - WAN, МТС стремится обеспечить полную безопасность сетей своих клиентов.[6]

SD - WAN от МТС позволяет компаниям определять приоритеты посетителей в зависимости от потребностей приложений, обеспечивая критически важным приложениям необходимую пропускную способность и производительность, сохраняя при этом неизменное удобство провайдера по всей сети.

Все перечисленные SD - WAN решения предлагают различные комбинации производительности, гибкости, безопасности и поддержки. Выбор между ними зависит от конкретных потребностей компании, ее бюджета и инфраструктуры, а также предпочтений в области поддержки и экосистемы продуктов.

Решения SD - WAN используют разнообразные протоколы и API для эффективной связи, динамической маршрутизации и интеграции с существующей инфраструктурой.

Оверлейные протоколы, такие как VXLAN и GRE, позволяют создавать виртуальные сети поверх существующей инфраструктуры, обеспечивая соединение географически разнесенных сайтов.

Протоколы плоскости управления, включая BGP, OSPF и MP-BGP, обеспечивают динамическую маршрутизацию и эффективный обмен информацией о маршрутах между устройствами SD - WAN и внешними сетями.

API-интерфейсы, такие как OpenFlow для южного направления и API северного направления, обеспечивают программное управление и интеграцию с другими системами управления и приложениями.

Все это обеспечивает организациям большую гибкость, масштабируемость и контроль над их сетями, позволяя эффективно управлять сетью, осуществлять динамическую маршрутизацию и бесшовную интеграцию с существующей инфраструктурой и приложениями.

Подводя итог, можно сказать, что программно-определяемая глобальная сеть - это современное решение для оптимизации управления и обеспечения безопасности корпоративных сетей. Компании, такие как Cisco и Citrix, предлагают инновационные подходы к SD - WAN, учитывая требования производительности, надежности и безопасности. В то же время отечественные разработчики, вроде Kaspersky и МТС, адаптируют решения под местные

потребности и особенности рынка. Все эти решения обеспечивают высокую производительность, гибкость и безопасность, необходимые для успешного ведения бизнеса в современной цифровой среде.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Бокарев А.Ю., Волошин В.И. Программно-ориентированные сети: будущее сетевых коммуникаций. — Москва, 2018.
2. Программно-определяемые сети (SDN): новые возможности управления сетью / Под ред. Тиркина В.М., Малышкина В.В. — Санкт-Петербург, 2017. — 336 с.
3. Рябов Н.В., Киреев В.В., Маслов В.Л., Чеппыжев А.А. Программно-ориентированные сети. — Санкт-Петербург, 2016.
4. Киев С.О., Ван Зинк Ж. Программно-определяемые сети: сверхагенты будущего / «Сети и системы телекоммуникации». — 2015. — Т. 12, № 2. — [Электронный ресурс] – Режим доступа: <https://www.cct.pu.ru/jour/article/view/76> (дата обращения: 10.04.2024).
5. Бирман С.М., Атанов Д.А. Программно-определяемые сети как основа облачных вычислений и мобильной связи / «Сеть и надежность». — 2014. — № 26. — [Электронный ресурс] – Режим доступа: <https://cyberleninka.ru/article/n/programmno-opredelyaemye-seti-kak-osnova-oblachnyh-vychisleniy-i-mobilnoy-svyazi>.
6. Организация распределенной сетевой ИТ-инфраструктуры // Cloud SD-WAN [Электронный ресурс] – Режим доступа: <https://cloud.mts.ru/services/sd-wan/> (дата обращения: 12.04.2024).
7. Kaspersky SD-WAN // Kaspersky [Электронный ресурс] – Режим доступа: <https://www.kaspersky.ru/enterprise-security/sd-wan> (дата обращения: 11.04.2024).
8. VMware SD-WAN: обзор решения // Хабр [Электронный ресурс] – Режим доступа: [https://habr.com/ru/companies/cloud\\_mts/articles/550536/](https://habr.com/ru/companies/cloud_mts/articles/550536/) (дата обращения: 11.04.2024).
9. Cisco Extended Enterprise SD-WAN Design Guide // Cisco [Электронный ресурс] – Режим доступа: <https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/DG/ee-WAN-dg.html> (дата обращения: 13.04.2024).
10. Citrix SD-WAN Planning Workshop // xtravirt.com [Электронный ресурс] – Режим доступа: <https://s3.eu-west-2.amazonaws.com/xtravirt-website-resources/Datasheets/Digital+Workspace/Xtravirt's+Citrix+SD-WAN+Planning+Workshop.pdf> (дата обращения: 10.04.2024).

## АЛГОРИТМ МНОГООКОННОЙ СИМВОЛЬНОЙ СИНХРОНИЗАЦИИ ПО ОТСЧЕТАМ КОМПЛЕКСНОЙ ОГИБАЮЩЕЙ

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

Ключевые слова: символьная синхронизация, вероятность ошибки, время синхронизации, ошибка синхронизации.

Предложен алгоритм символьной синхронизации по отсчетам комплексной огибающей, без использования фазовой автоподстройки частоты (ФАПЧ) для (D)BPSK и DQPSK модуляций. Проведено моделирование данного алгоритма, определено среднее время вхождения в синхронизм и вероятности ошибок.

O.G. Melent'ev, D.A. Goncharov, I.M. Kulikov

## THE ALGORITHM OF MULTI-WINDOW SYMBOLIC SYNCHRONIZATION BASED ON COMPLEX ENVELOPE COUNTS

Siberian State University of Telecommunications and Information Sciences (SibSUTIS),  
Novosibirsk, Russia

Keywords: symbol synchronization, error probability, synchronization time, synchronization error.

An algorithm for symbolic synchronization based on complex envelope counts is proposed, without using phase-locked frequency (PLL) for (D)BPSK and DQPSK modulations. The simulation of this algorithm was carried out, the average time of entering into synchronism and the probability of errors were determined.

### 1. Введение

Рассмотрим цифровую систему передачи (ЦСП) с фазовыми модуляциями типа (D)BPSK и DQPSK. Для обеспечения работоспособности подобных систем необходимо решить задачи фазовой, символьной и кадровой синхронизации. Некоторые алгоритмы синхронизаций рассмотрены в работах [1 – 3]. В данной статье предлагается достаточно простой в реализации алгоритм символьной синхронизации, который обеспечивает приемлемое время вхождения в синхронизм и высокую вероятность его сохранения в процессе работы.

### 2. Алгоритм символьной синхронизации

Рассмотрим ситуацию, когда на каждом символьном интервале, производится взятие восьми отсчетов (семплов) комплексной огибающей ( $n = 8$ ). Алгоритм предполагает использование трех, пяти или семи окон анализа ( $q = 3, 5, 7$ ). В каждом окне определяются суммарные значения действительных и мнимых частей восьми последовательных отсчетов и вычисляется сумма их квадратов.

$$Pw_j = \left( \sum_n I \right)^2 + \left( \sum_n Q \right)^2.$$

Каждое следующее окно сдвинуто относительно предыдущего на один семпл. Таким образом, во всех  $q$  окнах находятся  $(n+q-1)$  подряд идущих отсчетов. Суммарные семплы из центрального окна используются для дальнейшей обработки (демодуляции и т.п.). Пример расположения окон на оси времени с действительными семплами, для восьми семплов на символ,



пяти окон ( $n = 8, q = 5$ ) и состояния полной синхронизации, представлен на рисунке 1. Все окна пронумерованы от 0 до 4, в скобках указано на сколько семплов рассинхронизация в окне. Справа от окон указана сумма семплов в данном окне, в предположении, что все отсчеты символов одного знака и равны  $\pm 1$ .

Из рисунка 1 видно, что в нулевом окне два отрицательных отсчета предыдущего символа и шесть положительных следующего, то есть рассинхронизация на (-2), сумма отсчетов в окне (4). В первом окне один отрицательный предыдущего и семь положительных отсчетов следующего символа, рассинхронизация на (-1), сумма равна 6.

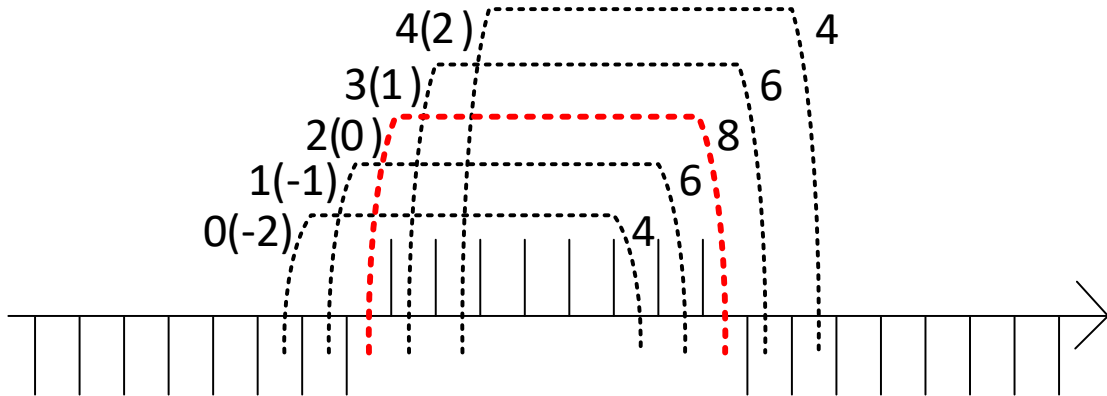


Рис. 1. Система с пятью окнами анализа в состоянии синхронизма

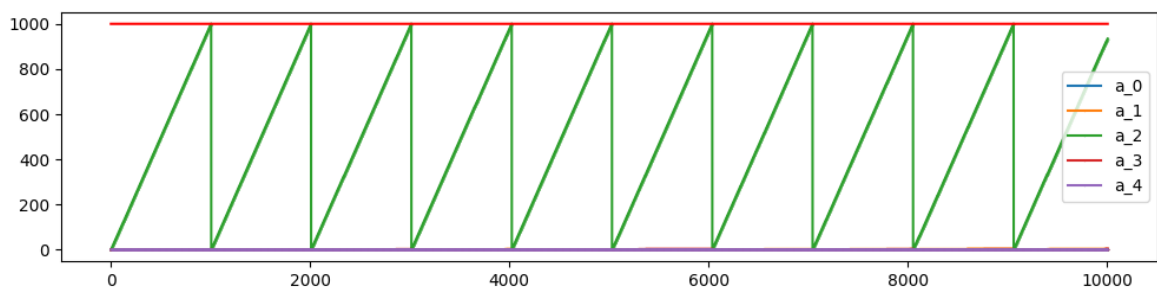
В центральном окне (2(0)) находятся семплы только одного символа (т.е. одного знака), значит их сумма будет максимальной, это есть момент полной синхронизации. В окнах 3 и 4 рассинхронизация на 1 и 2 семпла, соответственно.

Для каждого окна имеется счетчик (аккумулятор), значение которого инкрементируется, когда сумма квадратов квадратур в данном окне больше чем в других.

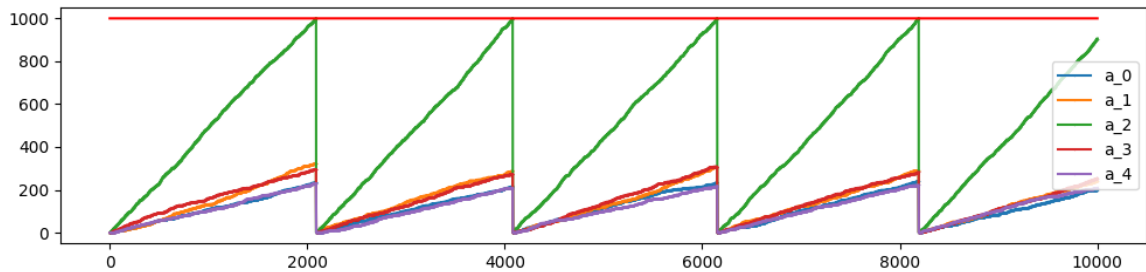
Таким образом, на каждом такте (цикле) мы смещаемся на  $n$  семплов, выдаем суммарные квадратуры из центрального окна на детектор, сравниваем амплитуды в окнах и увеличиваем счетчик окна с максимальной амплитудой.

При превышении одним из  $q$  аккумуляторов определенного порога ( $por\_ind$ ), происходит подстройка символьной синхронизации, при которой окно с максимальной амплитудой становится центральным. Если аккумулятор переполнился в центральном окне, то алгоритм обнуляет все счетчики без смещения.

На рисунке 2а представлен график значений аккумулятора, по оси  $x$  показано кол-во символов, на которых отработал аккумулятор. На каждом цикле, алгоритм проверял амплитуду символа в окнах и инкрементировал соответствующий счетчик.



а



б

Рис. 2. Пять окон, смещение 0,  $\text{por\_ind} = 1000$ : а –  $E_b/N_0 = 12$ ; б –  $E_b/N_0 = 2$ ;

Из рисунка видно, что при большом отношении энергии бита к спектральной плотности мощности шума ( $E_b/N_0 = 12$ ), амплитуда в центральном окне всегда была максимальной, а его аккумулятор, достигал порога за 1000 символов и обнулялся. Счетчики других окон, в данном примере не возрастали.

Как видно из рисунка 2б, алгоритм справляется со своей задачей и при наличии большого шума – остается в синхронизме. Все счетчики увеличивали свои значение, но аккумулятор центрального окна достиг порога за время в два раза большее (с 1000 до 2000 символов).

Рассмотрим рассинхронизацию, при которой центральное окно смещено на 1 семпл вправо, рисунок 3.

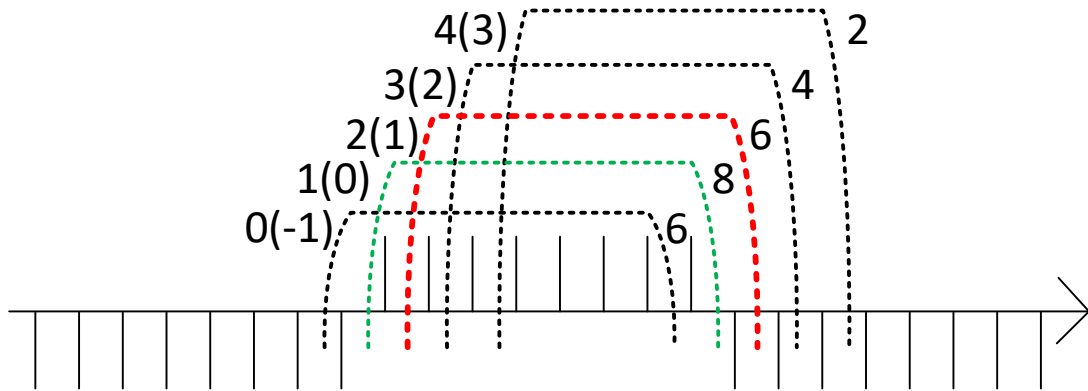


Рис. 3. Пять окон, смещение 1

Как видно из рисунка, теперь полный символ находится в окне под номером 1. Тогда как в окне 2 (центральное окно) в символе присутствует один семпл из следующего символа, но отсутствует первый семпл текущего символа. На рисунке 4 представлен график переполнения счетчиков при смещении на 1 семпл. Как видно из рисунка, при малом шуме возрастало значение только счетчика  $a_1$ , соответствующего первому окну, который достиг порога за 1000 символов. Аккумулятор  $a_1$  соответствует смещению центрального окна на один семпл влево. Значит, на следующем цикле алгоритм синхронизации смещается не на  $n$  семплов, а на  $n - 1 = 7$  семплов и попадает в состояние синхронизма.

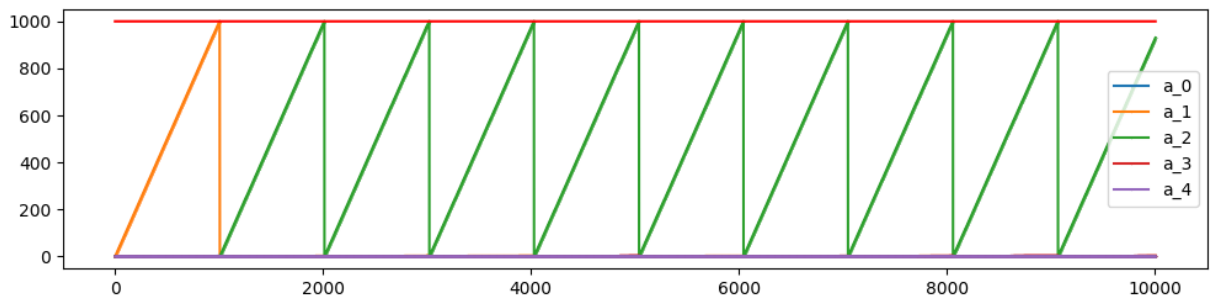


Рис. 4. Пять окон, смещение 1,  $\text{por\_ind} = 1000$ ,  $E_b/N_0 = 12$ ;

Как показали исследования, вероятность сохранения состояния синхронизма, практически не зависит от количества окон, а время вхождения в синхронизм уменьшается с увеличением их числа. При трех окнах алгоритм может приближаться к синхронизму, смещаясь только на один отсчет, при пяти – на один или два отсчета, а при семи сразу на три.

Порог, по достижению которого происходит подстройка синхронизации  $por\_ind$ , определяет время синхронизации и вероятность сохранения синхронизма. Алгоритм с наименьшим порогом быстрее приходит в синхронизм, но вероятность выхода из синхронизма соответственно выше. На рисунке 5 показано время вхождения в синхронизм из рассинхронизации на 4 семпла для разных порогов.

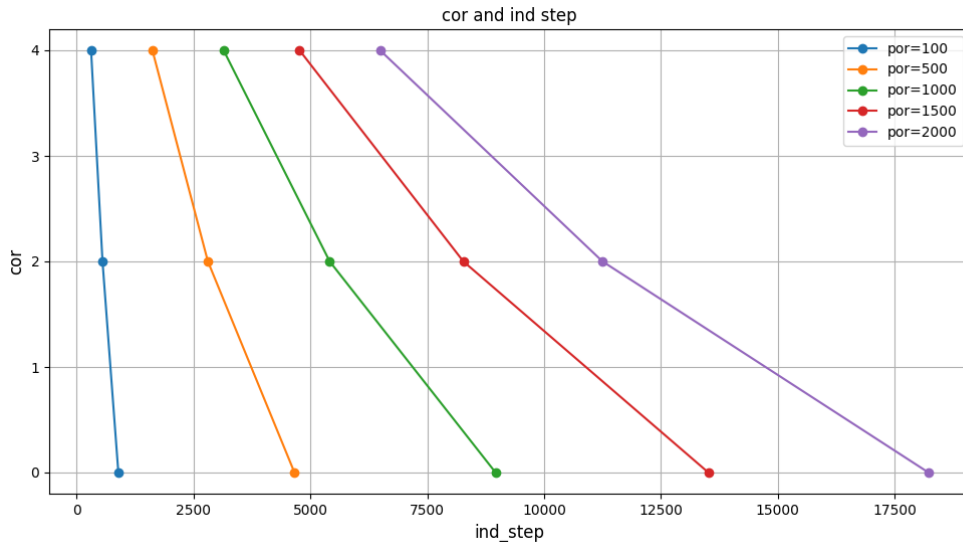


Рис. 5. Время вхождения в синхронизм при разных порогах

Как видно из графиков значительное время система проводит в состоянии рассинхронизации на 4 семпла. Рассмотрим ситуацию более подробно. Рассинхронизация на 4 семпла создает устойчивое состояние неопределенности. В данном случае, в центральном окне будет четыре семпла одного знака и четыре другого, в идеальном случае ноль, в реальном - минимум. В смежных с центральным - окнах, будет 3 и 5 семплов, соответственно разница два и в крайних окнах будут максимальные амплитуды.

На рисунке 6 показано поведение аккумуляторов пяти окон при пороге 100 и  $E_bN_0 = 12\text{dB}$ . Как видим аккумуляторы крайних окон  $a_0$  и  $a_4$  возрастают одинаково быстро и кто-то из них случайным образом выиграет, в данном примере побеждает нулевое окно и становится центральным, в котором смещение на 2 семпла. В следующем цикле неопределенности нет, так как есть явный фаворит – нулевое окно, его аккумулятор опережает другие и достигает порога значительно быстрее чем в предыдущем цикле. После переноса центрального окна в нулевое система входит в синхронизм.

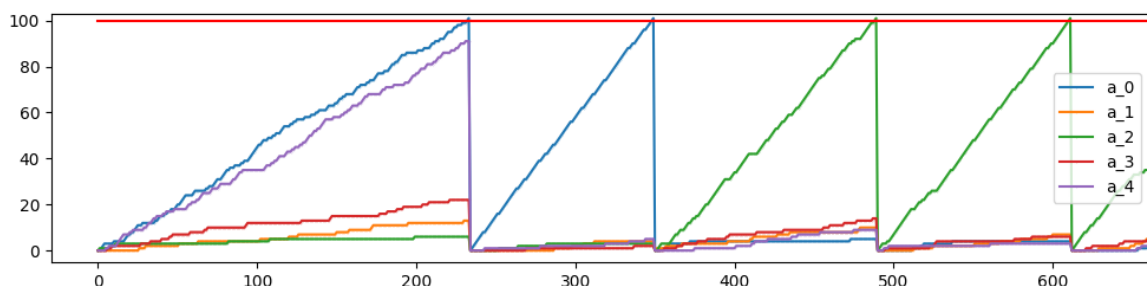


Рис. 6. Вхождение в синхронизм при рассогласовании на 4 семпла.

Сравним алгоритмы 7 – окон и алгоритм, предложенный в [1] (1-окно), по вероятности ошибок и вероятности нахождения в состояниях рассинхронизации в диапазоне  $E_bN_0 = 0..12\text{ dB}$ . На рисунке 7 приведены результаты моделирования для систем с модуляциями BPSK, DBPSK и DQPSK. Из рисунка видно, что при старте эксперимента в состоянии синхронизации алгоритм

1wind ведет себя нестабильно, и имеет вероятность выхода из синхронизма при большом шуме. Алгоритм 7 wind – стабильно сохранял синхронизм в данной серии эксперимента. Выходы из синхронизма приводят к некоторому повышению вероятности ошибок системы в целом, что заметно на левом графике рисунка 7.

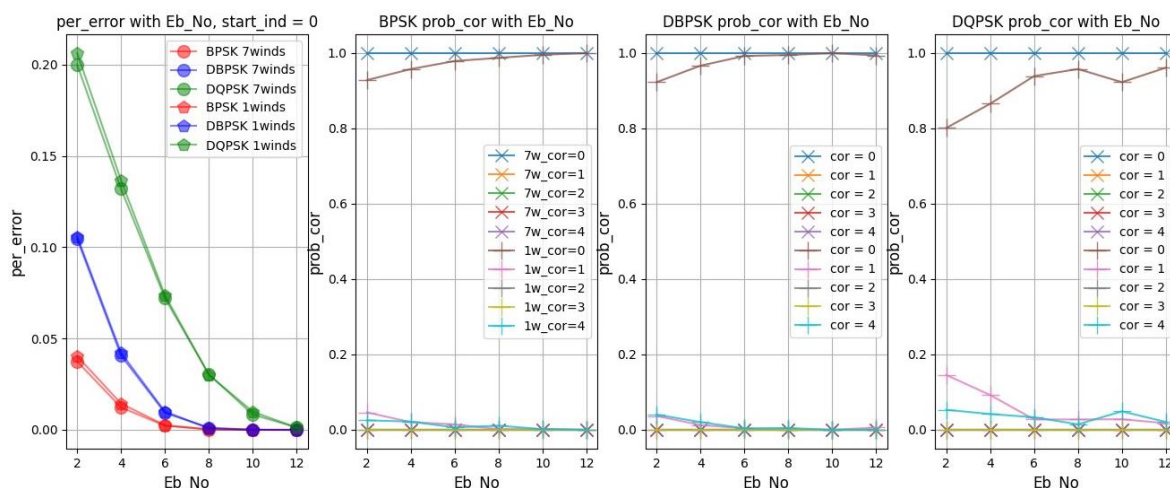


Рис. 7. Сравнение алгоритмов 7 окон и 1 окон (4), вероятности ошибок и вероятность прибытия в состоянии синхронизации или рассинхронизации на разное число

### 3. Заключение

Для данного исследования был реализован проект на языке Python. Проект представляет собой ряд классов элементов системы передачи, таких как, модуляция (демодуляция), формирование кадра, символьная синхронизация, канал передачи с шумом. Так же были созданы классы для генерации входных данных, постобработки и сбора статистики. Для визуализации использовалась открытая библиотека plt.

Результаты исследования показали, что предложенный алгоритм работает стабильно и имеет меньшее время синхронизации и выше вероятность сохранения синхронизма в сравнении с алгоритмом 1wind. Кроме того, в предложенном алгоритме быстрее выходит из устойчивого неопределенного состояния при рассинхронизации на 4 семпла.

Анализ показал, что при соотношении  $E_b/N_0 > 2$  dB, для надежного вхождения в синхронизм алгоритма с пятью окнами, можно порекомендовать порог 1000 и в начало кадра достаточно добавить 5000 символов меандра.

Рассмотренный алгоритм был реализован в прототипе цифровой системы передачи данных на базе SDR HackRF, что подтвердило его работоспособность в реальных условиях.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Мелентьев О. Г., Максимов И. Н. Алгоритм поэлементной синхронизации по отсчетам комплексной огибающей без использования ФАПЧ. Вестник СибГУТИ. 2021. №4 С.87-94.
2. Гончаров Д.А., Мелентьев О.Г., Максимов И.Н. Адаптивный механизм символьной синхронизации на основе учёта зашумлённости входного сигнала // Обработка информации и математическое моделирование: материалы Международной научно-технической конференции/ Сиб. гос. ун-т телекоммуникаций и информатики. Новосибирск: СибГУТИ, 2023. С.13-21.
3. Мелентьев О. Г., Максимов И. Н., Шевнина И. Е. Применение закодированных сверточным кодом преамбул для кадровой синхронизации. Вестник СибГУТИ 2019. №4 С.93-104.

## МИКРОСЕРВИСНАЯ АРХИТЕКТУРА: ЭФФЕКТИВНОЕ РЕШЕНИЕ ДЛЯ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ПЕРЕВОЗКАМИ

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

Ключевые слова: микросервисная архитектура, монолитная архитектура, автоматизация, kubernetes

В статье приведены схемы монолитной и микросервисной архитектуры. Автоматизация с использованием микросервисной архитектуры является важной темой в современной разработке программного обеспечения. В данный момент времени на РЖД используется монолитная архитектура. Целью данной статьи является определение наиболее подходящей для предприятия архитектуры. Задачи статьи – определить различия микросервисной и монолитной архитектуры, выявить преимущества использования микросервисной архитектуры.

К.N. Kudryavtseva, A.V. Volynskaya

## MICROSERVICE ARCHITECTURE: AN EFFECTIVE SOLUTION FOR AUTOMATED TRANSPORTATION MANAGEMENT

Ural State University of Railway Transport (USURT), Ekaterinburg, Russia

Keywords: microservice architecture, monolithic architecture, automation, Kubernetes

The article provides diagrams of monolithic and microservice architecture. Automation using microservice architecture is an important topic in modern software development. At this point in time, Russian Railways uses a monolithic architecture. The purpose of this article is to determine the most suitable architecture for the enterprise. The objectives of the article are to determine the differences between microservice and monolithic architectures and to identify the advantages of using microservice architecture.

В настоящее время на РЖД используется автоматизированная система оперативного управления перевозками (АСОУП). Она предназначена для создания и поддержания в реальном времени информационной модели перевозочного процесса, прогнозирования и текущего планирования эксплуатационной работы железных дорог. АСОУП обеспечивает оперативной информацией соответствующих работников своей дороги, соседних дорог и центрального аппарата ОАО «РЖД». Система АСОУП позволяет решать следующие задачи:

- контроль поездного положения;
- учёт перехода поездов, вагонов и контейнеров по стыковым пунктам;
- контроль за соблюдением норм массы и длины грузовых поездов;
- прогноз прибытия грузов на станции назначения;
- оперативный контроль погрузки и выгрузки;
- оперативный контроль дислокации и состояния локомотивов;
- слежение за дислокацией разрядных грузов на дороге, за специализированным подвижным составом, за нахождением на полигоне дороги вагонов стран СНГ и Балтии;
- пономерной учёт, контроль дислокации, анализ использования и регулирование вагонного парка [1].

Сервис контроля исполнения перевозочного процесса на микросервисной архитектуре предназначен для оперативного контроля соблюдения технологических нормативов выполнения грузовых и коммерческих операций и передачи сведений о выявленных нарушениях в Единый автоматизированный ресурс мониторинга и управления рисками нарушения сроков доставки

грузов и порожних собственных вагонов нового поколения (ЕАСАПР СД НП) для дальнейшего автоматического выявления причин задержек грузовых отправок.

Реализация обеспечит учет вагоно-часов задержек грузов и порожних грузовых вагонов при осуществлении перевозки железнодорожным транспортом и контроля выполнения технических, грузовых и коммерческих операций в соответствии с Методическими указаниями по сквозному хронологическому учету вагоно-часов задержек при осуществлении перевозок железнодорожным транспортом от 09.02.2021г. № 245р с последующей передачей сведений о выявленных задержках в программное обеспечение ЕАСАПР СД НП для оперативного выявления в автоматизированном режиме обстоятельств, приведших к задержке вагонов в пути следования.

Реализуемое ПО повысит уровень автоматизации и позволит исключить человеческий фактор при выполнении бизнес-процесса «Определение обстоятельств, приведших к задержкам грузов и порожних вагонов в пути следования», что в свою очередь позволит сократить убытки ОАО «РЖД» от выплат пени по исковым требованиям об уплате штрафов за просрочку доставки грузов и порожних грузовых вагонов.

Модель создается с целью обеспечения соответствия средств автоматизации современным подходам к управлению перевозочным процессом, таким как:

–переход на процессный подход, требующий контроля его исполнения и наличия объектно-событийной модели четко в соответствии с моделями процессов и контролем на уровне автоматизированной системы, а не человека, его безусловного выполнения с фиксацией всех отклонений в режиме on-line.

–управление доставкой каждой отправки, а не управление на основе средних значений показателей работы.

–переход на управление на основании прогнозной цепочки бизнес-процессов выполнения перевозки груза с учётом возможностей инфраструктуры, применением логических контролей, результат работы которых должен определять возможный сценарий будущего.

Система должна обеспечивать реализацию названных целей за счёт:

- создания единой импортонезависимой платформы;
- повышения эффективности процессов управления грузовыми перевозками и повышения эффективности автоматизированных систем, задействованных в управлении процессом перевозок.

Система АСОУП разработана с помощью такого подхода как «Монолит» и представляет из себя единую и прочную структуру, в которой все компоненты приложения крепко связаны между собой.

Монолитная архитектура — это подход к разработке программного обеспечения, при котором все компоненты приложения находятся внутри единого целого – монолита [2]. В рамках монолитной архитектуры весь код и функциональность приложения объединены в одно приложение, выполняющее все задачи, такие как обработка запросов, доступ к базе данных и взаимодействие с пользовательским интерфейсом.

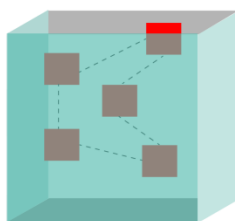


Рис. 1. Смеха монолитной архитектуры

Одно из главных преимуществ монолитной архитектуры — это ее простота. Такой подход позволяет разрабатывать и развертывать приложение относительно быстро и просто. Также монолитная архитектура позволяет использовать привычные и знакомые инструменты и технологии разработки.

Однако, у монолитной архитектуры есть и некоторые недостатки. Во-первых, монолиты могут стать очень крупными и сложными, особенно с ростом функциональности и объема кода.



Это может привести к сложностям в поддержке и модификации приложения. Во-вторых, монолитное приложение требует полной перекомпиляции и перезапуска при внесении изменений в любую его часть. Это может увеличить время разработки и задержать выпуск новых версий.

Для увеличения производительности и повышения оперативности в разработке новых компонентов системы необходимо перейти на микросервисную архитектуру.

Микросервисная архитектура — это модульный подход к разработке программного обеспечения, при котором приложение разделяется на небольшие, независимые компоненты - микросервисы. Каждый микросервис выполняет определенную функцию и может быть разработан, развернут и масштабирован независимо от других сервисов в приложении.

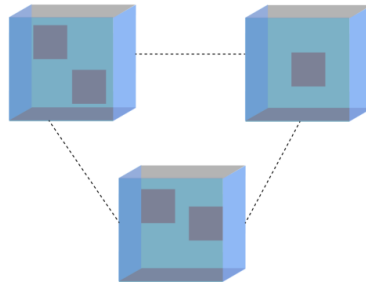


Рис. 2. Схема микросервисной архитектуры

Одно из главных преимуществ микросервисной архитектуры — это гибкость и масштабируемость. Благодаря разделению функциональности на отдельные сервисы, разработчики имеют большую свободу выбора технологий и инструментов для каждого сервиса. Это позволяет оптимизировать каждый сервис под его конкретные потребности и требования. Кроме того, микросервисы могут быть развернуты и масштабированы независимо друг от друга. Это означает, что при увеличении нагрузки на один сервис можно легко добавить ещё экземпляры данного сервиса или горизонтально масштабировать его. Такой подход позволяет эффективно использовать ресурсы и обеспечивать высокую производительность и отказоустойчивость всего приложения.

Микросервисная архитектура способствует повышению скорости разработки и обновлений. Каждый сервис может быть разработан и протестирован независимо, что позволяет распараллеливать процесс разработки и ускорять время доставки новых функций или исправлений ошибок.

Однако, у микросервисной архитектуры есть и некоторые вызовы. Управление и координация между различными сервисами может быть сложной задачей. Взаимодействие между сервисами должно быть осуществлено через сетевые вызовы, что может влиять на производительность и требовать обработки ситуаций сетевых сбоев. Кроме того, в случае большого количества микросервисов может возникнуть сложность в управлении инфраструктурой и мониторинге всей системы.

Таблица 1. Сравнение монолитной и микросервисной архитектур

Аспект	Монолитная архитектура	Микросервисная архитектура
Разработка и развертывание	Одна база кода; простые процессы разработки и развертывания	Децентрализованная разработка; каждый сервис разрабатывается и разворачивается по отдельности
Масштабируемость и производительность	Масштабируемость всего приложения; возможно нерациональное использование ресурсов	Детализированная масштабируемость; оптимальное распределение ресурсов, исходя из потребностей различных сервисов
Обслуживание и расширяемость	Единая база кода; проще понять и легче обслуживать	Независимые сервисы; проще добавлять новые функции, из изменяя всё приложение
Технологическое разнообразие и автономность	Ограниченный стек технологий; привязка к	Разнообразие технологий, доступных для каждого сервиса; можно выбрать более подходящие технологии

	определенному набору технологий	
Отказоустойчивость	Единая точка отказа; Отказы влияют на все приложения	Изолированные отказы; Отказоустойчивость лучше
Координация и взаимодействие	Прямые вызовы функций; более простая коммуникация и обмен данными	Взаимодействие между сервисами; дополнительные средства для координации и согласованности данных

Выбор между монолитной и микросервисной архитектурой зависит от конкретных требований и характеристик проекта. Монолитная архитектура может быть предпочтительна для небольших проектов с простой функциональностью, в то время как микросервисная архитектура предоставляет большую гибкость и масштабируемость для более сложных и требовательных проектов.

В целом, автоматизация с использованием микросервисной архитектуры является актуальным решением, которое способствует более гибкому, масштабируемому и эффективному управлению приложениями и системами.

Преимущества микросервисной архитектуры в контексте управления перевозками включают:

1. Масштабируемость. Микросервисная архитектура позволяет гибко масштабировать каждый сервис в соответствии с его потребностями. Это особенно полезно в сфере управления перевозками, где объем данных и запросов может значительно меняться в зависимости от времени суток или сезона.

2. Гибкость и модульность. Поскольку каждый сервис является отдельным и независимым компонентом, разработчики могут изменять и модифицировать каждый сервис по отдельности, без влияния на работу других сервисов. Это обеспечивает гибкость и возможность быстро адаптироваться к изменяющимся требованиям и новым бизнес-правилам.

3. Расширяемость и интеграция. Микросервисная архитектура облегчает интеграцию с другими системами и сервисами. Каждый сервис может взаимодействовать с внешними сервисами через API, что позволяет создавать эффективную сеть взаимодействия между различными частями системы управления перевозками.

4. Устойчивость к сбоям. При использовании микросервисной архитектуры отказ одного сервиса не приводит к полной остановке всей системы. Вместо этого, другие сервисы могут продолжать работать нормально, что обеспечивает более высокую отказоустойчивость и надежность системы.

Выпуская цифровые сервисы, даже крупный бизнес вынужден использовать стартап-подход. Ведь разрабатывать и выводить новые продукты на рынок нужно быстро, одновременно не забывая о качестве обслуживания клиентов, — только так можно выжить в высококонкурентной среде. Кроме того, компаниям важно сразу получать дополнительные IT-ресурсы, когда нагрузки на сервисы растут, и не переплачивать за них во время спадов активности пользователей.

В этом помогают такие технологии как микросервисы и контейнеризация, а для управления ими используют Kubernetes — этот инструмент уже стал стандартом разработки и позволяет IT-отделам создавать продвинутые архитектуры для достижения бизнес-целей компании [3].

Контейнеры — это способ упаковки приложения. В контейнере приложение можно передать на тот сервер, где оно будет работать, в том виде, в каком разработчик собрал его у себя на компьютере, такая «упаковка» как бы защищает его. Это исключает сюрпризы, вроде тех, когда во время теста приложение работает, а при переносе в рабочую среду — ломается. В эти же контейнеры стали упаковывать микросервисы, чтобы упростить их перенос из среды разработки туда, где им предстоит функционировать.

Естественно, что большие приложения — это много контейнеров с микросервисами внутри. Чем больше приложение, тем больше у него составных частей. С его помощью можно одной кнопкой обновить нужную часть приложения, откатить обновление назад, выделить ресурсы там, где их не хватает, и сократить мощности там, где их много.



При этом микросервисы и Kubernetes можно интегрировать с теми IT-системами, что уже работают в компании — не всегда нужно всё перестраивать с нуля, чтобы построить хорошо работающий конвейер разработки и быстрее выпускать новые продукты.

Такие технологии, конечно, дают целый ряд преимуществ — и разработчикам, и бизнес-подразделениям. Посмотрим, как и для чего используют Kubernetes известные компании.

Применение Kubernetes для РЖД имеет несколько преимуществ:

1. Для РЖД, где операционная деятельность включает в себя множество сервисов и приложений, особенно важна масштабируемость. Kubernetes может автоматически масштабировать приложения в зависимости от изменяющейся нагрузки, что позволяет РЖД гибко реагировать на изменения и обеспечить стабильность работы системы.

2. Kubernetes предоставляет мощные средства для управления ресурсами, такими как CPU и RAM, что позволяет более эффективно использовать вычислительные мощности. РЖД может легко выделить нужные ресурсы для каждого приложения или сервиса, а также контролировать их потребление. Это помогает снизить издержки и повысить производительность системы.

3. Kubernetes строит свою архитектуру с учетом отказоустойчивости. Он обеспечивает возможность автоматического восстановления после сбоев и распределения нагрузки на другие рабочие узлы. Для РЖД, где непрерывная доступность критична, это очень важно. Kubernetes гарантирует, что приложения продолжат работать даже в случае сбоя одного или нескольких узлов.

5. Общие стандарты: Kubernetes является популярной и широко используемой платформой для контейнеризации и оркестрации. Использование Kubernetes означает, что РЖД пользуется общими стандартами отрасли, что упрощает обновление и интеграцию новых сервисов и приложений. Это также дает возможность РЖД взаимодействовать с другими организациями, которые также используют Kubernetes.

Таким образом, применение Kubernetes для РЖД может значительно улучшить управление и масштабируемость системы, обеспечить высокую отказоустойчивость и снизить издержки, что является важным для такой крупной и комплексной организации.

#### Список литературы:

1. Автоматизированная система управления перевозками // Евразия Вести 2006. URL: <http://eav.ru/publ1.php?publid=2006-05a10> (дата обращения 12.09.2023)
2. Ньюмен С. От монолитам к микросервисам : учеб. пособие. М., 2021. 272 с.
3. Джиджи С. Оркестрация контейнерных архитектур : учеб. пособие М. 2019. 400 с.

## ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПИКОВОЙ МОЩНОСТИ И ФАЗЫ СМЕЖНЫХ СОЛИТОНОВ, РАСПРОСТРАНЯЮЩИХСЯ В TDM РЕЖИМЕ

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

Ключевые слова: смежные оптические солитоны, пиковая мощность, моделирование.

Современные телекоммуникационные системы связи базируются на волоконно-оптических линиях связи, благодаря которым обеспечивается высокая пропускная способность канала связи (десятки терабит в секунду) на расстояние в сотни, тысячи километров. Однако, реализация таких сетей крайне затруднительна, поскольку дальность связи и скорость передачи данных ограничена влиянием дисперсионного параметра оптоволокна. Одним из путей преодоления влияния дисперсии – это применение солитонных систем связи. Наука о солитонах развивалась в результате современных трудов физиков, математиков и специалистов в области математического и натурального моделирования солитонных систем связи. В последние десятилетия учеными в данной области рассматриваются вопросы устойчивого распространения солитонных импульсов в длиннопролетных линиях. Исследования, проводимые в данном направлении, имеют особую актуальность с точки зрения реализации оптической связи протяженностью в несколько тысяч километров. Целью статьи является исследование взаимодействия смежных солитонов разной пиковой мощностью и фазы, распространяющихся при нулевых потерях в оптоволокне протяженностью 780 км.

S.V. Mikheeva, E.A. Minina, I.I. Shestakov

## INVESTIGATION OF THE INFLUENCE OF PEAK POWER AND PHASE OF ADJACENT SOLITONS PROPAGATING IN TDM MODE

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

Keywords: adjacent optical solitons, peak power, modeling.

Modern telecommunication communication systems are based on fiber-optic communication lines, which ensure high bandwidth of the communication channel (tens of terabits per second) over a distance of hundreds, thousands of kilometers. However, the implementation of such networks is extremely difficult, since the communication range and data transfer rate are limited by the influence of the dispersion parameter of the fiber. One of the ways to overcome the influence of dispersion is the use of soliton communication systems. The science of solitons has developed as a result of modern works by physicists, mathematicians and specialists in the field of mathematical and full-scale modeling of soliton communication systems. In recent decades, scientists in this field have been considering the issues of stable propagation of soliton pulses in long-span lines. The research carried out in this direction is of particular relevance from the point of view of the implementation of optical communication with a length of several thousand kilometers. The purpose of the article is to study the interaction of adjacent solitons of different peak power and phase propagating at zero losses in a 780 km fiber.

Исследование взаимодействия пары оптических солитонов в оптоволокне выполнено при помощи моделирования в OptiPerformer, используя из библиотеки проект «Ch9 - Interaction of a pair of fundamental solitons.osp». На рисунке 1 представлена блок-схема эксперимента для исследования взаимодействия пары оптических солитонов распространяющихся в TDM режиме. Блок-схема состоит из: генератора псевдослучайной кодовой последовательности, генератора

оптического солитона, фазовращателя, идеального оптического мультиплексора, оптического волокна, анализатора спектра и визуализатора временной области.

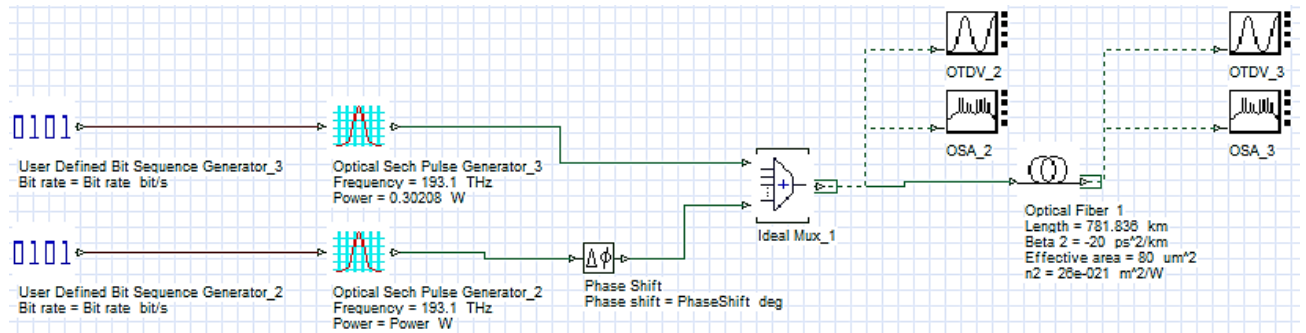


Рис. 1. Блок-схема исследования взаимодействия пары оптических солитонов

Исследование базируется на влиянии фазы и пиковой мощности смежного солитона на пиковую мощность солитонов действующих на выходе линии связи при распространении их в оптоволокне длиной 780 км с нулевым километрическим затуханием и битовой скоростью 40 Гбит/с. Нулевые потери в оптоволокне эквиваленты солитонной линии с оптическими усилителями, которые обеспечивают поддержания пиковой мощности для баланса дисперсии групповых скоростей (ДГС) и нелинейности оптоволокна [1-3].

Получены графики зависимости пиковой мощности первого ( $P_{1\_out}$ ) и второго ( $P_{2\_out}$ ) солитона в конце линии связи в зависимости от пиковой мощности первого солитона ( $P_{1\_in}$ ) в начале линии связи при постоянной пиковой мощности второго солитона ( $P_{2\_in} = 0,302$  Вт), действующих на входе линии связи. Графики зависимости  $P_{1\_out}(P_{1\_in})$  и  $P_{2\_out}(P_{1\_in})$  представлены на рисунке 2. Как видно из графиков, разная пиковая мощность солитонов в начале линии связи, в независимости от начальной фазы солитона, ведет к перекачке оптической энергии между солитонами. При равной пиковой мощности ( $P_{1\_in} = P_{2\_in} = 0,302$  Вт), солитоны ведут себя как фундаментальный солитон (солитон первого порядка [1-3]).

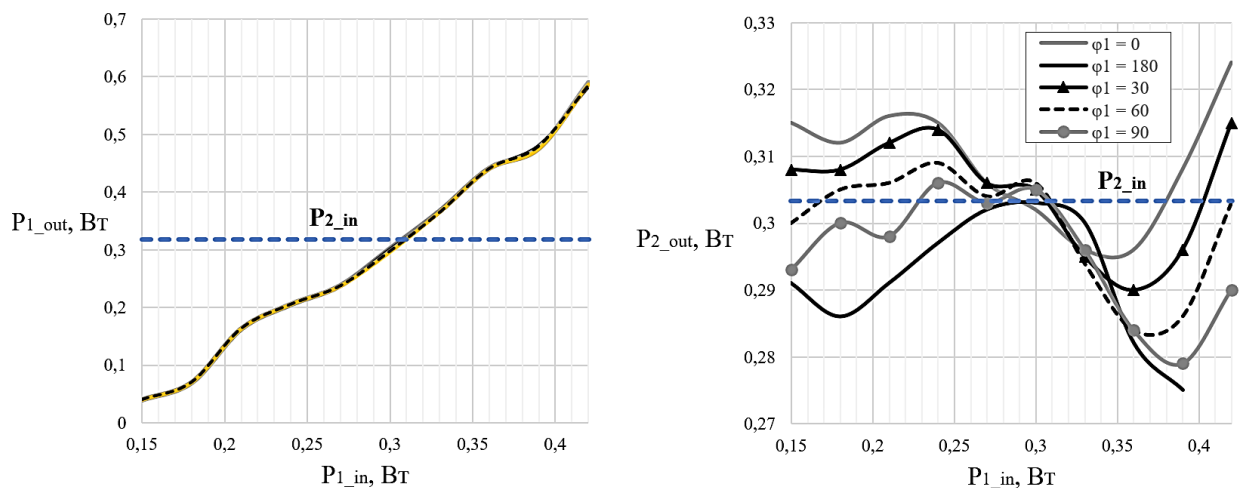


Рис. 2. Графики зависимости  $P_{1\_out}(P_{1\_in})$  и  $P_{2\_out}(P_{1\_in})$

В процессе эксперимента замечено незначительно влияние фазы смежного солитона на пиковую мощность солитонов в конце линии связи при равной пиковой мощности солитонов в начале линии связи. Максимальное отклонение пиковой мощности смежных солитонов ( $\Delta P$ ) составило 9 мВт при фазе первого солитона равной  $\phi_1 = \phi_2 - 90^\circ$  (рисунок 3).

В случае изменения пиковой мощности смежного солитона, распространяющихся в линии связи с затуханием, произойдет нарушение баланса ДГС и нелинейности оптоволокна, что приведет к уширению солитонов. Можно предположить, что на изменение пиковой мощности смежных солитонов, передаваемых в TDM канале, влияет процесс усиления сигнала. Дело в том,

что пиковая мощность информационного сигнала, представляющего собой случайную последовательность оптических солитонов, зависит от частоты следования солитонов. Если частота следования солитонов увеличивается, (например, на усилитель поступает кодовая комбинация 1111111) – наблюдается увеличение пиковая мощность сигнала, но, если частота следования уменьшается (например, на усилитель поступает кодовая комбинация 1000001) – наблюдается уменьшение пиковой мощности сигнала. В таком случае, сигнал, действующий на входе оптического усилителя, обладает средней пиковой мощностью, что влияет на уровень выходного сигнала в процессе усиления. На выходе усилителя будут действовать усиленные оптические солитоны с разной пиковой мощностью.

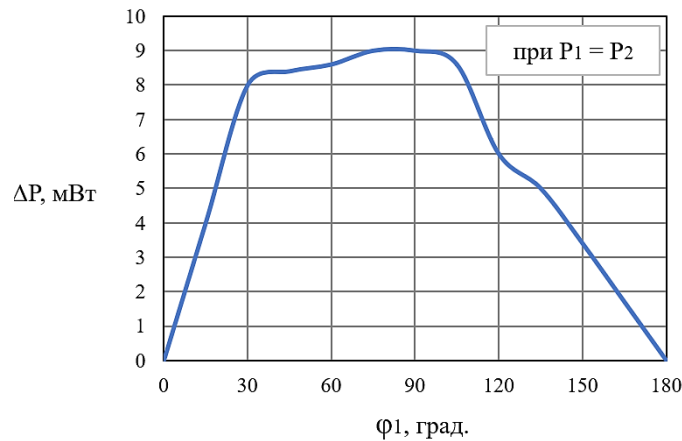


Рис. 3. График зависимости  $\Delta P(\varphi_1)$

Также следует учитывать то, что в процессе усиления солитона, происходит фазовое смещение момента импульса на выходе усилителя, и чем больше усилителей на линии, тем сильнее смещается фазовый момент импульса.

Подводя итогу, можно утверждать то, что даже при нулевых потерях в линии связи, для поддержания солитонного эффекта требуется поддержание не только заданной пиковой мощности, но и начальной фазы импульса [4,5]. Данный эксперимент показывает не эффективность солитонных систем связи в случае применения фазовой модуляции или многоуровневой амплитудной модуляции от символа к символу, что ограничивает их пропускную способность не более 40 Гбит/с. Наглядное представление многоуровневой модуляции можно показать в виде временной диаграммы двух смежных солитонов (рисунок 4).

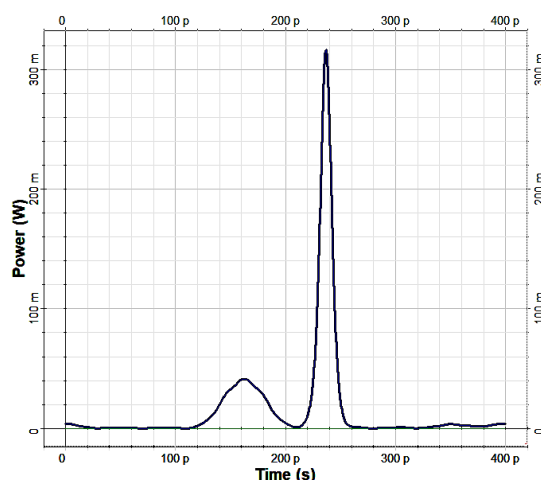


Рис. 4. Временная диаграммы смежных солитонов в конце линии связи при пиковой мощности в начале линии связи  $P_{1\_in} = 0,152$  Вт и  $P_{2\_in} = 0,302$  Вт

Из временной диаграммы видно, что разная пиковая мощность не позволяет сохранять солитонный режим. Даже в условиях отсутствия затухания в линии связи, для первого солитона

(при начальной пиковой мощности 0,152 Вт) наблюдается не только уменьшения мощности импульса, но и уширение, что показывает существование солитонного режима в условиях равной мощности солитонов при пиковой мощности не менее 0,3 Вт.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Новокшенов В.Ю. Введение в теорию солитонов / Новокшенов В.Ю. - Ижевск: Институт компьютерных исследований, 2019. – 96 с. - [Электронный ресурс]. - URL: <http://www.iprbookshop.ru/91922.html>
2. Беспрозванных В.Г. Нелинейные эффекты в волоконной оптике: учеб. пособие / В.Г. Беспрозванных, В.П. Первадчук. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2011. – 228 с. - [Электронный ресурс]. – URL: [https://pstu.ru/files/file/FPMM/of/bvg/besprozvannyh\\_pervadchuk\\_nelinejnie\\_effecti.pdf](https://pstu.ru/files/file/FPMM/of/bvg/besprozvannyh_pervadchuk_nelinejnie_effecti.pdf)
3. Гончаренко А.М. Оптические гауссовы пучки и солитоны: монография / Гончаренко А.М. – Минск: Белорусская наука, 2011. – 125 с. – ISBN 978-985-08-1294-0. - Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. - URL: <http://www.iprbookshop.ru/10081.html>
4. Андреева Е.И., Былина М.С., Глаголев С.Ф., Доценко С.Э., Чаймарданов П.А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Часть 3. Труды учебных заведений связи. Т. 4. № 3, 2018. С.5-16. [Электронный ресурс]. - Режим доступа: [https://tuzs.sut.ru/release/tuzs\\_v4\\_i3\\_y2018/article\\_1.pdf](https://tuzs.sut.ru/release/tuzs_v4_i3_y2018/article_1.pdf)
5. Мاستин А.А., Рябочкина П.А. Влияние мощности насыщения, глубины модуляции и времени релаксации насыщающегося поглотителя на параметры импульса солитонного волоконного лазера. [Электронный ресурс]. - Квантовая электроника. 2020. Т. 50. № 4. С. 419-424. - Режим доступа: [www.mathnet.ru/qe17225](http://www.mathnet.ru/qe17225)

## К РАСЧЕТУ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ СЕТИ ДОСТУПА

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

Ключевые слова: волоконно-оптическая линия связи, затухание сигнала, участок оптического кабеля, деградация оптоволокна, отказ, техническое обслуживание и ремонт, показатели надежности.

В статье рассматриваются вопросы расчета готовности волоконно-оптической линии связи пассивной оптической сети доступа в условиях постепенных и внезапных отказов. Волоконно-оптическая линия связи разбивается на участки, каждый из которых характеризуется своей механической нагрузкой. Для каждого из участков определяется, исходя из гамма-процентной наработки на отказ, срок службы, обусловленный деградацией волоконно-оптической линии и коэффициент готовности в условиях действия постепенных и внезапных отказов. При вычислении коэффициентов готовности участков учитывается применяемый метод технического обслуживания и ремонта.

V.P. Shuvalov, I.G. Kvitkova

## ON THE EVALUATION THE DEPENDABILITY MEASURES OF THE ACCESS NETWORK FIBER-OPTIC COMMUNICATION LINE

Siberian State University of Telecommunications and Information Science (SibSUTIS),  
Novosibirsk, Russia

Keywords: fiber-optic communication line, signal attenuation, optical cable section, fiber degradation, failure, maintenance, dependability measures.

The article considers the issues of calculating the availability of a passive optical access network fiber-optic communication line in conditions of gradual and sudden failures. The fiber-optic communication line is divided into sections, each of which is characterized by its own mechanical load. For each of the sections, the service life due to degradation of the fiber-optic line and the availability factor under conditions of gradual and sudden failures are determined based on the gamma-percentile operation time to failure. When calculating the availability factor for sections, the applied method of maintenance and repair is taken into account.

Надежность относится к одному из основных показателей, характеризующих качество предоставляемых услуг. При этом вопросам обеспечения надежности систем уделяется в литературе особое внимание. Проблематике надежности посвящены статьи и монографии, доклады на конференциях [1-8 и др.]. Для оценки надежности восстанавливаемых систем и элементов чаще всего используется такой комплексный показатель как коэффициент готовности, который вычисляется по формуле

$$K_{\Gamma} = \frac{T_{\text{Н}}}{T_{\text{Н}} + T_{\text{В}}}, \quad (1)$$

где  $T_{\text{Н}}$  – время наработки на отказ;  
 $T_{\text{В}}$  – время восстановления.

В ряде случаев определяется не коэффициент готовности (1), а коэффициент простоя  $K_{\text{П}}$ :

$$K_{\Pi} = 1 - K_{\Gamma} = \frac{1}{T_{\text{H}}/T_{\text{B}} + 1} \quad (2)$$

Т.к.  $T_{\text{H}}/T_{\text{B}} \gg 1$ , то вместо  $K_{\Pi}$  из (2) можно использовать

$$K_{\Pi}^* \approx T_{\text{B}}/T_{\text{H}} \quad (3)$$

Очевидно, что  $K_{\Pi} > K_{\Pi}^*$ .

В соответствии с требованиями к современным телекоммуникационным сетям  $K_{\Gamma}$  должен быть равен 0.999999 [9], который необходимо обеспечить за счет соблюдения технологий на всех жизненных этапах системы, т.е. производства и эксплуатации.

В настоящее время на оптических сетях доступа широко используется технология пассивных оптических сетей доступа PON. При этом физический тракт передачи состоит из элементов, представленных на рис. 1.

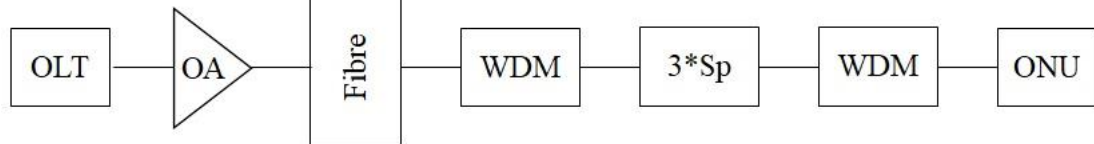


Рис. 1. Физический тракт передачи информации WDM-PON

На рис. 1 представлены основные элементы физического тракта передачи WDM-PON. Это оптический линейный терминал OLT, оптический усилитель OA, оптоволоконная линия (ОВЛ), мультиплексор и демультиплексор WDM соответственно, сплиттер Sp и абонентский оптический терминал ONU, который является приемником. В соответствии с [10] значение FIT (Failure rate) – среднее число отказов в течение периода  $10^9$  часов – для OLT равно 256, для сплиттера 1:2 – 50, для AWG мультиплексора – 200, для ONU – 256 и, наконец, для ОВЛ – 570 на 1 км. Таким образом, наибольший вклад в снижение надежности вносит ОВЛ.

Исходя из определения понятия FIT, для расчета времени наработки на отказ можно воспользоваться формулой для ОВЛ

$$T_{\text{H}} = \frac{10^9}{570 \cdot l}, \text{ ч}, \quad (4)$$

где  $l$  – длина участка волоконно-оптической линии связи (ВОЛС).

Из формулы (4) следует, что время наработки на отказ обратно пропорционально длине участка ОВЛ. Тогда, подставив выражение (4) в (3), получим

$$K_{\Pi}^* = T_{\text{B}} \cdot \frac{570l}{10^9}.$$

Различают конструкционные, производственные, эксплуатационные и деградационные отказы. Отказы могут быть внезапными и постепенными. Примером последних являются отказы, вызванные старением оптоволоконной линии связи. Главным признаком постепенных отказов является возрастающий характер накопления повреждений ОВЛ. При постоянной скорости  $\dot{v}$  (рис.2) накопление повреждений имеет характер, представленный на рис. 3 [11].

Скорость накопления повреждений определяется как

$$\dot{v} = \frac{dv}{dt},$$

где  $v$  – накопление повреждений.

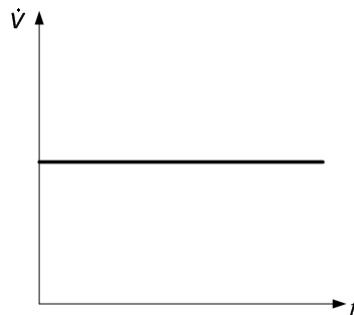


Рис. 2. Скорость накопления повреждений

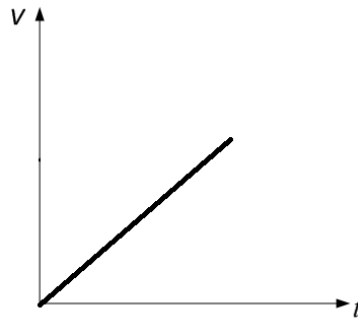


Рис. 3. Накопление повреждений во времени  $v(t)$

В качестве примера накопления повреждений можно взять износ, тогда  $v(t) = kt$ , где  $k$  – коэффициент, характеризующий износ.

Применительно к оптоволокну накопление повреждений можно рассматривать как рост затухания в линии. Этот процесс относится к деградиционным. Рост затухания постепенно приводит к отказу. В данном случае отказом является достижение затухания в ОВЛ такого значения, при котором прием сигнала становится невозможным. Такой подход к определению срока службы ОВЛ можно найти в работе [12]. На деграцию оптического кабеля также влияет ряд факторов, таких как механические воздействия, вода, перепады температур. [13] При этом можно вычислить исходный цикл деградации, используя [14] в условиях гамма-процентной наработки на деградиционный отказ.

Процесс деградации ОВЛ можно представить как марковский процесс размножения. Использование марковских процессов для моделирования явления деградации было впервые предложено и обосновано в работах [15-19].

Внезапные отказы в зависимости от метода технического обслуживания и ремонта (ТО и Р) приводят или к соединению места обрыва, или к замене участка оптического кабеля. При использовании разъемных соединений в месте обрыва происходит ослабление сигнала, передаваемого по ОВЛ сети доступа, т.е. увеличивается затухание на значение  $\Delta b$  и уменьшается энергетический запас. Время исходного цикла деградации при этом уменьшается на  $\Delta t$ .

На рис. 4 представлена диаграмма, поясняющая влияние внезапных отказов на цикл деградации. Влияние внезапных отказов следует отразить путем исключения одного из состояний деградации, что обеспечивается замыканием контактов в блоках К1 и К2 на рис. 4. Вследствие этого происходит обход состояний деградации  $i$  и  $i+1$  при появлении внезапного отказа на  $i-1$  и  $i$ -м состояниях деградации, соответственно. Блоки НР1 и НР2 отражают неработоспособные состояния после внезапного отказа.

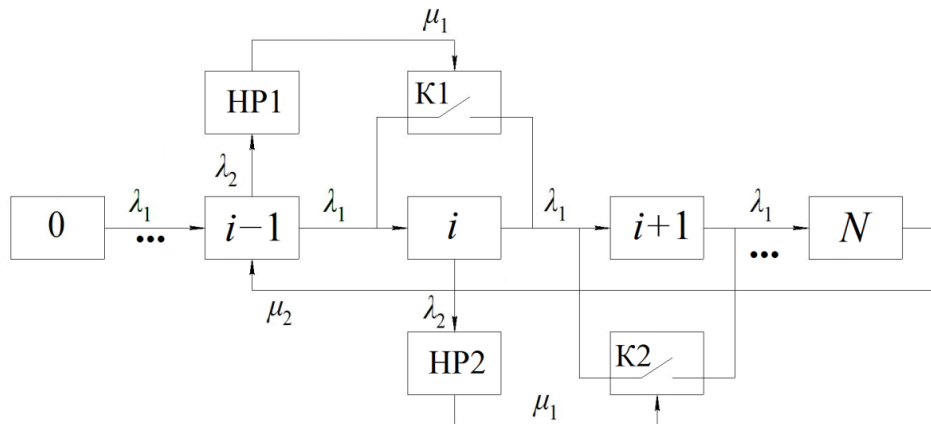


Рис.4. Диаграмма, поясняющая влияние внезапных отказов на цикл деградации

Значение  $\Delta b$  зависит от того, какое соединение используется (сварное или разъемное). Таким образом, при соединениях в месте отказа цикл деградации уменьшается, что приводит к необходимости более ранней замены участка ОВЛ. И, наоборот, при замене участка ОВЛ



вследствие внезапного отказа, как это следует из [20], цикл деградации растет. Соответственно, коэффициент готовности также увеличивается.

Как уже отмечалось, помимо постепенных отказов в процессе эксплуатации возникают внезапные отказы, которые можно считать независимыми от постепенных отказов. Основной причиной внезапных отказов в ОВЛ являются земляные работы в месте прокладки кабеля. Такие отказы составляют 80 % и более от всех типов внезапных отказов и происходят практически с одинаковой интенсивностью во времени, независимо от степени износа оптоволокна.

Отказы также делятся на явные и скрытые. К явным отказам относятся отказы, обнаруживаемые визуально или штатными методами и средствами контроля и диагностирования при подготовке объекта к применению или в процессе его применения. Скрытый отказ – отказ, не обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования, но выявляемый при проведении технического обслуживания или специальными методами диагностирования. [21]

В процессе контроля и диагностирования отказов возможны ситуации, когда при отсутствии отказа система контроля фиксирует «отказ» (ошибка контроля первого рода) и, наоборот, при наличии отказа система контроля его не фиксирует (ошибка контроля второго рода). Часто задается вопрос о том, насколько критично наличие ошибок 1-го и 2-го рода. Для пояснения влияния этих ошибок на показатели надежности рассмотрим процесс появления отказов и процесс ремонта во времени (рис. 5).

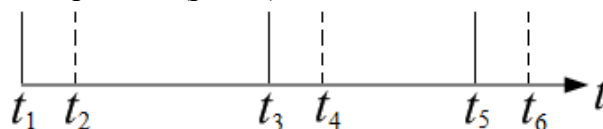


Рис. 5. Процесс появления отказов и восстановлений

Моменты времени  $t_1, t_3, t_5$  и т.д. на рис.5 соответствуют времени появления «отказа». Отрезки времени  $(t_2-t_1), (t_4-t_3), (t_6-t_5)$  определяют время восстановления. При этом отрезки времени  $(t_3-t_2) = (t_5-t_4)$  много больше отрезков времени  $(t_2-t_1) = (t_4-t_3) = (t_6-t_5)$ . При фиксации отказа на отрезках времени  $(t_3-t_2)$  или  $(t_5-t_4)$  имеет место ошибка контроля первого рода. Если считать, что интенсивность реальных отказов равна  $10^{-n}$ , где  $n$  - любое целое число, и отказ будет фиксироваться в результате контроля в интервале  $(t_3-t_2) = (t_5-t_4)$  с одинаковой интенсивностью, например,  $10^{-6}$  1/ч, то число фиксируемых отказов примерно удваивается со всеми вытекающими последствиями.

Что касается ошибок контроля 2-го рода, то при прочих в равных условиях влияние ошибок контроля 2-го рода на надежность будет существенно ниже. Так, если вероятность наличия отказа  $10^{-6}$ , а его условная вероятность пропуска будет также  $10^{-6}$ , то ситуация с пропуском отказа будет  $10^{-12}$ . Это следует из выражения вероятности появления двух событий:  $A$  – отказ;  $B$  – отсутствие отказа:

$$P(AB) = P(A) \cdot P(B/A),$$

где  $P(A)$  – вероятность отказа;

$P(B/A)$  – вероятность необнаружения отказа при его наличии.

Надежность ОВЛ как технической системы зависит от качества материалов, применяемых для изготовления оптического кабеля, конструкции, процессов производства, условий эксплуатации, технического обслуживания и ремонта. Следует учитывать наличие внезапных и постепенных отказов, причинами которых являются различные факторы, такие как механические повреждения линии, деградация оптического волокна. В процессе контроля и диагностирования отказов возможно появление ошибок контроля, которые также влияют показатели надежности.

Используемый метод технического обслуживания и ремонта способствует увеличению или уменьшению цикла деградации оптического кабеля, который позволяет определить время замены оптического кабеля или его участка.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Шувалов В.П., Квиткова И.Г., Зеленцов Б.П. Обеспечение показателей надежности сетей доступа на этапах жизненного цикла: монография. – Новосибирск: СибГУТИ, 2022. – 124 с.
2. Оценка надежности ВОЛС с учетом влияния внешних факторов. / С.С. Лутченко, Е.Ю. Копытов, И.В. Богачков // Динамика систем, механизмов и машин. – 2017. – Т. 5. - №4. – С. 34-39.
3. Wosinska L., Chen J. Reliability performance analysis vs deployment cost of fiber access networks // 7<sup>th</sup> Int'l Conf. Optical Internet, 2008. - P. 1-2.
4. Калимулина Э.Ю. Моделирование и анализ надежности корпоративной сети // Стандарты и качество. - 2008. - № 3. - С. 96–112.
5. Шаманов В.И. Математические модели надежности систем железнодорожной автоматики и телемеханики // Автоматика на транспорте. - 2017. - Т.3. - №1. - С. 7-19.
6. 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.
7. Давыденко А.А. Марковские модели накопления повреждений в оценке и прогнозировании технического состояния мостов // Мосты та тунелі: теорія, дослідження, практика. - 2014. - №6. - С. 40-46.
8. Ромашкова О.Н. Анализ отказоустойчивости плоскости управления / О.Н. Ромашкова, П.А. Иванов, Д.С. Васюк // Спецификация Generalized Multi-Protocol Label Switching ИКСЗТ. - 2010. - № 5. – С. 14-17.
9. Пшеничников А.П., Росляков А.В. Будущие сети: учебник для вузов. – М.: Горячая линия-Телеком, 2022. - 255 с.
10. Wosinska L.W., Chen J. Cost vs reliability performance study of fiber access network architecture. // IEEE Communications Magazine. – 2010. - Vol. 48. - № 2. - P. 56-65.
11. Ушаков И.А. Курс теории надежности систем : учебное пособие для вузов. - М.: Дрофа, 2008. - 239 с.
12. Цым А.Ю. Сроки службы оптических кабелей. Анализы. Риски. // Кабели и провода. – 2020 - № 2 (382). - С. 20-26.
13. Анализ внешних факторов, влияющих на работоспособность волоконно-оптических систем передач / О.А. Губская, М.Н. Плут, О.Р. Спиридонов, Е.В. Фатьянова. // Известия ТулГУ. Технические науки. - 2020. - №5. - С. 102-107.
14. Андреев В. Сценарии прогноза срока службы оптического волокна в КЛС. / В. Андреев, В. Бурдин, А. Нижгородов // Первая миля. - 2020. - № 4 (89). - С. 34-43.
15. Bogdanoff J.L. A new cumulative damage model, part 1. // Journal of applied mechanics, 1978. – Vol. 45. – P. 246-250.
16. Bogdanoff J.L. A new cumulative damage model, part 3. // Journal of applied mechanics, 1978. – Vol. 45. – P. 733-739.
17. Bogdanoff J.L., Krieger W. A new cumulative damage model, part 2. // Journal of applied mechanics, 1978. – Vol. 45. – P. 251-257.
18. Bogdanoff J.L., Kozin F. A new cumulative damage model, part 2. // Journal of applied mechanics, 1980. – Vol. 47. – P. 40-44.
19. Bogdanoff J.L., Kozin F. On stationary cumulative damage models, part 2. // Journal of applied mechanics, 1982. – Vol. 49. – P. 39-42.
20. Shuvalov V.P., Zelentsov B.P., Kvitkova I.G. On the Effect of Sudden Failures and Control Errors of the First Kind on the Degradation Cycle of an Optical Cable // 2023 IEEE 16th international conference of actual problems of electronic instrument engineering (APEIE). Novosibirsk. 10 -12 November, 2023 – P. 550-555.
21. ГОСТ Р 27.102-2021. Надежность в технике: надежность объекта. Термины и определения [Текст]. – Введ. 2022-01-01. - М.: Российский институт стандартизации, 2021. - 36 с.

## ОПТОВОЛОКОННЫЕ ДАТЧИКИ И СЕНСОРНЫЕ СЕТИ

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

Ключевые слова: оптоволоконные датчики, сенсорные сети, волоконные решетки Брэгга, рассеяние Манделъштама-Бриллюэна.

В докладе представлены характеристики многоточечного и распределенного зондирования. Высокий потенциал сенсорных систем, особенно способность выполнять одновременные измерения по длинному и непрерывному оптоволоконному кабелю, а также способность измерять различные параметры с использованием одного и того же чувствительного элемента, являются ценными функциями для мониторинга больших структур или сред, где другие технологии измерения являются проблематичными или их невозможно развернуть. Представленный в докладе материал показывает, что сенсорные сети могут применяться в различных областях, таких как экологический мониторинг, гражданское строительство и машиностроение. Проведено сравнение характеристик коммерческих решений для измерения температуры и деформации.

В работе определены области потенциальных будущих применений, в частности в качестве диагностического инструмента для мониторинга волоконно-оптических линий связи.

**N.I. Gorlov**

## FIBER OPTIC SENSORS AND SENSOR NETWORKS

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

Keywords: fiber-optic sensors, sensor networks, Bragg fiber gratings, Mandelstam-Brillouin scattering.

The report presents the characteristics of multipoint and distributed sensing. The wide range of sensor system functionality is a very valuable advantage in relation to other measurement systems, the use of which is problematic or completely impossible

The material presented in the report shows that sensor networks can be used in various fields, such as environmental monitoring, civil engineering and mechanical engineering. The characteristics of commercial solutions for measuring temperature and deformation are compared. The paper identifies areas of potential future applications, in particular as a diagnostic tool for monitoring fiber-optic communication lines.

### 1. Введение

Оптические волокна обеспечивают высокопроизводительные сенсорные решения для многих типов приложений. Оно выполняет роль чувствительного элемента и среды передачи. Оптоволоконные датчики имеют ряд преимуществ по сравнению с другими типами датчиков. Эти преимущества, по существу, связаны со свойствами оптического волокна, т.е. небольшими размерами, легким весом, устойчивостью к высоким температурам и давлению, электромагнитной пассивностью и другими. Кроме того, оптоволоконные датчики могут использоваться для формирования волоконно-оптической сенсорной сети, что позволяет производителям создавать универсальные решения для мониторинга с несколькими приложениями, например, периодический мониторинг на больших расстояниях в экстремальных или опасных условиях, внутри конструкций и т. д.

Волоконно-оптические датчики могут быть использованы для измерения различных параметров в сетях связи, таких как температура, давление, деформация и другие физические величины [2]. Их высокая точность, быстрая реакция и устойчивость к электромагнитным помехам делают их идеальным выбором для обеспечения надежности и эффективности телекоммуникационных систем. Применение волоконно-оптических датчиков также может повысить уровень безопасности сетей связи, обеспечивая раннее обнаружение неисправностей и предотвращая возможные сбои. Благодаря своей миниатюрности и гибкости, эти датчики могут быть легко интегрированы в различные устройства и системы связи, что делает их очень удобными в использовании. Кроме этого, они могут быть успешно применены для мониторинга состояния крупных инженерных сооружений (газо- и нефтепроводы, плотины, мосты, туннели и другое).

Они способны поддерживать электромагнитную пассивность и устойчивость к влиянию окружающей среды, а также без активных оптоэлектронных компонентов управлять большими массивами распределенных датчиков.

Применение волоконно-оптических датчиков в телекоммуникациях открывает широкие перспективы для улучшения качества связи, оптимизации процессов мониторинга и обеспечения более эффективного функционирования современных телекоммуникационных сетей.

## 2. Классификация волоконно-оптических датчиков

В таблице 1 представлена классификация волоконно-оптических датчиков по принципам функционирования, измеряемым параметрам и сенсорным приложениям [1].

Таблица 1. Классификация волоконно-оптических датчиков

Тип датчика	Измеряемые параметры	Сенсорные приложения	Конфигурации	Основные характеристики
Волоконные решетки Брэгга	Сдвиг длины волны	Температура, давление, деформация, смещение, соленость	Одно/многоточечное зондирование	Погрешности измерения: длины волны < 1%; температуры < 1° С
Интерферометры	Фазовый сдвиг в оптическом диапазоне	Навигация, геодезия, контроль давления элементов конструкции	Одно/многоточечное зондирование	Погрешности в зависимости от сенсорного приложения
Оптические рефлектометры на принципе рассеяния Рэлея	Продукты рассеяния Рэлея	Волоконно-оптические сети, криогенная техника	Распределенное зондирование	Диапазон зондирования – до 150 км, пространственное разрешение < 1 м
Оптические рефлектометры на принципе рассеяния Рамана	Комбинационное рассеяние	Мониторинг инженерных сооружений в режиме реального времени, распределенное измерение температуры	Распределенное зондирование	Диапазон зондирования – до 25 км, пространственное разрешение < 1,5 м
Оптические рефлектометры на принципе рассеяния Мандельштама-Бриллюэна	Рассеяние Мандельштама-Бриллюэна	Распределенный мониторинг температуры и деформации в режиме реального времени	Распределенное зондирование	Диапазон зондирования – до 150 км, пространственное разрешение < 1 м, погрешность измерения температуры < 0,5° С

На рисунке 1 представлены спектры сигналов, рассеянных по Рэлю, Манделъштаму-Бриллюэну и Раману. Центральная частота спектра рассеяния Манделъштама-Бриллюэна смещена приблизительно на 13 ГГц, а комбинационного рассеяния Рамана на 13 ТГц. В первом случае ширина спектра значительно уже значительно уже (~30 МГц по сравнению с ~6 ТГц). По этим причинам рассеяние Манделъштама-Бриллюэна является более привлекательным для распределенного зондирования по сравнению с комбинационным рассеянием Рамана[1].

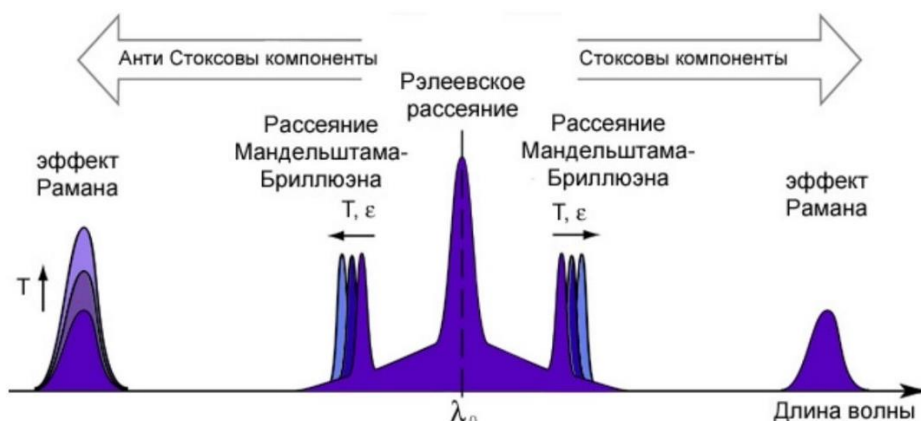


Рис. 1. Спектры сигналов обратного рассеяния

Сдвиг частоты и интенсивность спонтанного обратного рассеяния Манделъштама – Бриллюэна зависят от температуры и деформации и описываются матрицей  $2 \times 2$

$$\begin{bmatrix} \Delta \nu_B \\ \Delta I_B \end{bmatrix} = \begin{bmatrix} C_{\nu_B \epsilon} & C_{\nu_B T} \\ C_{I_B \epsilon} & C_{I_B T} \end{bmatrix}. \quad (1)$$

Используемые в матрице коэффициенты сдвига частоты  $C_{\nu_B \epsilon}$ ,  $C_{\nu_B T}$  и интенсивности  $C_{I_B \epsilon}$ ,  $C_{I_B T}$  из-за изменений деформации  $\Delta \epsilon$  и температуры  $\Delta T$  зависят от концентрации легирующих добавок и определяются экспериментально для конкретного типа оптического волокна и длины волны измерения.

По измеренным значениям сдвига частоты и интенсивности спектра обратного рассеяния становится возможным вычисление изменений деформации и температуры

$$\begin{bmatrix} \Delta \epsilon \\ \Delta T \end{bmatrix} = \frac{1}{|C_{\nu_B \epsilon} C_{I_B T} - C_{I_B \epsilon} C_{\nu_B T}|} \begin{bmatrix} C_{I_B T} & -C_{\nu_B T} \\ -C_{I_B \epsilon} & C_{\nu_B \epsilon} \end{bmatrix}. \quad (2)$$

### 3. Оптоволоконные сенсорные сети

Во многих случаях желательно или даже обязательно измерять деформацию и температуру в нескольких местах одновременно. Эти задачи решаются с помощью оптоволоконных сенсорных сетей, в которых используются принципы многоточечного или распределенного зондирования. В первом случае проводятся измерения параметров только вблизи локализованных датчиков. При этом необходимо объединение информационных сигналов от отдельных датчиков в единый поток. Это значительно сокращает капитальные затраты за счет уменьшения количества активных и пассивных компонентов. Метод мультиплексирования определяется архитектурой сенсорной сети и адресацией датчиков.

Мультиплексирование с временным разделением — один из самых популярных методов мультиплексирования, при котором измерения от каждого датчика получаются с учетом времени прохождения световых импульсов. Он применяется при мультиплексировании сигналов с интерферометрических датчиков и волоконных решеток Брэгга. При этом используются преимущества решеток Брэгга, которые имеют определенное положение по длине волокна. Метод мультиплексирования по длине волны обычно применяется при измерении температуры или деформации. Существуют также другие известные методы мультиплексирования, например, когерентный, пространственный и гибридный.

Для распределенного зондирования чаще всего используются сенсорные системы, основанные на рассеянии Бриллюэна и комбинационном рассеянии Рамана. Они нашли широкое применение для мониторинга направляющих сред оптических телекоммуникационных систем в качестве диагностического инструмента, а также крупных инженерных сооружений (плотины, дамбы, туннели, трубопроводы, мосты и др.).

В таблице 2 представлено сравнение многоточечного и распределенного зондирования с использованием волоконных решеток Брэгга и рефлектометров Мандельштама-Бриллюэна для измерения температуры и деформации, что представляет собой наиболее распространенное использование этих волоконно-оптических сенсорных систем.

Таблица 2. Сравнение многоточечного и распределенного зондирования

Метрологические характеристики	Волоконные решетки Брэгга	Рефлектометр Мандельштама-Бриллюэна
Пространственное разрешение	Зависит от расстояния между решетками Брэгга (можно настроить)	1 м (до 10 км); 5 м (до 60 км)
Одновременное зондирование	Для измерения температуры или деформации необходимо использовать отдельные датчики	Одновременно измеряет температуру и деформацию
Динамический диапазон	20 км (без усиления)	от 100 м до 200 км
Температурный диапазон, (°C)	до [-40, +250]	[-200, 700]
Разрешение, (°C)	0,1	0.1
Погрешность измерения, (°C)	от 0,1 до 1,0	0.1
Температурная повторяемость, (°C)	0,1	0,8
Диапазон деформации, (мкм ε)	до [-3000, 3000]	[-30 000, 40 000]
Разрешение, %	От 0,1 до 2,0	0.1
Погрешность, %	От 0,1 до 1,0	0.1
Повторяемость деформации (мкм ε)	0.1	0.1
Пространственное представление результатов измерения	Физические параметры, измеренные в нескольких дискретных точках	Физические параметры измеряются непрерывно по всей длине волокна.

Из таблицы следует, что волоконно-оптические датчики на принципе рассеяния Мандельштама-Бриллюэна обладают наилучшими метрологическими характеристиками и более широким спектром функциональных возможностей.

### Заключение

Из всего множества сосредоточенных и распределенных волоконно-оптических датчиков выделяются датчики на принципе рассеяния Мандельштама-Бриллюэна своей способностью производить измерения в широко динамическом диапазоне с высокой точностью и пространственной разрешающей способностью. Актуальными направлениями дальнейших исследований являются метрологическое обоснование технических требований к основным компонентам и разработки алгоритмов обработки спектрограмм, обеспечивающих расширение функциональных возможностей волоконно-оптических датчиков.

### СПИСОК ЛИТЕРАТУРЫ:

1. Горлов Н.И. Волоконно-оптические датчики в телекоммуникациях: учебное пособие / Н.И. Горлов, И.В. Богачков, А.А. Ступникова; Сибирский государственный университет телекоммуникаций и информатики. – Новосибирск, 2022. – 142 с.
2. Pendão C, Silva I. Optical Fiber Sensors and Sensing Networks: Overview of the Main Principles and Applications // Sensors, 2022, 22, 7554.

## ОБЗОР МЕТОДОВ И СПОСОБОВ ИЗМЕРЕНИЯ ЭЛЕКТРИЧЕСКИХ ХАРАКТЕРИСТИК ЖИДКИХ ДИЭЛЕКТРИКОВ

<sup>1</sup>Уральский технический институт связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия

<sup>2</sup>Уральский государственный аграрный университет, Россия

Ключевые слова: электрические параметры, диэлектрическая проницаемость, диэлектрики.

В статье представлен анализ зависимостей электрических свойств диэлектриков (диэлектрическая проницаемость и проводимость) от различных параметров; основные методы их измерения в различных частотных диапазонах.

S.Y. Krasnykh<sup>1</sup>, N.M. Barbin<sup>2</sup>, V.T. Kuanyshev<sup>1</sup>

## AN OVERVIEW OF WAY AND METHOD FOR MEASURING THE ELECTRICAL CHARACTERISTIC OF LIQUID DIELECTRICS

<sup>1</sup>Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics in Yekaterinburg (UrTISI SibGUTI), Russia

<sup>2</sup>Ural State Agrarian University, Russian

Keywords: electrical parameters, dielectric constant, dielectrics.

The article presents an analysis of the dependences of the electrical properties of dielectrics (permittivity and conductivity) from various parameters; the main methods of measuring them in different frequency ranges.

Для жидких диэлектриков характерным является диэлектрическая проницаемость, так как магнитные свойства мало отличаются от магнитных свойств вакуума. Удобно представлять диэлектрическую проницаемость в виде комплексной величины:  $\hat{\epsilon} = \epsilon' - i\epsilon''$ . Отношение мнимой и действительной частей комплексной диэлектрической проницаемости именуется углом диэлектрических потерь:  $tg \delta = \epsilon''/\epsilon'$ . Тангенс угла потерь связан с проводимостью (потерям) в диэлектрике

Данные электрические характеристики зависят: от вида и структуры вещества (строение молекул, видов связей между ними, агрегатного состояния, формы кристаллической решетки, наличия дефектов и неоднородностей в структуре включая наличия примесей); от физических характеристик (температура, давление, плотность); напряжения воздействия (частота, амплитуда, форма). Поэтому измерения электрических характеристик имеют широкое практическое применение при анализе вещества, например: контроль производства, определении концентрации солевых растворов, содержания солей в морской и проточной воде, оценки загрязненности сточных вод, определение следов воды в неводных растворителях, газах, твердых солях, целлюлозе, бумаге, зерне и т.п. [1,2]

Большинство видов промышленных измерителей комплексной диэлектрической проницаемости не выпускается в нашей стране, поэтому данная статья первый шаг к самостоятельной разработке и изготовлению приборов данного рода.

Выделяют следующие методы измерения пассивных электрических параметров:

- кондуктометрические;
- диэлькометрические;
- импедансометрические.





Мост представляют собой схему, содержащую несколько сопротивлений (чаще всего, четыре) одно из которых, измеряемое, его определяют сравнением с эталонным сопротивлением. Сопротивление необходимо подобрать так, чтобы ток в диагонали отсутствовал, в качестве нуля индикатора используют амперметр, вольтметр или гальванометр. В качестве переменного сопротивления (плечо сравнения) берут из магазина сопротивлений и устанавливают близкое к сопротивлению измеряемого объекта. Аналогично можно выполнить измерения электрической емкости, если в схеме заменить резисторы на конденсаторы, а измерения выполнять на переменном токе. Если измеряемый конденсатор содержит проводимость, тогда фаза тока в диагонали не будет совпадать и определить нуль станет невозможно, поэтому в измеряемое плечо, помимо магазина емкостей, параллельно включают магазин сопротивлений (если параллельная проводимость мала, то магазин сопротивлений включают последовательно).

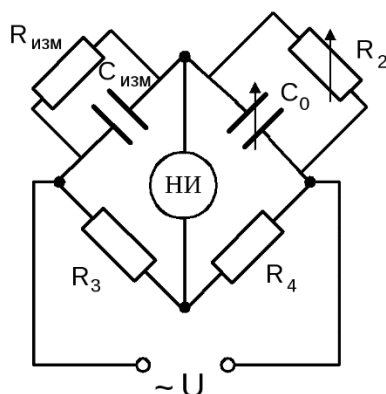


Рисунок 2 – Схема измерения мостом

В целях организации автоматического измерения, применяют небалансный метод измерения, то есть вывод о величине комплексного сопротивления в измеряемой ветви делается не только по значениям комплексного сопротивления/емкости в других ветвях, но и по силе и фазе потенциалов в диагонали схемы.

Данный метод является одним из основных способов измерений комплексной диэлектрической проницаемости, точность измерения, в общем случае, зависит только от допуска элементов в магазине сопротивлений и емкости. В частотной области данный метод применим до единиц МГц, так как наличие большого числа проводников, систем коммутации приводит к появлению значимых паразитных параметров, которые усугубляются с ростом частоты.

Отдельно можно отметить трансформаторные мосты (мосты с индуктивно связанными плечами), которые обладают высокой защитой от паразитных связей. Заявленные параметры измерения частоты от единиц герц до сотен МГц, активное сопротивление от 0.0001 Ом до 1 000 Ом с погрешностью 0.01-0.001 %, емкости от  $10^{-20}$  до  $10^{-2}$  Ф с погрешностью порядка 0.0001 %, индуктивность от  $10^{-8}$  до 100 Гн с погрешностью 0.01 %. [11]

Резонансные методы основываются на измерении характеристик резонансной кривой колебательного контура. Схема измерения представляет собой, чаще всего параллельную RLC цепь с известными параметрами (рисунок 4), параллельно контуру подключается измерительный конденсатор. Данный контур является нагрузкой генератора. В качестве измеряемой величины выбирается АЧХ контура по напряжению (току). При достаточно высокой добротности  $Q > 3$ , по полученной АЧХ можно определить частоту резонанса, добротность и полосу пропускания контура:

$$\omega_0 = \frac{1}{\sqrt{L_1 * (C_1 + C_2 + C_x)}}, Q = \frac{1}{G_0 + G_x} \sqrt{\frac{(C_1 + C_2 + C_x)}{L_1}}, \Pi_{0.707} = \frac{\omega_0}{Q} = \omega_B - \omega_H \quad (6)$$

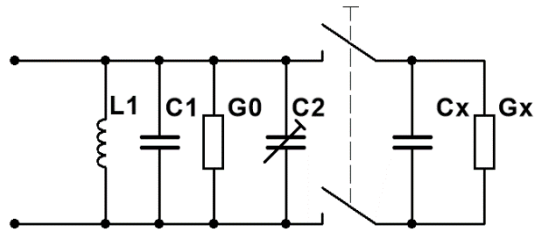


Рисунок 4 – Схема параллельного колебательного контура,  $C_x, G_x$  – измеряемые величины,  $L1, C1$  – известные индуктивность и емкость контура,  $C2$  – подстроечный конденсатор

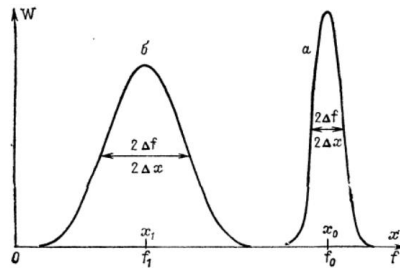


Рисунок 5 – Резонансная кривая, а – без измерительной ячейки (диэлектрика), б – с ней.

Соответственно, измерения выполняют до включения измеряемой ячейки и после. Иногда во время измерения схемы с включенной ячейкой выполняют компенсацию с помощью градуированного подстроечного конденсатора, до тех пор, пока характеристики контура не станут такими же как до включения ячейки, соответственно значения емкости определяют из разницы емкости подстроечного резистора до и после компенсации. Такая компенсация позволяет добиться большей стабильности работы схемы, так как измерения выполняются на одной частоте. [7]

Другой способ измерения характеристик колебательного контура, заключается в установке данной цепи в выходную цепь генератора, тогда выходная частота генератора будет равняться  $\omega_0$ , а измерения выполняют с помощью частотомера.

Еще один способ измерения заключается в использовании двух синхронизированных генераторов, нагруженных на одну нагрузку. Выходные колебательные контура таких генераторов одинаковы, измерительную ячейку подключают к одному из контуров, в результате сложения двух колебаний наблюдаются биения. Частота следований биений определяется разностью между частотами генераторов (метод биений).

В [12] приводятся схемы организации резонансных измерений. Метод отличается высокой помехоустойчивостью (благодаря избирательным свойствам контура), Высокой чувствительностью: измерение характеристик контура по чувствительности примерно равно мостовому методу, для фазогенераторных схем примерно в 100-200 раз выше. По частотной области – довольно сложно организовать измерения на низкой частоте, вследствие требования больших емкостей и индуктивностей, с другой стороны, отсутствует верхняя граница по частоте. При повышении частоты больше 100-300 МГц, измерительная ячейка и колебательный контур изготавливается на элементах с распределенными параметрами (например, на коаксиальных [13], полосковых (микростриповых) линиях), то есть в СВЧ диапазоне и выше, данный метод становится методом объемного резонатора. Резонатор представляет собой колебательный контур, чьи характеристики зависят от его геометрических размеров и диэлектрической проницаемости диэлектрика, резонатор можно выполнить на волноводной линии, коаксиальной линии или полосковой линии [14].

$$\frac{\varepsilon - 1}{2} = \frac{f_0 - f_1}{f_0}, \quad \operatorname{tg} \delta = \frac{1}{Q_1} - \frac{1}{Q_0}, \quad (8)$$

Метод измерения комплексного тока и напряжения (в иностранной литературе встречается название метод I-V), смысл его в определении амплитуды и фазы входного тока и напряжения на

исследуемой ячейке. Тогда, комплексное сопротивление можно определить, как  $Z = \dot{U}/\dot{I}$ , по формуле (2) определить активную и реактивную составляющую. Частотные характеристики метода до порядка 3 ГГц.

Метод стоячих волн заключается в измерениях распределения напряжения в длинной линии, окруженной (заполненной) измеряемым диэлектриком, в режиме стоячих волн. Для создания режима стоячих волн необходимо замкнуть накоротко один из концов линии (реже создают режим холостого хода), при этом к другому концу подключить генератор. Далее с помощью диодного детектора и вольтметра строится зависимость распределения напряжения от расстояния от нагрузки. В качестве измерительного прибора используется вольтметр с диодным детектором. Для измерения лучше всего подходит коаксиальная или волноводная измерительная линия. По частоте метод применим до, примерно 10 ГГц, далее длина волны становится слишком маленькой для измерения.

Методы отражения заключается в измерении характеристик измеряемого объекта (измерительной ячейки, резонансной системы и т.п.) основываясь на коэффициенте отражения (прохождения) от него в линии или свободном пространстве. Выполнять измерения можно с помощью векторного анализатора цепей, либо с помощью двух антенн в свободном пространстве.

Калориметрический метод заключается в измерении тангенса угла потерь по степени нагрева материала.

#### Заключение

Для исследования электрических свойств диэлектрических материалов было разработано большое количество способов, все они обладают разной точностью измерения, применимы в разном частотном диапазоне и обладают разными достоинствами и недостатками. С практической точки используются следующие методы: мостовой (до порядка 1 МГц), резонансные методы (до 300 МГц, резонансный волновод от 300 МГц), метод измерения тока напряжения (до 3 ГГц), метод отражения (от 1 ГГц).

#### Список источников:

1. Б.М. Тареев. Физика диэлектрических материалов. Москва, Энергоиздат, 1982 г., 320 с.
2. Борисова М.Э., Койков С.Н. Физика диэлектрических материалов, учебное пособие, Ленинград, 1979 г. 240 с.
3. В.С. Андреев, Е.П. Попичителей. Лабораторные приборы для исследования жидких сред, Ленинград, Машиностроение, 1981 г. 312 с.
4. Андреев В.С. Кондуктометрические методы и приборы в биологии и медицине. "Медицина", Москва, 1973 г., 335 с. стр 90-93, 105
5. Худякова Т.А., Крешков А.П. Кондуктометрический метод анализа. Учебное пособие для вузов, Москва "Высшая школа" 1975 г., 207 стр. стр 8, 114-118, 127-133
6. Надь Ш.Б. Диэлектрометрия. Перевод с венгерского В.Д. Калашников, под редакцией В.В. Малова, Москва, Энергия, 1976 г. стр 11-15, 21-28, 53-58, 66-70
7. Ч. Ф. Смайс. Диэлектрическая постоянная и структура молекул. Перевод с английского В.Г. Васильева, Я.Г. Сыркина, ОНТИ, главная редакция химической, Москва, 1937 г. стр 44-76
8. Диэлектрические измерения для количественного анализа и для определения химической структуры. Эме Ф. перевод с немецкого Штиллер Б.Н. под редакцией Заславского И.И. Издательство "Химия", Москва 1967 г. 223 с.
9. К.Б. Карандеев. Специальные методы электрических измерений. Государственное энергетическое издание Москва–Ленинград, 1963 г. 344 с.
10. К.Б. Карандеев. Методы электрических измерений (дифференциальные, мостовые и компенсационные). Государственное энергетическое издательство, Москва, Ленинград, 1952 г. 335 с.
11. Трансформаторные измерительные мосты. Под общей редакцией К.Б. Карандеев, издательство Энергия, Москва 1970 г. 280 с.
12. Полулях К.С. Резонансные методы измерений. Москва, Энергия, 1980 г. 120 с.

13. В.В. Рудаков, А.А. Коробко. Высокочувствительный СВЧ измеритель влагосодержания в неполярных диэлектрических жидкостях на основе ступенчатого неоднородного коаксиального резонатора. *Электротехніка і Електромеханіка*. 2016. №5.
14. Семенов Н.А. *Техническая электродинамика*. Учебное пособие для вузов, Москва, "Связь", 1973 г. 480 с. Стр. 255-259.

## АНАЛИЗ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ АППАРАТНО-ПРОГРАММНОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ С ОБРАБОТКОЙ РЕАЛЬНОГО ТРАФИКА

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

Ключевые слова: коммутатор, точка доступа, протокол, беспроводная сеть, кабель, сервер, виртуальная сеть.

В статье представлена структурная схема виртуальной системы передачи данных с обработкой реального трафика. Проведен анализ экономической эффективности внедрения аппаратно-программной системы передачи данных с обработкой реального трафика.

E.S. Tarasov, N.V. Budyldina, A.S. Nikitin

## ANALYSIS OF THE ECONOMIC EFFICIENCY OF IMPLEMENTING A HARDWARE-SOFTWARE DATA TRANSMISSION SYSTEM WITH REAL TRAFFIC PROCESSING

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

Keywords: switch, access point, protocol, wireless network, cable, server, virtual network.

The article presents a block diagram of a virtual data transmission system with processing of real traffic. An analysis of the economic efficiency of introducing hardware and software system data transmission with processing of real traffic was carried out.

### Введение

Нынешняя ситуация в мире показывает на необходимость пересмотреть применение различного иностранного оборудования практически во всех областях деятельности государства РФ, одной из которых являются сети передачи данных. На данный момент многие современные сети связи РФ в основном построены с использованием не отечественного оборудования, а их вендоры ушли с рынка России – в итоге нет возможности покупать их оборудование и ПО, а также поддерживать уже существующие сети, поэтому стоит важная задача о его замене.

На сегодняшний день уже имеются отечественные компании по поставке телекоммуникационного оборудования, такие как: Вектор, F+, Eltex, Аквариус, Qtech и Nateks. Однако данные производители делают аппаратную продукцию, некоторые комплектующие до сих пор необходимо закупать у стран-союзников. Такая ситуация порой очень сильно влияет на стоимость при построении сетей передачи данных. Также, в будущем, обслуживание сетей передачи данных также является крайне затратным, ввиду закупки нового сетевого оборудования, ПО и конечно кабеля.

Чтобы уменьшить затраты на создание и обслуживание корпоративных сетей передачи данных в УрТИСИ СибГУТИ было решено провести исследование, целью которого является реализация такой возможности. Чтобы решить проблему большого количества аппаратной составляющей, можно использовать беспроводные сети вместо кабеля, а виртуализация системы заменит аппаратные устройства. Для этого разработана аппаратно-программная система передачи данных с обработкой реального трафика. В статье рассматривается два варианта

использования виртуальных сетей с обработкой реального трафика. Целью исследования является сравнительный анализ затрат, связанных с созданием и обслуживанием проводной сети передачи данных и аналогичной аппаратно-программной.

## 1 Структурная схема сети связи

Чтобы уменьшить затраты на создание и обслуживания сетей в компаниях и предприятиях, следует пользоваться беспроводными сетями. Самым главным плюсом будет снижение использования кабеля в таких сетях передачи данных. 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, причем не в одном экземпляре, а в нескольких, где они объединяются в виртуальную сеть[4].

На рисунке 1 показана структурная схема созданной системы связи.

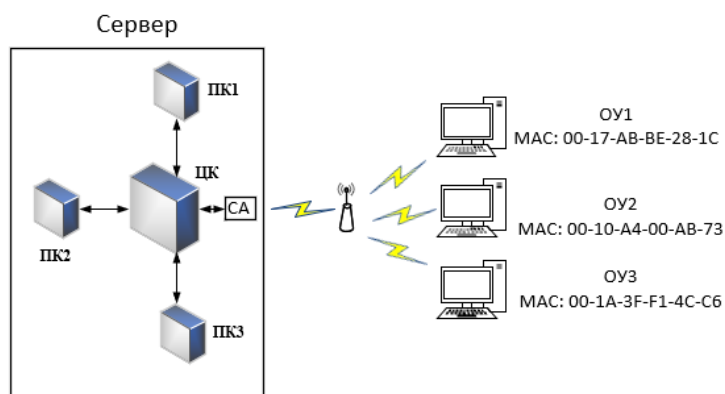


Рисунок 1 – Структурная схема системы связи

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 сет 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 будет поступать 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 коммутатор в его физический порт при помощи кабеля UTP.

Однако в созданной системе все ОУ подключаются через одну точку доступа к виртуальной сети для того, чтобы использовать сервисы VLAN, STP и т.д. необходимо подключать ОУ к отдельным портам. Поэтому для этого следует на ПК создать логические порты, к которым логически будут подключаться рабочие станции или другие ОУ[5].

Ранее для виртуальной сети был разработан протокол WVNIP, принцип работы которого заключался в добавлении в кадр Ethernet специального поля «Идентификатор логической связи» на рабочей станции, после чего кадр передавался по беспроводной связи на виртуальную сеть.

Данный протокол работоспособен, однако имеет свои недостатки[6]. Самым главным недостатком являлось то, что, изменяя кадр Ethernet, менялся сам стандарт. Также так как в кадре появлялось новое поле означало, что кадр будет более громоздким, что скажется на пропускной способности при передаче данных. В связи с этим было решено разработать альтернативный ему протокол SNSP. При его работе, по беспроводной сети передается обычный стандартный кадр. Но при этом, требуется ручная регистрация оконечных устройств на коммутаторах, что значительно усложняет процедуру настройки и администрирования сети.

В связи с этим, был разработан протокол динамической коммутации в виртуальной сети (DSPVN), который полностью автоматизирует процесс регистрации оконечных устройств на программных коммутаторах и позволяет коммутировать реальный трафик, поступающий из беспроводной сети.

Ввиду того, что прием данных будет вестись через сетевой адаптер, это может сильно сказаться на пропускной способности. В связи с этим структурную схему было решено модернизировать, чтобы повысить количество передаваемого трафика путем добавления в сеть простого коммутатора уровня L2 с портами хотя бы 1Гбит/с, к которому по кабелю будет подключаться точка доступа и сетевая карта сервера. Кроме того, сервер и коммутатор будут располагаться в одном сетевом шкафу, что позволит минимизировать затраты на кабель и монтаж. Пример структурной схемы представлен на рисунке 2.

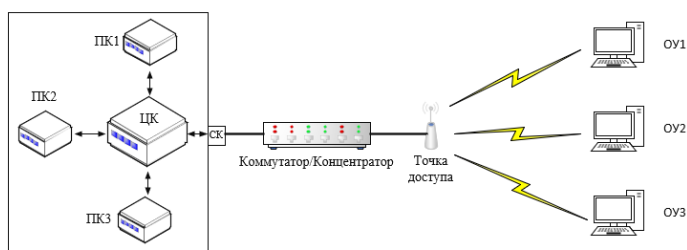


Рисунок 2 – Модернизированная структурная схема системы связи

### 3 Затраты на организацию и обслуживание проводной сети передачи данных.

При расчете проводной сети передачи данных основным расходным материалом будет являться кабель. На рисунке 3 представлен пример создания небольшой проводной локальной сети передачи данных.

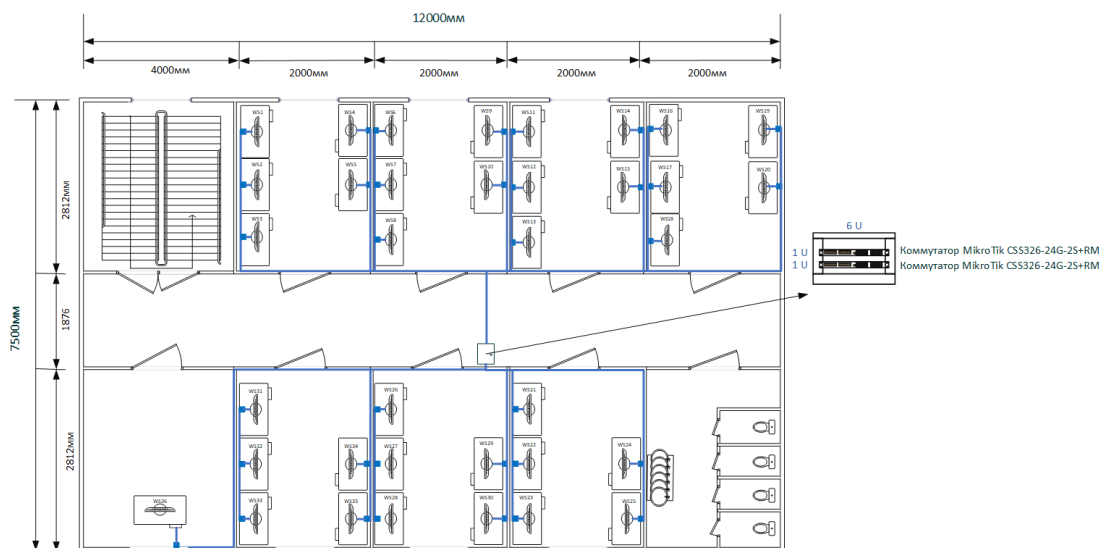


Рисунок 3 – Схема проводной сети передачи данных

В офисе площадью 120x75м установлено 36 компьютеров. В качестве сетевого оборудования были использованы коммутаторы CSS326-24G-2S+RM от Mikrotik. Каждый такой коммутатор управляемый, 2 уровня на базе SwOS имеет 24 гигабитных Ethernet-порта, 2 порта





Выполнив расчет, получится, что дальность покрытия точки доступа составит порядка 70м, что обеспечит связью весь офис.

Стоимость данной сети будет составлять около 100 тысяч рублей, куда входит сервер стоимостью 67 тысяч рублей, точки доступа, стоимостью 20 тысяч рублей и коммутатор, стоимостью 30 тысяч рублей. Однако сама установка оборудования, монтаж выйдет на порядок дешевле по сравнению с проводной локальной сетью и составит порядка 150 тысяч суммарно за всё. Кроме всего, в случае расширения сети не будет требоваться дорогостоящий ремонт, что позволит очень сильно сэкономить на обслуживании.

### **Заключение**

Разработанная аппаратно-программная система связи позволит небольшим компаниям значительно уровень снизить уровень затрат, при организации и обслуживании сетей передачи данных, а также упростить их эксплуатацию, так как станет меньше применяемых аппаратных средств. Разрабатываемые протоколы WVNIP, SNSP, DSPVN дадут возможность осуществить взаимодействие беспроводной сети с виртуальной, что является одним из основных условий работоспособности разрабатываемой системы. Изначальные затраты на создание проводной и виртуальной системы примерно равны, однако в случае расширения сетей передачи данных выиграет беспроводная сеть за счет минимального использования аппаратных составляющих, практически отсутствия использования кабеля, а также ремонта, который программная часть системы не требует.

### **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](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 виртуального 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.
5. Патент № 2814522. Программно-аппаратная система передачи данных с обработкой реального трафика : № 2023101916 : заявл. 27.01.2023 : опубл. 29.02.2024 / Е. С. Тарасов ; заявитель, патентобладатель – 2 с.
6. Тарасов Е. С., Будылдина Н. В., Никитин А. С., Фастов Д. А. Разработка протокола коммутации реального трафика в виртуальных сетях // Информационные технологии и когнитивная электросвязь. Сборник научных трудов IX Всероссийской научно-практической конференции. 2023 г., г. Екатеринбург, с. 152-156.

## **ОПРЕДЕЛЕНИЕ ЭПЮР СИГНАЛОВ СОВМЕЩЕННОГО КАНАЛА ПИТАНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ**

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

Ключевые слова: канал, распределенные параметры, питание, информация, передача, сигнал, эпюра, метрологические характеристики, эксплуатационные качества.

В статье определены эпюры сигналов совмещенного канала связи и передачи информации. Выполненная работа позволяет определить метрологические характеристики и некоторые другие параметры совмещенных каналов питания и передачи информации, а также выявить часть необходимых конструктивных особенностей таких каналов. Полученные результаты могут быть использованы для обоснования сферы использования совмещенных каналов, упростить устройства передачи информации и увеличить скорость ее передачи

**O.D. Lobunets**

## **DEFINITION OF COMBINED CHANNEL SIGNAL PLOTS POWER SUPPLY AND INFORMATION TRANSMISSION**

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

Keywords: channel, distributed parameters, power supply, information, transmission, signal, plot, metrological characteristics, operational qualities.

The article defines the signal plots of the combined communication channel and information transmission. The work performed makes it possible to determine the metrological characteristics and some other parameters of combined power and information transmission channels, as well as to identify some of the necessary design features of such channels. The results obtained can be used to justify the scope of use of combined channels, simplify information transmission devices and increase the speed of its transmission.

Совмещение каналов питания и передачи информации позволяет в ряде случаев значительно упростить схемные решения соответствующих технических средств и обеспечить получение и направление информационных сообщений в условиях опасной окружающей среды, например, во взрывоопасной атмосфере. При этом в пунктах получения информации могут отсутствовать какие-либо стационарные источники питания, а параметры, как совмещенного канала связи, так и его сигналов выбраны с учетом обеспечения свойств искробезопасности данного устройства.

Физически совмещенный канал питания и передачи информации при обеспечении условий искробезопасности может быть реализован на основе незащищенного от физических воздействий телефонного кабеля длиной до нескольких километров. Применение каналов связи с названными техническими характеристиками необходимо на предприятиях химической промышленности, а также в угольных и других добывающих природных ресурсы объектах [1].

Телефонный кабель при его использовании в качестве совмещенного канала связи и передачи информации может быть представлен в виде линии с распределенными параметрами, продольными активным сопротивлением  $R_0$  и индуктивностью  $L_0$  и поперечными проводимостью  $G_0$  и емкостью  $C_0$ . При этом в справочной литературе данные распределенные параметры обычно указываются в расчете на один километр.

Уравнения, описывающие процессы изменения сигналов в линиях с распределенными параметрами во временной области [2] получили название уравнений телеграфиста:

$$\frac{\partial}{\partial x} u(x, t) = -L \frac{\partial}{\partial t} i(x, t) - R i(x, t);$$

$$\frac{\partial}{\partial x} i(x, t) = -C \frac{\partial}{\partial t} u(x, t) - G u(x, t).$$

Когда элементы потерь  $R$  и  $G$  являются достаточно существенными для того, что их не учитывать, для облегчения их решения эти уравнения часто дифференцируют и после некоторых преобразований получают два уравнения, каждое из которых имеет только одно неизвестное

$$\frac{\partial^2}{\partial x^2} u = LC \frac{\partial^2}{\partial t^2} u + (RC + GL) \frac{\partial}{\partial t} u + GRu;$$

$$\frac{\partial^2}{\partial x^2} i = LC \frac{\partial^2}{\partial t^2} i + (RC + GL) \frac{\partial}{\partial t} i + GRi.$$

Последние уравнения могут быть решены с помощью, например, приложения Maple.

Еще одним способом получения эюр сигналов в каналах передачи информации является компьютерное моделирование процессов в этих каналах.

В качестве примера ниже рассмотрен канал связи, который выполнен из телефонного кабеля длиной три километра. Распределенные параметры использованного для моделирования канала передачи информации телефонного кабеля имеют следующие значения:  $R_0 = 50$  Ом/км,  $G_0 = 0,072$  мкС/км,  $L_0 = 612$  мкГ/км,  $C_0 = 52$  нФ/км. Схема модели совмещенного канала питания и передачи информации изображена на рис. 1.

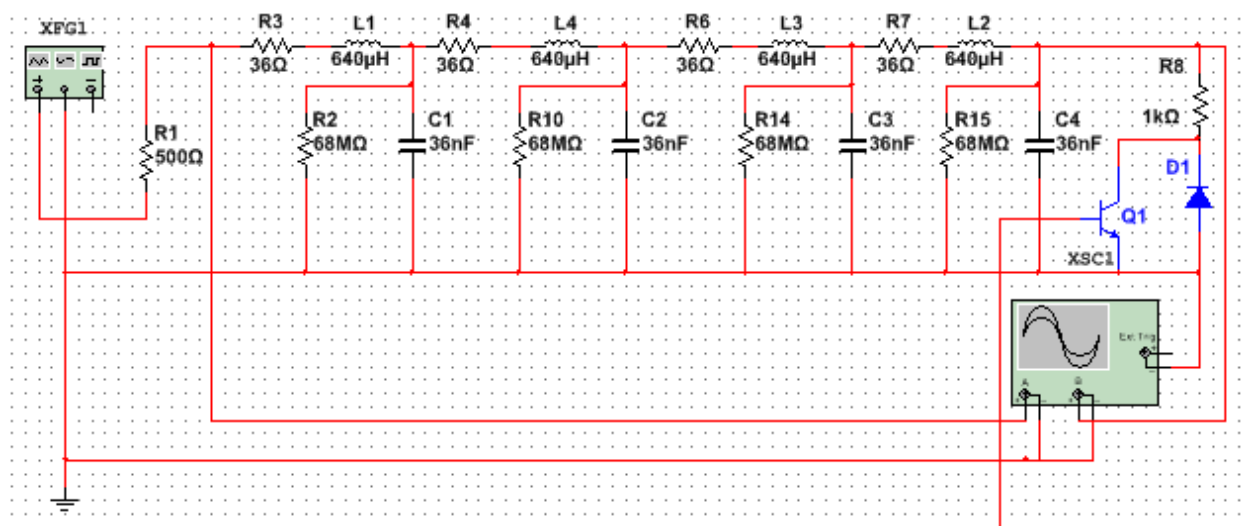


Рис.1. Схема модели совмещенного канала питания и передачи информации

Схема модели совмещенного канала питания и передачи информации состоит из источника напряжения питания прямоугольной формы, выход которого соединен с одним из выводов балластного резистора  $R_1$ , другой вывод которого присоединен к входу модели собственно канала связи. Модель канала связи содержит продольные резистивные и индуктивные элементы, а также поперечные резистивные и емкостные элементы, реализованные на соответствующих элементах семы. Выходные выводы канала связи присоединены к нагрузке, которой является собственно устройство контролируемого пункта, представленного в данной модели

совмещенного канала питания и передачи информации резистором R8. Устройство коммутации нагрузки линии связи реализовано с использованием транзистора Q1 и диода D1. Для непосредственного определения эпюр использован осциллограф.

При изменениях контролируемой величины происходит сдвиг фазы несущего информацию об измеряемой величине импульса. На стороне приема информации она восстанавливается с помощью дискриминатора амплитуды, реализованного с помощью порогового устройства.

Осциллограмма полученной эпюры напряжения в конце линии связи приведена на рис.2.

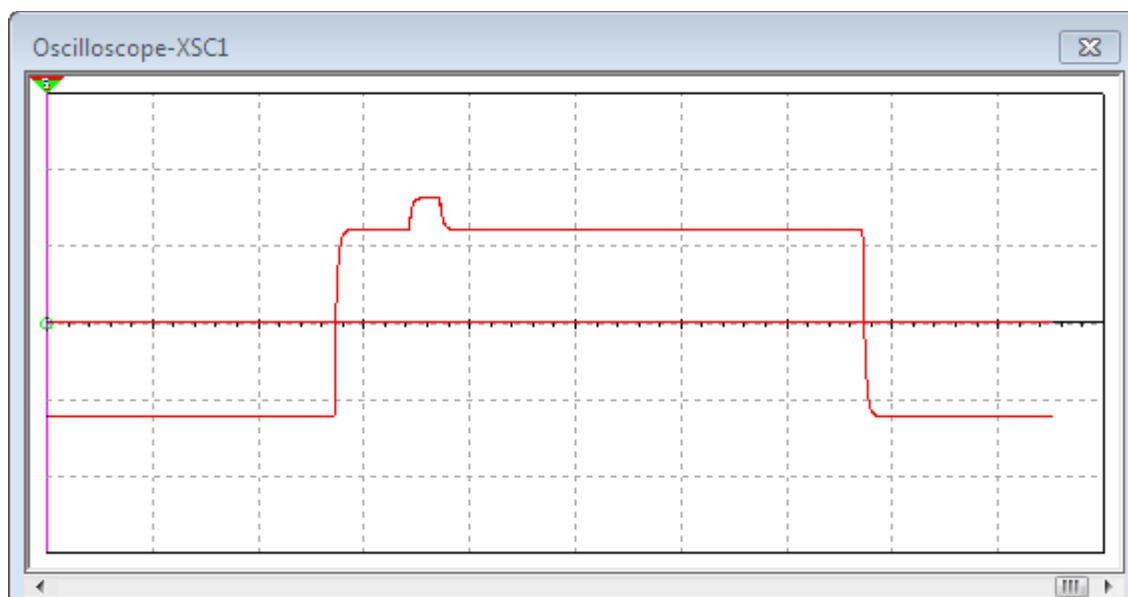


Рис. 2. Осциллограмма эпюры напряжения в конце линии связи

Аналогичная осциллограмма эпюры напряжения, действующего в начале линии связи, изображена на рис. 3.

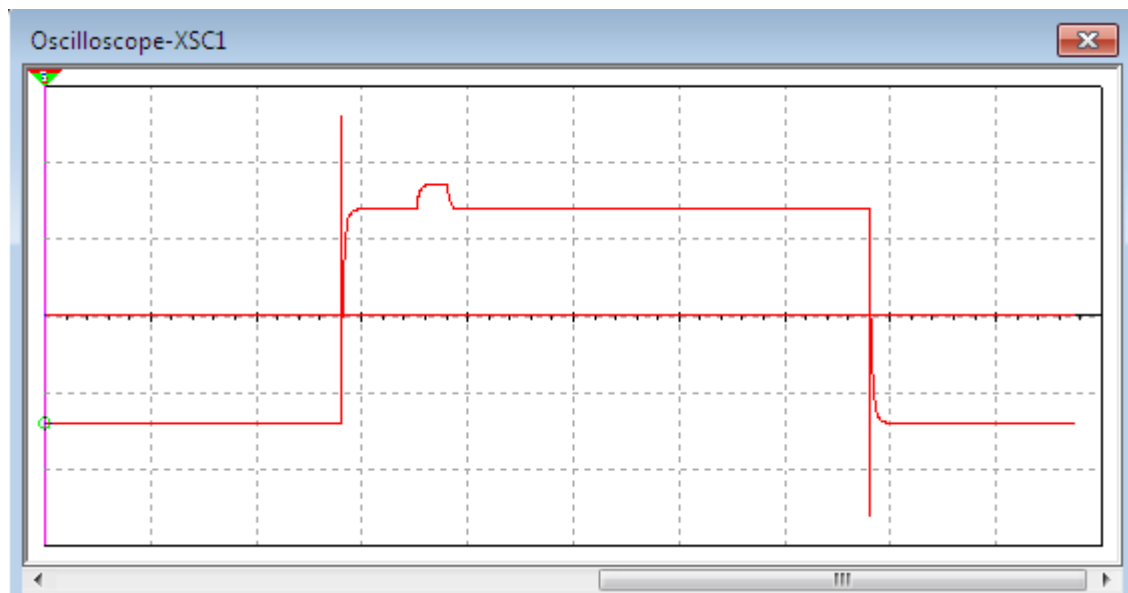


Рис. 3. Осциллограмма эпюры напряжения в начале линии связи

Полученные эпюры сигналов совмещенного канала питания и передачи информации позволяют сделать вывод о сфере использования описанного выше способа передачи данных, а также дают возможность определить метрологические характеристики подобного рода устройств. Сфера применения совмещенных каналов связи и передачи информации ограничена уменьшением полезной мощности из-за влияния элементов каналов на величину потерь. Поэтому длина совмещенных каналов ограничена. Кроме того, уменьшение крутизны информационных

импульсов отрицательно влияет на метрологические характеристики устройства в целом, а также увеличивает требования к точности пороговых элементов, используемых в качестве детекторов информационных импульсов.

Таким образом, выполненная работа позволила восполнить недостающую информацию для расширенного использования положительных свойств данного типа устройств передачи информации.

#### СПИСОК ЛИТЕРАТУРЫ:

1. А. с. 1471208 СССР, МКИ<sup>4</sup> С 08 С 19/16. Устройство контролируемого пункта телеизмерительной системы. / О. Д. Лобунец (СССР). – 4 с.: ил.
2. Бессонов Л. А. Теоретические основы электротехники: в 3-х ч. М.: Высшая школа, 1964. 751 с.
3. Крук Б. И. Телекоммуникационные системы и сети. Уч. пособие в 3-х томах / Б. И. Крук. – М.: ГЛТ, 2012.
4. Загидуллин Р. Ш. Multisim, LabVIEW и Signal Express. Практика автоматизированного проектирования электронных устройств: справочное издание. / Р. Ш. Загидуллин. М.: Горячая линия Телеком, 2009. 366 с.

## РАЗРАБОТКА ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ПРОГНОЗИРОВАНИЯ ЭНЕРГОПОТРЕБЛЕНИЯ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ

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

Ключевые слова: интернет вещей, нейронная сеть, прогнозирование, энергопотребление

В статье представлена схема организации сети «Умного дома» по беспроводной сети Fi-Wi. Описано моделирование рекуррентной нейронной сети. Приведены результаты прогнозирования, выполнен анализ прогнозируемого энергопотребления с практическими значениями. Приведены графики зависимости прогнозируемых данных нейронной сети с практическими.

E.V. Yurchenko, A.E. Kamenskov

## DEVELOPMENT OF AN ARTIFICIAL NEURAL NETWORK TO PREDICT THE ENERGY CONSUMPTION OF THE INTERNET OF THINGS NETWORK

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

Keywords: Internet of things, neural network, forecasting, energy consumption

The article presents a scheme for organizing a Smart Home network over a wireless Fi-Wi network. Modeling of a recurrent neural network is described. The results of forecasting are presented, the analysis of the projected energy consumption with practical values is performed. Graphs of the dependence of the predicted neural network data on practical ones are presented.

Современные технологии позволяют организовать цифровые сети в домашних условиях, что позволяет автоматизировать работу умных устройств. Для организации такой сети выбирают практически не совместимые между собой беспроводные стандарты умного дома. К таким стандартам можно отнести общеизвестные Wi-Fi [1] и Bluetooth, а также специализированные протоколы — Z-Wave, ZigBee и Thread. Каждый из протоколов решает определенные проблемы в сфере домашней и производственной автоматизации, обладает разной степенью защиты, предусматривает различную скорость передачи данных и соответствует различным стандартам энергопотребления.

Рассмотрим сеть умного дома, данные которой будут использоваться для прогнозирования в искусственной нейронной сети. Сеть включает в себя:

- датчики – передают информацию о состоянии контролируемого параметра на панель управления. Данные датчики подключается по протоколу Wi-Fi версии 4, 802.11n. В качестве микроконтроллера, используется AminaNodeMCUV3[3];

- шлюз – телефон марки Asus ZB602KL, который работает по протоколу Wi-Fi 4 802.11n. Шлюз предназначен для взаимодействия всей сети;

- устройства управления (далее IoT сервер) – может быть центральный блок или элемент управления децентрализованной сети. Они синхронизируют работу IoT оборудования, управляют им и обеспечивают взаимодействие интеллектуального комплекса с пользователем. В качестве IoT сервера был выбран RaspberryPi 4 ModelB 4 Gb, он включает в себя две программы. Первая из которых Blynk, отвечающая за аутентификацию датчиков и сбор данных. Вторая программа NodeRed, обрабатывает собранные данные с Blynk и отправляет эти данные на облако;

- облако – предназначено для сбора и вывода данных, в качестве облака используется Яндекс (Yandex Smart Home). Данное облако, предназначено для отображения данных с датчиков для пользователя.

Сеть умного дома показанная на рисунке 1.



Рисунок 1 – Имитационная сеть «Умного дома»

При выполнении измерений для каждого датчика было установлено свое время опроса. Данные снимались в течении четырех часов, при этом, контрольные точки были каждый час. Во время контрольных точек, снимались показания отправленного трафика и энергопотребление шлюза.

Данные, полученные во время эксперимента, были использованы в моделировании искусственной нейронной сети (ИНС). Задача ИНС является прогнозирование параметров энергопотребления датчиков по объему переданного трафика. В качестве ИНС была выбрана рекуррентная нейронная сеть с использованием LSTM (Long short-term memory) [4]. Данная нейронная сеть (НС) качественно справляется с прогнозированием параметров при последовательном и непрерывном потоке данных, так как каждый нейрон в данной НС имеет обратную связь, что позволяет сохранять параметры, информацию и выполнять прогнозирование на основе сохраненной информации. Схема ИНС показана на рисунке 2.

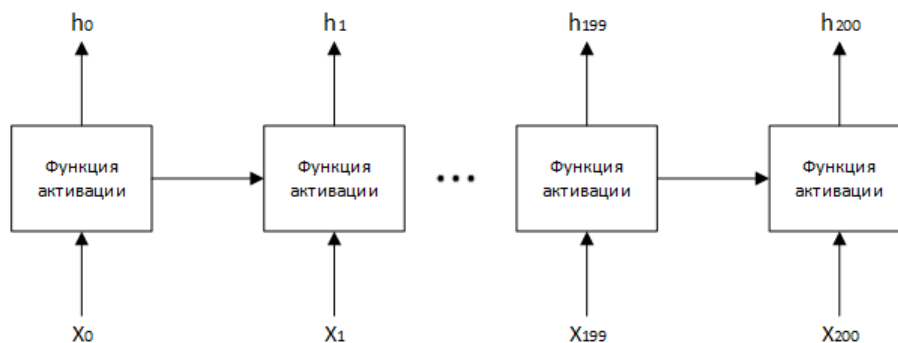


Рисунок 2 - Схема искусственной нейронной сети

Как показано на рисунке 2, в данной ИНС используются 200 нейронов LSTM. С  $X_0$  по  $X_{200}$  это входные исходные данные. В качестве исходных данных был использован трафик от четырех датчиков. С  $h_0$  по  $h_{200}$  выходные спрогнозированные данные. В качестве выходных данных было использовано энергопотребление от четырех датчиков. В функции активации находится сохраненная информация в период обучения ИНС.

На рисунке 3 показан набор данных, в котором находятся 104 выборки, где  $t_{\text{traf}}$  – объем трафика,  $I$  – затрачиваемое энергопотребление. Из них 100 были выбраны для обучения ИНС, оставшиеся 4 выборки были использованы в тестировании ИНС.

	t_traf	I
0	47690	86
1	51266	136
2	55677	196
3	55918	92
4	343513	116
...	...	...
99	1258585	629
100	1152014	603
101	1269673	648
102	318985	541
103	1407509	604

104 rows x 2 columns

Рисунок 3 – Набор данных для прогнозирования энергопотребления по объему трафика

В ИНС имеются три основных параметра для ее моделирования (рисунок 4):

- windows – количество окон, в которых будут записываться прогнозируемые параметры (в данном случае энергопотребление);
- input – количество входных значений;
- output – количество выходных значений.

```
n_windows = 100
n_input = 1
n_output = 1
```

Рисунок 4 – Параметры рекуррентной нейронной сети

Для запоминания информации, их паттернов и для дальнейшего прогнозирования было выполнено разделение набора данных на отдельные партии, что приводит к наилучшему результату (рисунок 6).

```
x_data = train[:size_train-4] #: Select all the training instance minus 4 I
X_batches = x_data.reshape(-4, n_windows, n_input) #: create the right shape for the batch e.g (1, 100, 1)
def create_batches(df, windows, input, output):
    ## Create X
    x_data = train[:size_train-4] # Select the data
    X_batches = x_data.reshape(-4, n_windows, n_input) # Reshape the data
    ## Create y
    y_data = train[n_output+3:size_train]
    y_batches = y_data.reshape(-4, n_windows, n_output)
    return X_batches, y_batches
```

Рисунок 6 – Разделение исходных данным на партии [5]

На рисунке 7 представлено моделирование ИНС. Так как исходные данные имеют большой диапазон значений, что плохо влияет на обучение ИНС, практическим методом была выбрана функция для определения ошибок MSE (среднеквадратичная ошибка), которая позволяет обучать ИНС с высокой точностью при большом диапазоне исходных данных.

На рисунке 8 показано обучение ИНС.



```

tf.compat.v1.reset_default_graph()
r_neuron = 200

## 1. Construct the tensors
X = tf.compat.v1.placeholder(tf.float32, [None, n_windows, n_input])
y = tf.compat.v1.placeholder(tf.float32, [None, n_windows, n_output])

## 2. create the model
basic_cell = tf.compat.v1.nn.rnn_cell.BasicRNNCell(num_units=r_neuron, activation=tf.nn.relu)
rnn_output, states = tf.compat.v1.nn.dynamic_rnn(basic_cell, X, dtype=tf.float32)

stacked_rnn_output = tf.reshape(rnn_output, [-1, r_neuron])
stacked_outputs = tf.compat.v1.layers.dense(stacked_rnn_output, n_output)
outputs = tf.reshape(stacked_outputs, [-1, n_windows, n_output])

## 3. Loss + optimization
learning_rate = 0.001

loss = tf.reduce_sum(tf.square(outputs - y))
optimizer = tf.compat.v1.train.AdamOptimizer(learning_rate=learning_rate)
training_op = optimizer.minimize(loss)

init = tf.compat.v1.global_variables_initializer()

```

Рисунок 7 – Модель нейронной сети

```

iteration = 1000

with tf.compat.v1.Session() as sess:
    init.run()
    for iters in range(iteration):
        sess.run(training_op, feed_dict={X: X_batches, y: y_batches})
        if iters % 100 == 0:
            mse = loss.eval(feed_dict={X: X_batches, y: y_batches})
            print(iters, "\tmSE:", mse)

y_pred = sess.run(outputs, feed_dict={X: X_test})
print(iters, "\tmSE:", mse)

```

Рисунок 8 – Обучение нейронной сети [5]

В результате обучения ИНС обучилась с ошибкой MSE равной 378.7 (рисунок 9), что является хорошим результатом при большом разбросе данных.

0	MSE: 13127211.0
100	MSE: 610436.6
200	MSE: 251996.81
300	MSE: 27165.55
400	MSE: 9585.445
500	MSE: 41810.66
600	MSE: 2732.399
700	MSE: 1046.962
800	MSE: 504.98056
900	MSE: 378.7118
999	MSE: 378.7118

Рисунок 9 – Результат обучения с функцией ошибки MSE

На рисунке 10 показан график исходных данных, действительных значений и спрогнозированных данных.

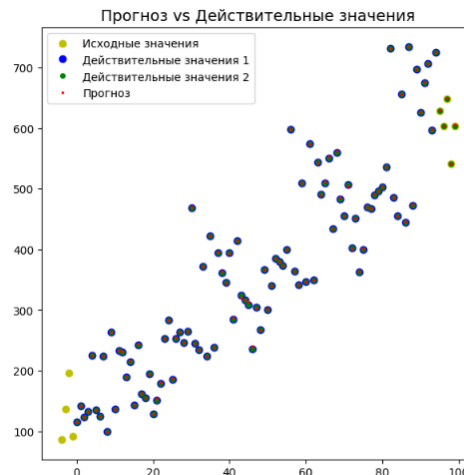


Рисунок 10 – Вывод графика

Из графика на рисунке 10 видно, что прогнозируемые значения находятся близко к действительным значениям и показывают высокую точность, малую погрешность работы ИНС с использованием LSTM.

На рисунке 11 видно, что расхождение исходных данных и прогнозируемых значениях не превышает 1,65, что является хорошим показателем точности.

Исходные значения из таблицы 101: Трафик 1152014 Энергопотребление исх. 603 Энергопотребление прог. 603.32935  
Исходные значения из таблицы 102: Трафик 1269673 Энергопотребление исх. 648 Энергопотребление прог. 649.58575  
Исходные значения из таблицы 103: Трафик 318985 Энергопотребление исх. 541 Энергопотребление прог. 541.61945  
Исходные значения из таблицы 104: Трафик 1407509 Энергопотребление исх. 604 Энергопотребление прог. 605.65283

Рисунок 11 – Оценка результата

Таким образом, разработанная искусственная нейронная сеть полностью выполняет свою задачу по прогнозированию энергопотребления сети интернета вещей. В точности выполнения прогнозирования можно убедиться, проанализировав среднеквадратичную ошибку, которая составила 378.7, что является хорошим результатом при большом разбросе данных, а также по значениям расхождения исходных и прогнозируемых данных. Следовательно, при разработке сетей интернета вещей без постоянного источника энергоснабжения, данная искусственная нейронная сеть может помочь в расчете затрат энергопотребления сети.

#### СПИСОК ЛИТЕРАТУРЫ:

- 1 Nekta[Электронный ресурс] Режим доступа URL:<https://neka.tech/obzor-wi-fi-i-primenenie-v-iot/>. Дата обращения 10.01.2024
- 2 Cyberleninka[Электронный ресурс] Режим доступа URL:<https://cyberleninka.ru/article/n/analiz-trafika-ustroystv-interneta-veschey>. Дата обращения 15.01.2024
- 3 Петин В.А. Новые возможности Arduino, ESP, Raspberry Pi в проектах IoT. - СПб.: БХВ-Петербург, 2022. - 320 с.: ил. - (Электроника).
- 4 LSTM – сети долгой краткосрочной памяти [Электронный ресурс] Режим доступа URL: <https://habr.com/ru/companies/wunderfund/articles/331310/>
- 5 Учебное пособие по RNN (рекуррентной нейронной сети): пример TensorFlow [Электронный ресурс] Режим доступа URL: <https://www.guru99.com/ru/rnn-tutorial.html>

## **АНАЛИЗ ПРИМЕНЕНИЯ НЕЙРОННЫХ СЕТЕЙ В КОНЦЕПЦИИ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ**

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

Ключевые слова: интернет вещей, рекуррентные нейронные сети, глубокая нейронная сеть

В статье представлены различные виды нейронных сетей, применяемых в концепции сетей Интернета вещей. Рассмотрены работы по возможности использования нейросетей в реальных устройствах с практическим применением. Представлено описание рекуррентных и глубоких нейронных сетей, сфера их применения и потенциал в концепции Интернета вещей, а также многослойные перцептроны и свёрточные нейронные сети.

**E.V. Yurchenko, D.V. Chadayev**

## **ANALYSIS OF THE APPLICATION OF NEURAL NETWORKS IN THE CONCEPT OF INTERNET OF THINGS NETWORKS**

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

Keywords: Internet of things, recurrent neural networks, deep neural network

The article presents various types of neural networks used in the concept of Internet of Things networks. Work on the possibility of using neural networks in real devices with practical applications is considered. A description of recurrent and deep neural networks is presented, their scope of application and potential in the concept of the Internet of Things, as well as multilayer perceptrons and convolutional neural networks.

Нейронные сети, в последнее время, все шире применяются для изучения интернета вещей (IoT). Это связано с возрастающим объемом данных, генерируемых устройствами IoT, которые требуют сложного анализа и обработки. Нейросети являются инструментом для обработки и анализа информации, что делает данную технологию наиболее подходящей для решения задачи изучения и управления устройствами IoT.

Используя нейронные сети, исследователи и разработчики могут создавать более эффективные и интеллектуальные системы управления устройствами IoT. Например, нейронные сети могут быть использованы для прогнозирования поведения устройств, выявления аномалий в их работе, оптимизации энергопотребления.

Существует несколько видов нейронных сетей, которые используются в сетях интернета вещей. Одной из таких является рекуррентная нейронная сеть. Рекуррентные нейронные сети (RNN – Recurrent Neural Network) — это класс нейронных сетей, которые хороши для моделирования последовательной информации, такой как временные ряды или естественный язык [1]. Данные нейронные сети способны запоминать информацию в процессе работы одного элемента и передавать эту же информацию следующему элементу. Применять такой класс нейронных сетей можно в разных задачах, таких как защита информации от несанкционированного доступа и вредоносного ПО, распознавание речи, обработки естественного языка и так далее.

Ассоциативная случайная нейронная сеть рассмотрена Эрелом Геленбе и Мертом Накипом [2]. Данная нейронная сеть была создана для предотвращения сетевых атак, таких как «Отказ в обслуживании» и подобных. Принцип работы заключается в том, что случайная нейронная сеть,

состоящая из двух подсетей, связанных друг с другом и дополняющих друг друга в рекуррентной структуре, называемой ассоциированной (ARNN – Associated Recurrent Neural Network). Для каждого устройства сети два нейрона отстаивают противоположные точки зрения: присутствует ли нарушение в сети или нет. Ассоциативная нейронная сеть отслеживает весь входящий на узел трафик, изучает взаимосвязи между узлами и формирует рекомендации по защите устройства или IP-адреса. На рисунке 1 представлена оценка кибератак на основе ассоциативной случайной нейронной сети

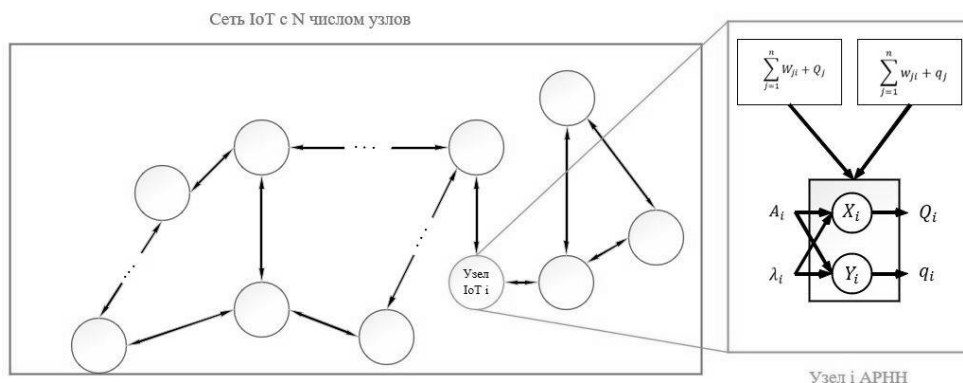


Рисунок 1 - Оценка кибератак на уровне сети на основе ARNN для  $n$  узловой сети

Данная нейронная сеть может использоваться не только для защиты устройств интернета вещей, но и для защиты IP-адресов в сети. Из результатов работы можно сделать вывод, что скорость реакции данной нейронной сети меньше, чем у прочих подобных, но для обучения с реальным и средним трафиком для последующей работы уходит гораздо больше времени, из-за чего использование может быть неуместно в ограниченных по времени приложениях.

Похожую работу о динамическом анализе для обнаружения вредоносных программ IoT (DAIMD – Dynamic Analysis for IoT Malware Detection), который выполняет динамический анализ вредоносных программ IoT во вложенной облачной среде виртуальных машин и изучает изображения поведения, сжатые огромным количеством данных о поведении, на основе модели сверточной нейронной сети (CNN – Convolution Neural Network) провели Цзюын Чон, Пак Чон Хок и Ёк Син Чон[3]. Схема DAIMD динамически анализирует вредоносное ПО, представляющее угрозу для IoT-устройств, оснащенных ограниченными аппаратными ресурсами, в облачной вложенной виртуальной среде и обучает их с помощью модели CNN с помощью специальных процессов анализа и обнаружения, аналогичных тем, которые используются в общих системах обнаружения вредоносного ПО. Процессы детектирования вредоносных программ в общей системе обнаружения вредоносных программ и DAIMD показаны на рисунке 2.

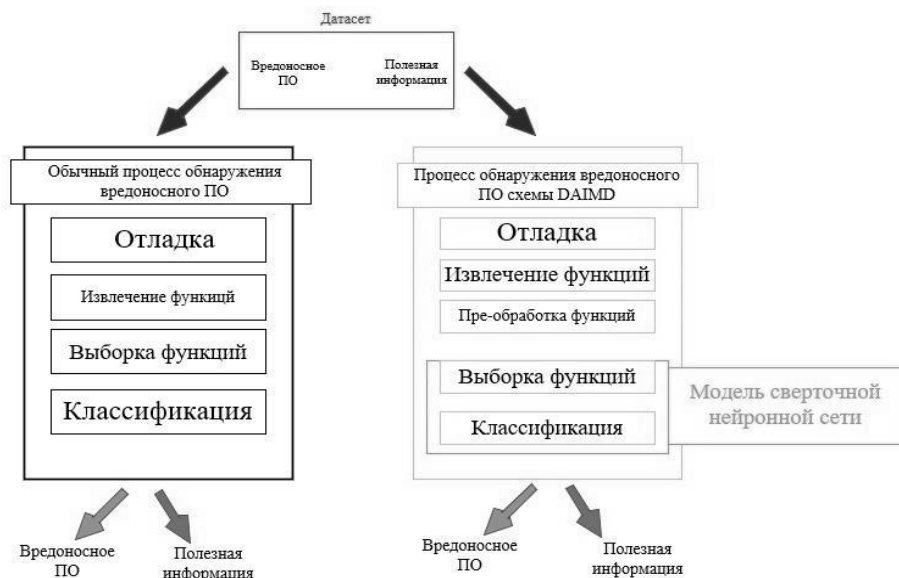


Рисунок 2 - Сравнение процесса обнаружения вредоносных программ в общей системе обнаружения вредоносных программ и DAIMD.

Результатом работы стало заключение, что схема DAIMD справляется с анализом и предотвращает случаи заражения устройств IoT. Однако некоторые вредоносные ПО способны распознавать среду, в которой они запускаются, в следствии чего избегать систем и обнаружения анализа со стороны.

Улучшенный алгоритм оптимизации серого волка (IGWO - Improved Grey Wolf Optimization) и нейронная сети Элмана (IGWO-Elman) были рассмотрены Лингвей Сюем, Сюй Юем и Т. Аароном Гулливером [4]. Данная архитектура создавалась для обеспечения стабильной работы мобильных сетей Интернета вещей. Чтобы достигнуть этого, необходимо прогнозирование вероятности отключения электропитания. Алгоритм оптимизации серого волка используется для подбора параметров оптимального прогнозирования.

Использование системы искусственного интеллекта на основе модифицированного на основе глубокого обучения (EG-CRNN - Element-wise Attention Gate) для прогнозирования количества пакетов в сети и управления кластерной головкой датчиков рассмотрели Надя Андан Шилгат Аль-Джамали и Хаммед С. Аль-Равешиди[5]. В данной работе предложена искусственная интеллектуальная система для устранения эффектов перегрузки в транспортной нагрузке в интеллектуальной сети Интернета вещей на основе сверточной рекуррентной нейронной сети глубокого обучения с модифицированным элементарным шлюзом внимания. Архитектура EG-CRNN имеет один входной слой, четыре слоя CRNN, слой выпрямленных линейных единиц и выходной слой. EG-CRNN обучается в автономном режиме, чтобы определить размер буфера платформы IoT, а затем обучается в режиме онлайн для идентификации потока трафика. В результате данной работы было выявлено, что использование EG-CRNN повышает эффективность работы IoT сети, а соответственно, повышает качество обслуживания QoS.

Систему распознавания речи на аутсорсинге с сохранением конфиденциальности для интеллектуальных устройств Интернета вещей рассмотрели Чжоу Ма, Ян Лю, Симен Лю Фейфей Лю и Цзяньфен Ма[6]. С ростом популярности умного дома и устройств управления домом с помощью голоса, таких как Алиса или Алекса, возрастает и риск утечки и фальсификации данных пользователей. В ходе исследований было выявлено, что привычная рекуррентная нейронная сеть (RNN) становится ненадежной в сложных прикладных средах. Вместо этого лучше использовать нейронную сеть, основанную на RNN - долгую краткосрочную память - LSTM. Отличие от RNN заключается в том, что нейроны заменены на блоки памяти, что помогает запоминать долговременные зависимости. Данные в аудиосигнале разделяются на секретные разделители и обрабатываются в виде зашифрованного текста, что обеспечивает хорошую конфиденциальность данных.

Помимо рекуррентных нейронных сетей, рассмотрим метод глубокого построения нейронной сети. Данная нейронная сеть может в себе содержать несколько слоёв, как правило их должно быть более трёх. Каждый слой отвечает за различные типы фильтрации, а также категоризацию в процессе выполнения работы. Данные глубокой нейронной сети зависят от количества в ней слоёв. Большое количество слоёв применяется в решении сложных задач, таких как распознавание изображения, лингвистика, обучение с подкреплением и генерацией данных[7].

Метод многозадачного обучения по обнаружению ключевых слов на основе глубоких нейронных сетей для устройств Интернета вещей изучили Сон-Гюн Лим, Ин-Чул Ю и Донсук Юк[8]. Предлагаемое обнаружение ключевых слов на основе глубокой нейронной сети с использованием скрытых Марковских моделей может применяться в качестве распознавательного устройства для активации модуля распознавания речи в различных устройствах Интернета вещей. В ходе работы было произведено 6130 взысканий в различных условиях и выявлено, что использование подхода к многозадачному обучению для системы на основе DNN-НММ с использованием моделей ключевого слова трифон и моделей-заполнителей монофонов дает наивысшую точность, одновременно уменьшая вычислительные затраты в сравнении с использованием DNN-НММ с двумя DNN. Таким образом, использование многозадачного обучения для определения ключевых слов на основе DNN-НММ является эффективным методом в независимых от словаря системах определения ключевых слов.

Рассмотрим такие методы построения нейронных сетей, такие как многослойные перцептроны (MLP – Multi-layer Perceptron) и сверточные[7]. Метод многослойных перцептронов состоит из нескольких слоёв нейронов, таких как входные, скрытые и выходные слои. Взаимодействие слоёв нейронов при обработке данных выполняется по принципу, когда данные, находясь на одном из слоёв нейронов, выполняют свои функции и задачи для дальнейшего перехода в следующий слой. Данный метод нейронной сети применяется для решения сложных задач, таких как распознавание речи, анализ текста, работа с временными рядами и другие.

Свёрточный метод построения нейронной сети предназначен для обработки мультимедийных данных. При обработке данных свёрточной нейронной сетью извлекаются различные характеристики за счёт фильтров, после чего применяется нелинейная функция для улучшения производительности сети. После этого за счёт уменьшения размерности данных, выделяется наиболее значимая характеристика. Данные нейронные сети являются основным инструментом для обработки мультимедийных данных и широко используются для определения объектов, классификации изображений и анализа видео.

Таким образом, было исследовано применение нейронных сетей в концепции сети интернета вещей. В сетях интернета вещей наиболее часто используются рекуррентные и глубокие методы построения нейронных сетей, так как они являются наиболее гибкими и удобными для исследований параметров сети. Метод построения многослойных перцептронов менее популярен из-за упрощенного функционала по сравнению с глубокими нейронными сетями. Свёрточный метод построения нейронных сетей в концепции интернета вещей практически не используются, так как возможности данных нейронных сетей больше подходят для обработки изображений и видео, а не для анализа трафика или предсказания событий.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Рекуррентные нейронные сети (RNN) с Keras / Хабр (habr.com) Дата обращения 15.04.2024
2. E. Gelenbe and M. Nakip, "IoT Network Cybersecurity Assessment With the Associated Random Neural Network," in *IEEE Access*, vol. 11, pp. 85501-85512, 2023, doi: 10.1109/ACCESS.2023.3297977. Дата обращения 14.04.2024
3. J. Jeon, J. H. Park and Y. -S. Jeong, "Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model," in *IEEE Access*, vol. 8, pp. 96899-96911, 2020, doi: 10.1109/ACCESS.2020.2995887. Дата обращения 14.04.2024
4. L. Xu, X. Yu and T. A. Gulliver, "Intelligent Outage Probability Prediction for Mobile IoT Networks Based on an IGWO-Elman Neural Network," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1365-1375, Feb. 2021, doi: 10.1109/TVT.2021.3051966. Дата обращения 14.04.2024

5. N. A. S. Al-Jamali and H. S. Al-Raweshidy, "Smart IoT Network Based Convolutional Recurrent Neural Network With Element-Wise Prediction System," in *IEEE Access*, vol. 9, pp. 47864-47874, 2021, doi: 10.1109/ACCESS.2021.3068610. Дата обращения 14.04.2024
6. Z. Ma, Y. Liu, X. Liu, J. Ma and F. Li, "Privacy-Preserving Outsourced Speech Recognition for Smart IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8406-8420, Oct. 2019, doi: 10.1109/IJOT.2019.2917933. Дата обращения 15.04.2024
7. Сущеня Р.В., Кокаев А.Э. НЕЙРОННЫЕ СЕТИ И ИХ КЛАССИФИКАЦИЯ. ОСНОВНЫЕ ВИДЫ НЕЙРОННЫХ СЕТЕЙ // Вестник науки. 2023. №8 (65). URL: <https://cyberleninka.ru/article/n/neyronnye-seti-i-ih-klassifikatsiya-osnovnye-vidy-neyronnyh-setey> (дата обращения: 16.04.2024).
8. S. -G. Leem, I. -C. Yoo and D. Yook, "Multitask Learning of Deep Neural Network-Based Keyword Spotting for IoT Devices," in *IEEE Transactions on Consumer Electronics*, vol. 65, no. 2, pp. 188-194, May 2019, doi: 10.1109/TCE.2019.2899067.

## К ВОПРОСУ О МЕХАНИЧЕСКОЙ НАДЕЖНОСТИ ОПТОВОЛОКОННЫХ ЛИНИЙ СВЯЗИ

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

Ключевые слова: надежность; оптические компоненты; оптическое волокно; волоконно-оптический датчик.

В статье рассматриваются общие концепции и методы проектирования механической надежности оптоволоконных датчиков и обсуждаются в какой степени они могут быть применены к оптическим компонентам, используемым в волоконно-оптических датчиках.

A.S. Yakovlev

## ON THE QUESTION OF MECHANICAL RELIABILITY OF FIBER OPTIC COMMUNICATION LINES

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

Keywords: reliability; optical components; optical fiber; fiber optic sensor.

This article reviews general concepts and techniques for mechanical reliability design of fiber optic sensors and attempts to discuss the extent to which they can be applied to optical components used for fiber optic sensors.

Волоконно-оптические датчики уже много лет используются в самых различных областях. Каждое использование датчиков выдвигает свои специфические требования, к которым инженеры-оптики всегда находили разумные решения. В результате было разработано множество методов оптического зондирования и разработано, изготовлено и применено множество различных датчиков, причем весьма успешно. Эти датчики построены с использованием различных видов оптических волокон и волноводов. В случае внешних волоконных датчиков волокно должно быть сопряжено и упаковано с внешним чувствительным телом, например полостью Фабри-Перо. Это требует использования отражающих торцевых покрытий, эпоксидных смол, соединителей, линз, капилляров, химических реагентов и т. д. Вообще говоря, волоконный или волноводный датчик следует рассматривать как сложную систему, состоящую из отдельных частей и компонентов между оптическим источником и оптическим детектором.

Проблема надежности волоконно-оптических и волноводных датчиков становится все более важной, поскольку они все чаще используются в приложениях, где отказ датчика может иметь серьезные последствия для безопасности и значительно увеличит общую стоимость системы. Примером такого приложения является структурный мониторинг работоспособности. Оценка надежности волоконного датчика остается сложной проблемой, поскольку эта надежность может быть определена на разных уровнях:

- надежность модуляции;
- надежность взаимодействия измеряемой физической величины и датчика-зонда;
- надежность демодуляции и обработки сигналов;
- надежность калибровки или повторной калибровки;
- надежность на компонентном уровне.

В данном случае речь пойдет о надежности компонентов с точки зрения механической надежности.



Вопрос механической надежности оптических волокон и оптических кабелей очень важен в области оптических датчиков, например в интеллектуальных структурах и приложениях мониторинга состояния конструкций, где волокна встроены в материалы или в структуры, которые нуждаются в мониторинге и в которых они постоянно испытывают усталость и высокие уровни напряжений [1, 2]. Также можно упомянуть все оптические волокна, соединяющие между собой другие типы волоконных или волноводных датчиков, включая резонаторные или интерферометрические датчики деформации или смещения типа Фабри-Перо.

Волоконно-оптические кабели для телекоммуникационной промышленности обычно рассчитаны на срок службы, превышающий 25 лет. Поэтому для количественной оценки механической надежности в разумные сроки необходимо проводить ускоренные эксперименты при более высоких уровнях напряжений в лаборатории и экстраполировать полученные результаты на более низкие напряжения в условиях эксплуатации. Например, в серии трудов SPIE [4–8] было опубликовано много интересной информации о том, как решать эту задачу.

Рассмотрим основы надежности оптического волокна на основе заключительного отчета COST246 [9], работ [10] и [11]. Механизмом отказов является разрушение волокна вследствие ослабления, вызванного ростом трещин дефектов вследствие напряжения. Поэтому для прогнозирования времени до разрушения при заданном приложенном эксплуатационном напряжении или максимально допустимом эксплуатационном напряжении, гарантирующем заданный срок службы, обычно используют уравнения усталости механики разрушения, основанные на степенном законе кинетики роста трещин. Для этого предполагается, что скорость роста трещины  $v$  пропорциональна мощности интенсивности напряжений на вершине трещины  $K_I$  (выражение 1):

$$v = \frac{da}{dt} = AK_I^n \quad (1)$$

где  $a$  - длина трещины,  $A$  и  $n$  - параметры подгонки.

В механике отказов коэффициент интенсивности напряжений  $K_I$  связан соотношением к перпендикулярно приложенному напряжению  $\sigma$  и параметру формы  $Y$  в зависимости от геометрии трещины выражением (2).

$$K_I = Y\sigma\sqrt{a} \quad (2)$$

Подставляя в выражение (1) коэффициент интенсивности из выражения (2) получаем дифференциальное уравнение, которое может быть решено для конкретного изменения приложенной нагрузки  $\sigma(t)$ . Например, считается, что волокно в кабеле испытывает долгосрочное событие загрузки. В статическом случае  $\sigma(t)$  является постоянной  $\sigma(t) = \sigma_a$ . Она определяет начальную или инертную силу  $\sigma_i$  через выражение 3:

$$K_{IC} = Y\sigma_i\sqrt{a} \quad (3)$$

$K_{IC}$  является критическим значением  $K_I$ , то есть то значение интенсивности напряжений на вершине трещины, при котором происходит катастрофическое разрушение. Начальная прочность уменьшается при больших размерах трещин. Значения  $K_{IC} = 8 \cdot 10^5 \text{ Нм}^{-3/2}$  для силикатного стекла и  $\sigma_i = 13 \text{ ГПа}$  для телекоммуникационного волокна. Отказ произойдет, когда убывающая прочность достигнет приложенного напряжения.

В статическом случае можно найти время до отказа (или разрушения)  $t_f$ :

$$t_f = \frac{2}{(n-2)} \cdot \frac{(\sigma_i^{n-2} - \sigma_a^{n-2})}{AY^2\sigma_a^n K_{IC}^{n-2}} \quad (4)$$

Выражение (4) упрощается до выражения 5:

$$t_f = B \frac{\sigma_i^{n-2}}{\sigma_a^n} \quad (5)$$

где  $B$  равно:

$$B = \frac{2}{(n-2)} \cdot \frac{1}{AY^2 K_{IC}^{n-2}} \quad (6)$$

зная, что приложенное напряжение ниже, чем инертная прочность, и что  $n$  обычно велико для кремнеземных волокон (выражение 6).

Таким образом, для статической нагрузки модель степенного закона связывает усталость, вызванную напряжением, с двумя параметрами роста трещин, зависящими от окружающей среды:  $B$ , который является параметром сохранения трещиностойкости и мерой ослабляющего влияния конкретных приложенных напряжений на волокно, и  $n$ , который является постоянной усталости и служит параметром восприимчивости к коррозии под напряжением. Параметр  $n$  измеряет, как быстро растет трещина под воздействием воды и напряжения. Оба значения необходимы для расчета времени жизни под напряжением. Значения  $n$  - в диапазоне от 20 до 40 и  $B$  - в диапазоне от  $10^{-8}$  ГПа<sup>2</sup> до 0,1 ГПа<sup>2</sup> для стандартных телекоммуникационных волокон.

Аналогичное рассуждение можно привести и для динамической усталости с постоянной величиной  $\sigma'$  и приложенной нагрузкой  $\sigma(t) = \sigma' t$  [10]. В этом случае можно найти разрушающее напряжение  $\sigma_f$  выражение 7:

$$\sigma_f^{n+1} = (n + 1)\sigma' B \sigma_i^{n-2} \quad (7)$$

Оценка срока службы волокна на практике является относительно трудоемкой задачей. При лабораторных испытаниях обычно устанавливают заранее известное напряжение к волокну и измеряют время до разрушения при статической нагрузке или напряжение волокна при постоянной скорости деформации и измерении нагрузки при разрушении при динамической усталости. Это необходимо делать многократно на статистически значимом количестве выборок и предпочтительно по стандартному методу [12-16]. Опыт показал, что для современных волокон допустима статическая деформация 2% в течение всего срока службы строительных конструкций при условии отсутствия дополнительных поверхностных трещин при монтаже [17]. В телекоммуникационных приложениях разрушение волокна из-за стресса и окружающей коррозии, способствующей росту трещин в соединениях волоконных кабелей, имеет типичную интенсивность отказов от 0,5 до 2,3 FIT/км. Это значение почти ничтожно по сравнению с повреждением волокна из-за перекопки кабеля, для которого частота отказов составляет от 400 до 800 FIT/км [18].

После процесса старения с нулевым напряжением в агрессивных условиях, таких как влажные условия и присутствие щелочи и других ионов у волокон появляется модифицированная механическая прочность. Химия на поверхности кремнезема волокна играет существенную роль. Во всех случаях важно ограничить механическое повреждение поверхности волокна, так как это может привести к развитию поверхностных трещин. Кроме того, вода должна быть удалена от поверхности волокна, например, с помощью герметичных покрытий. Однако многие волоконные датчики используют модифицированные волокна с локально удаляемыми покрытиями, локальным повторным покрытием или специальными типами покрытия, которые допускают определенное взаимодействие для химического зондирования. Известно, что зачистка ухудшает прочность волокна. Удаление покрытия без повреждения волокна имеет важное значение, и необходимо убедиться, что покрытие полностью удалено. Присутствие пыли, влажного воздуха и химических веществ во время обработки волокон может привести к дополнительному ухудшению прочности, а старение может быть ускорено химическими остатками. Кроме того, сенсорные волокна часто подвергаются воздействию уровней напряжений (с точки зрения температуры, механического воздействия и химической агрессивности), которые могут превышать те, которые рассматриваются для стандартного телекоммуникационного волоконного кабеля. В открытой литературе имеется лишь несколько сведений о механической надежности таких модифицированных волокон в этих весьма специфических условиях.

Надежность является ключевой темой для оптических компонентов и систем, например, когда они реализуются как не подлежащие ремонту детали в инфраструктурных системах с длительным сроком службы. Модели ожидаемой продолжительности жизни и частоты отказов являются важными инструментами для оценки надежности этих компонентов. В связи с этим методы оценки надежности, разработанные в последние десятилетия в области механики и электроники, могут быть применены к оптическим компонентам. Такие модели в идеале

базируются на характеристике механизмов физического отказа, подкрепленной статистически устойчивым (ускоренным) тестированием который учитывает соответствующие экологические и эксплуатационные условия. Некоторые рекомендации, применимые к оптическим телекоммуникационным компонентам, могут быть перенесены в сенсорное поле, но многие проблемы, связанные с волоконно-оптическим зондированием, должны решаться индивидуально, и руководящие принципы все еще должны быть установлены.

Кроме того, новые фотонные технологии внедряются значительными темпами, в то время как расширяется спектр областей их применения. Эти технологии включают в себя новые материалы, включают микро - и нанофотонику, опираются на микрооптико-электромеханические системы и т. д. Примеры новых применений можно найти, в частности, в космосе, в авиации, в биомедицинской области, в автомобильной промышленности и на ядерных объектах. Поэтому моделирование надежности и прогнозирование частоты отказов, вероятно, останутся междисциплинарным и постоянным процессом.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Z. Xu, A. Bassam, H. Jia, A. Tennant and F. Ansari, Fiber optic sensor reliability issues in structural health monitoring, *SPIE Proceedings* 5758, 390–404 (2005).
2. E. Udd, M. Winz, S. Kreger and D. Heider, *SPIE Proceedings* 5758, 409–416 (2005).
3. Optical Fiber Reliability and Testing, *SPIE Proceedings* 3848, edited by J. Matthewson (1999).
4. Optical Fiber and Fiber Component Mechanical Reliability and Testing, *SPIE Proceedings* 4215, edited by M.J. Matthewson (2001).
5. Optical Fiber and Fiber Component Mechanical Reliability and Testing II, *SPIE Proceedings* 4639, edited by M.J. Matthewson and C.R. Kurkjian (2002).
6. Reliability of Optical Fiber Components, Devices, Systems, and Networks, *SPIE Proceedings* 4940, edited by H.G. Limberger and M.J. Matthewson (2003).
7. Reliability of Optical Fiber Components, Devices, Systems, and Networks II, *SPIE Proceedings* 5465, edited by H.G. Limberger and M.J. Matthewson (2004).
8. Reliability of Optical Fiber Components, Devices, Systems and Networks III, *SPIE Proceedings* 6193, edited by H.G. Limberger and M.J. Matthewson (2006).
9. *Reliability of Optical Fibres and Components – Final Report of COST 246*, edited by T. Volotinen, W. Griffioen, M. Gadonna and H. Limberger, (Springer-Verlag, London, 1999).
10. M.J. Matthewson, Strength Probability Time Diagrams using Power Law and Exponential Kinetics Models for Fatigue, *SPIE Proceedings* 6193, 619301 (2006).
11. L.K. Baker, Comparison of Mechanical Reliability Models for Optical Fibers, Corning White Paper WP5049 (2001).
12. IEC 60793-1-30 First Edition, Optical fibres – Part 1–30: Measurement methods and test procedures – Fibre proof test (IEC, 2001).
13. IEC 60793-1-31 First Edition, Optical fibres – Part 1–31: Measurement methods and test procedures – Tensile strength (IEC, 2001).
14. IEC 60793-1-32 First Edition, Optical fibres – Part 1–32: Measurement methods and test procedures – Coating strippability (IEC, 2001).
15. IEC 60793-1-33 First Edition, Optical fibres – Part 1–33: Measurement methods and test procedures – Stress corrosion susceptibility (IEC, 2001).
16. TIA/EIA-455-28-C FOTP-28 - Measuring Dynamic Strength and Fatigue Parameters of Optical Fibers by Tension (TIA/EAI, 2004)
17. U. Sennhauser and Ph.M. Nellen, in: *Trends in Optical Nondestructive Testing and Inspection*, edited by P.K. Rastogi and D. Inaudi (Elsevier Science Ltd. Oxford, 2000), pp. 473–485.
18. T. Volotinen, C. Kurkjian and A. Opacic, in: *Reliability of Optical Fibres and Components – Final Report of COST 246*, edited by T. Volotinen, W. Griffioen, M. Gadonna and H. Limberger (Springer-Verlag, London, 1999), pp. 37–77.

## ИССЛЕДОВАНИЕ КОЭФФИЦИЕНТА ОТРАЖЕНИЯ РАДИОВОЛН В ЗАВИСИМОСТИ ОТ ГЕОМЕТРИЧЕСКИХ РАЗМЕРОВ ЕМКОСТИ

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

Ключевые слова: анализ водных растворов, диэлектрическая проницаемость, коэффициент отражения радиоволн, коэффициент прохождения радиоволн, многослойные структуры.

В статье описаны результаты математического анализа коэффициента отражения электромагнитных волн радиодиапазона от емкостей конечного размера.

**D.A. Ovchinnikov, S.A. Baranov, N.M. Barbin, V.T. Kuanyshev**

## RESEARCH OF RADIO WAVE REFLECTION COEFFICIENT DEPENDING ON THE GEOMETRIC DIMENSIONS OF THE CONTAINER

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

Keywords: analysis of aqueous solutions, dielectric constant, radio wave reflection coefficient, radio wave transmission coefficient, multilayer structures.

The article describes the results of a mathematical analysis of the reflection coefficient of electromagnetic radio waves from finite-sized containers.

Существует ряд задач, который требует возможности исследования внутренней структуры объекта без нарушения его целостности. Примером таких задач, например, будет исследование содержимого контейнеров, закрытых и опломбированных тар. Одним из методов проведения такого рода исследований может быть метод интроскопии.

Интроскопия - неинвазивное исследование внутреннего строения объекта или протекающих в нём процессов с помощью звуковых волн, сейсмических волн, электромагнитного излучения различных диапазонов, постоянного и переменного электромагнитного полей или потоков элементарных частиц [1].

Как известно, на любой неоднородности, на любой границе раздела сред с различными свойствами будет наблюдаться отражение и преломление волн. Иными словами, стенки контейнера и его объем будут искажать результаты измерений. Поэтому для объективной оценки получаемых результатов при проведении исследования следует отличать эффекты, вызванные свойствами содержимого контейнера, от свойств самого контейнера.

Так, например, метод радиоинтроскопии предполагает, что исследуемый объект будет подвержен облучению электромагнитными волнами радиодиапазона, которые при взаимодействии с объектом будут отражаться от него. По величине отраженного сигнала, его яркостной картине можно судить о природе и размерах объекта, скрытых от прямого наблюдения. Но в такой модели исследования отражение будет носить сложный характер: радиоволна будет отражаться от всех границ раздела сред и интерферировать между собой.

Следует заметить, что это свойство справедливо и для преломленной волны. Но с точки зрения удобства практического исследования в виду возможности всецело изучить объект имея в доступе только одну его сторону, целесообразно рассматривать исключительно отраженные волны.

Модель отражения радиоволны изображена на рисунке 1.

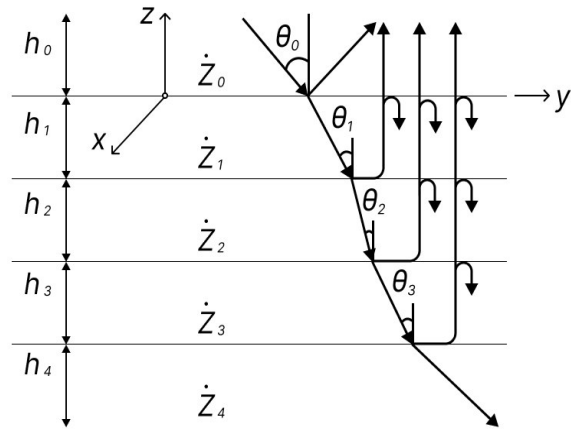


Рисунок 1 – Модель отражения радиоволны от емкости конечного размера

Обозначения на рисунке:

- $h$  – толщина слоя;
- $\theta$  – угол падения ЭМВ на границу раздела сред;
- $Z_0$  – характеристическое сопротивление воздуха,  $Z_1$  – сопротивление стенки емкости,  $Z_2$  – сопротивление водного раствора,  $Z_3$  – сопротивление стенки емкости,  $Z_4$  – характеристическое сопротивление воздуха.

Рассматривалось три случая:

- трехслойная задача, радиоволна падала из воздуха в слой воды конечного размера и затем снова попадала в воздух (стенками контейнера в данном случае пренебрегалось);
- пятислойная задача, канистра с водой, радиоволна проходит сквозь стенку канистры, попадает в слой воды, затем снова сквозь стенку канистры в воздух;
- пятислойная задача, пустая канистра, радиоволна проходит сквозь стенку канистры, попадает в слой воздуха, затем снова сквозь стенку канистры в воздух.

Толщина стенки контейнера была фиксированной и принята за 2 миллиметра, толщина контейнера изменялась от 0 до 1 метра. Слой воздуха за контейнером брался бесконечно большой длины. Комплексная диэлектрическая проницаемость материалов:

- воздух  $\epsilon_{возд.} = 1 - j0$ ;
- стенка контейнера  $\epsilon_{пласт.} = 2.4 - j0$ ;
- воды  $\epsilon_{возд.} = 79.13 - j4.1$ .

Математическая модель пресной воды взята из рекомендации МСЭ-R[4], расчет отражения выполнялся по методике, изложенной в [5]. Угол падения радиоволны на исследуемый контейнер равен 90 градусам. Частота радиоволны 1 ГГц.

График отражения радиоволны сквозь измерительную ячейку согласно рассмотренной модели полученные аналитическим методом приведены на рисунках 2 и 3.

Из рассматриваемых графиков видно, что размер контейнера оказывает существенный характер на коэффициент отражения радиоволн – отражение имеет синусоидальный характер. Период колебаний кратен половине длины волны (хорошо видно на примере пустого контейнера рисунок 2). Наличие диэлектрика в контейнере в виде воды уменьшает длину волны в контейнере, из-за чего частота колебаний коэффициента отражения увеличивается.

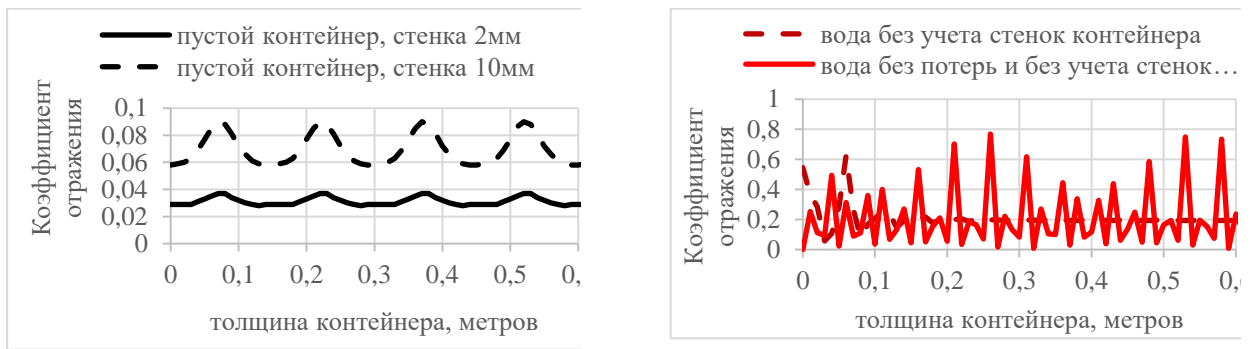


Рисунок 2 - Отражение радиоволны от пустого контейнера и слоя воды конечного размера

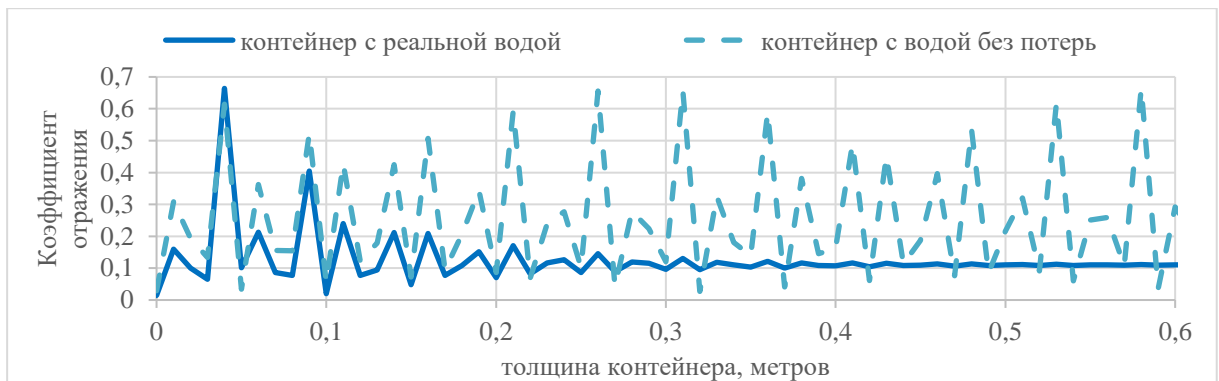


Рисунок 3 - Отражение радиоволны от контейнера с водой

При рассмотрении коэффициента отражения от среды с потерями, колебания носят затухающий характер. В рамках рассмотренных сред, при глубине контейнера более 50 сантиметров коэффициент отражения становится постоянным и такую среду можно рассматривать как среду бесконечного размера.

Таким образом, при радиоинтроскопии необходимо учитывать геометрические размеры емкости. Для повышения качества исследования требуется нивелировать вклад многократного отражения сигнала, например, проведением исследования в широком диапазоне частот с усреднением полученных результатов.

#### Литература:

1. Интроскопия [Электронный ресурс] // Режим доступа: <https://ru.wikipedia.org/wiki/Интроскопия> – Загл. с экрана.
2. М.И. Финкельштейн В.А. Кутев В.П. Золотарев Применение радиолокационного подповерхностного зондирования в инженерной геологии. Москва "Недра" 1986, 128с
3. В.В. Сысуев Георадарные исследования полимасштабных структур в ландшафтах на примере смоленско-московской возвышенности вестн. моск. ун'та. сер. 5. география. 2014. № 4
4. Рекомендация МСЭ-R P.527-4 (06/2017) Электрические характеристики земной поверхности Серия Р Распространение радиоволн
5. Бреховских Л.М. Волны в слоистых средах 2-е изд., доп. и испр. — М.: Наука, 1973. — 343 с.: ил.



## **Секция 2. СИСТЕМЫ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

**В.Н. Коваленко**

### **СИСТЕМЫ УПРАВЛЕНИЯ ПОЕЗДАМИ НА БАЗЕ РАДИОКАНАЛА И С ИСПОЛЬЗОВАНИЕМ СПУТНИКОВЫХ ТЕХНОЛОГИЙ**

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

Ключевые слова: система, мониторинг, состояние, спутниковая система ГЛОНАСС/GPS, локомотив, точечный датчик, рельсовая цепь, тормозной путь, безопасность, интервальное регулирование, пропускная способность.

Статья посвящена вопросам стратегического решения ОАО «РЖД» о создании комплексных информационно-управляющих систем (КИУС). Для решения этого направления в создании систем управления поездами большое внимание уделяется разработке единого пространства координат и единой базы данных на основе электронных карт с использованием геоинформационной системы, которая разработана специалистами ООО «НИИАС».

**V.N. Kovalenko**

### **RADIO-BASED TRAIN CONTROL SYSTEMS AND USING SATELLITE TECHNOLOGITS**

Ural State University of Railway Transport (URGUPS), Ekaterenburg, Russia

Key words: system, monitoring, condition, GLO-NASS/GPS satellite system, locomotive, point sensor, track circuit, braking distance, safety, interval control, throughput

The article is devoted to the issues of the strategic decision of JSC "Russian Railways" on the creation of integrated information management systems (CIUS). To solve this problem, in the creation of train control systems, much attention is paid to the development of a single coordinate space and a single database based on electronic maps using a geoinformation system developed by specialists of NIIAS LLC.

В ОАО «РЖД» принято стратегическое решение о создании комплексных информационно-управляющих систем (КИУС). Для решения этого направления в создании систем управления поездами большое внимание уделяется разработке единого пространства координат и единой базы данных на основе электронных карт с использованием геоинформационной системы, которая разработана специалистами ООО «НИИАС».

Точность определения местоположения и параметров движения поездов может быть реализована с помощью спутниковых систем ГЛОНАСС/GPS, при этом также появляется и возможность оценивания параметров локомотивных устройств. Непрерывный мониторинг параметров ж.-д. пути и состояния подвижных единиц является критерием безопасности движения и позволяет принять незамедлительные действия для предотвращения опасных ситуаций [1]. В настоящий момент времени наблюдается возможность использования искусственного интеллекта для управления движением поездов.

Для высокоскоростных магистралей специалистами ООО «НИИАС» разработана высокоточная координатная система (ВКС). Эта многофункциональная автоматизированная информационная система, занимающаяся сбором, хранением и обработкой координат о местоположении стационарных и движущихся объектов железнодорожного транспорта. Таким образом, ВСК обеспечивает единое пространство координат с использованием системы ГЛОНАСС/GPS.

На рисунке 1 представлена работа системы на базе спутниковой связи и радиосвязи. Информация о координатах поездов может быть получена с помощью либо системы ГЛОНАСС, либо системы GPS.

Сигналы спутниковых передатчиков ГЛОНАСС/GPS принимаются на подвижном составе, с помощью приемных устройств. Затем производится их обработка, в результате которой вычисляется координата локомотива, определяется скорость и ускорение поезда. На основании этих параметров движения поезда, также информации о весе поезда, длине и состоянии тормозной системы поезда, вычисляется реальная длина тормозного пути данного поезда.

С другой стороны, для определения минимального безопасного интервала попутного следования надо знать координату хвоста впереди движущегося поезда и величину его тормозного пути. Эта информация передается на локомотив следующей за ним по спутниковой системе связи (ССС). Для этого на всех локомотивах установлены приемопередатчики СССР и устройства сопряжения. Информация передается в аппаратуру спутника СССР, которая транслирует его в узловую наземную станцию (УЗС). Потом передатчик УЗС через аппаратуру спутника СССР передает эту информацию на локомотив следующим за первым, рассчитывается минимально допустимый интервал между поездами [2].

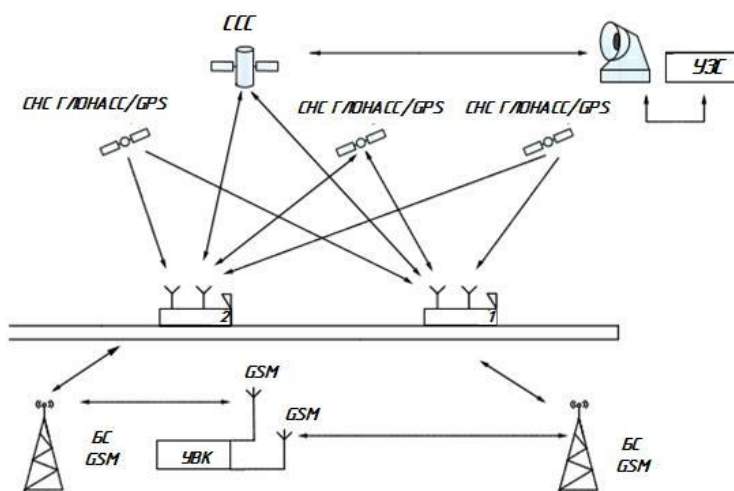


Рис. 1. – Спутниковая связь и радиосвязь

При использовании радиосвязи GSM-R (Gliai System for Mobile Communication), на локомотивах также устанавливаются специальные модули. Информация о координатах поездов и длинах их тормозных путей передается сначала на базовую станцию (БС), а затем с БС в управляющий вычислительный комплекс (УВК), что позволяет организовать безопасный процесс движения поезда, целью которого является обеспечение безопасных межпоездных интервалов.

Большой опыт эксплуатации цифровых систем радиосвязи получен при эксплуатации электропоездов «Сапсан» на линии Санкт – Петербург – Москва.

Например, данные для системы «Автодиспетчер» передает подсистема контроля координат и скорости движения поездов, которая реализована с помощью радиоканала системы ТЕТРА и средств геоинформационной системы спутниковой радионавигации ГЛОНАСС/GPS.

Как правило, увеличивать пропускную способность следует при увеличении интенсивности движения поездов, а путями решения этого вопроса являются, во-первых, сокращение интервала попутного следования составов и, во-вторых, увеличение скорости движения поездов. Это становится возможным только при модернизации систем автоматической блокировки (АБ). Ниже приведены некоторые системы, которые при своем функционировании используют радиоканал.



Так, например, разработана микропроцессорная автоблокировка с централизованным размещением аппаратуры и рельсовыми цепями тональными частоты АБТЦ-М. Эта система использует информацию о координатах поездов, принятой от них по радиоканалу, имеет безопасный алгоритм функционирования с использованием сигналов от рельсовых цепей. Эта система предназначена для организации оптимального процесса движения как грузовых, так и пассажирских поездов на перегонах. Структура этой системы приведена на рисунке.2.

Организовать единое информационное пространство для организации оптимального процесса движения поездов на перегоне при полном отсутствии светофоров по виртуальным блок-участкам и взаимодействие с европейской системой ERTMS/ ETCS [3] позволит использование цифрового радиоканала системой АБТЦ-МШ.

К современным зарубежным системам можно отнести такие как: европейская система контроля движения поездов - ETCS (European Train Control System); глобальная система мобильной связи для железнодорожного транспорта - GSM-R (Global System for Mobile Communication for Railway), а также европейская система управления движением поездов - ERTMS (European Rail Traffic Management system).

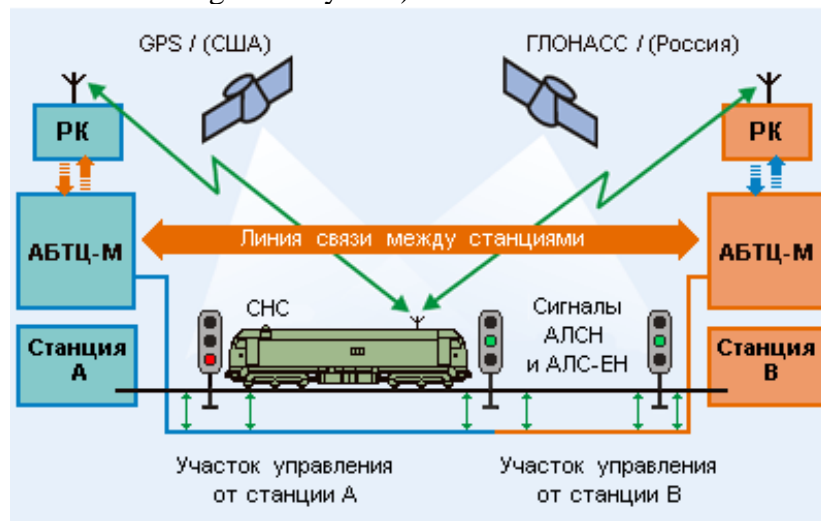


Рис. 2. – Система АБТЦ-М

В этих системах для связи напольных и локомотивные устройств используются в качестве напольных передатчиков EUROBALISE. Они передают на локомотив информацию о состоянии впереди расположенных, блок-участков (свободно, занято). В качестве одного из критериев безопасности движения в этих системах используется контроль максимально допустимой скорости движения. Информацию о положении поезда также передают эти передатчики.

При этом информация о распределении поездов на участке непрерывно по системе GSM-R передается на локомотив. Движение поездов осуществляется по сигналам локомотивных устройств, а напольные светофоры применяются в качестве дублирующих. Состояния участков железной дороги определяются рельсовыми цепями или точечными датчиками. При этом организация движения поездов в этом случае, т.е. интервальное регулирование на участке организуется исключительно по радиоканалу GSM-R. На рисунке 3 представлен принцип работы этой системы.

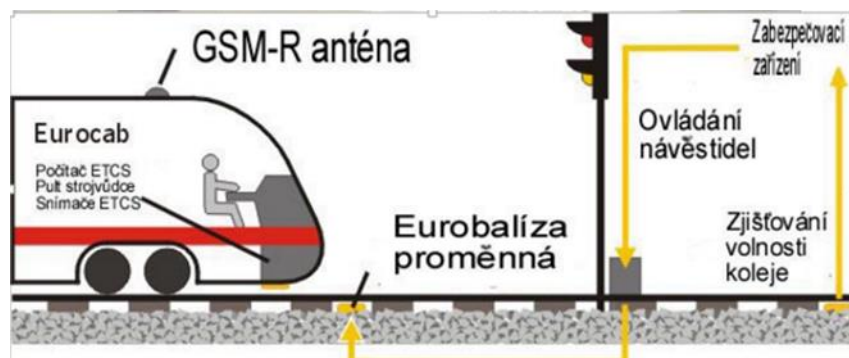


Рис. 3. - ETCS – уровень 1

На базе радиоканала российское подразделение компании ООО «Бомбардье Транспортейшн (Сигнал)» разработала и ввела в постоянную эксплуатацию систему интервального регулирования движения поездов (СИРДП-Е). Рисунок 4 поясняет принцип работы этой системы.

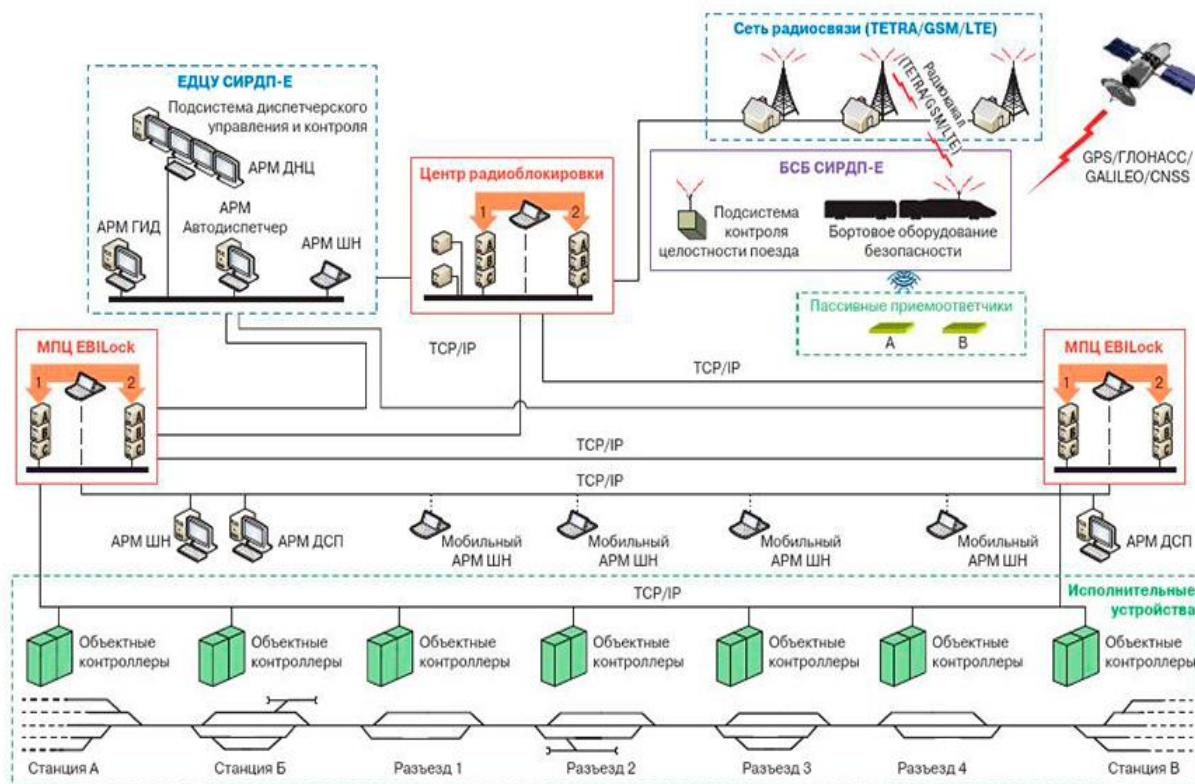


Рис. 4. – Система СИРДП-Е

Контроль за безопасностью движения поезда осуществляется бортовой системой безопасности. Между поездом и центром радиоблокировки обмен информацией осуществляется через систему радиосвязи стандарта TETRA. При этом необходимо отметить, что система СИРДП-Е может работать со всеми стандартами радиосвязи (GSM-R, LTE, TETRA, DMR). Контроль целостности состава в системе СИРДП-Е, осуществляет подсистема контроля целостности поезда (СКЦП). В системе СИРДП-Е реализован принцип регулирования движения поезда на «хвост» впереди идущего поезда. Таким образом, всей поездной работой на линии управляет СИРДП-Е.

Кроме этого, при производстве маневров бортовой компьютер системы СИРДП-Е контролирует выделения зоны производства работ и скорости движения, а также выполнение условий безопасности в отношении движения локомотивов. При этом, как утверждается в работе [4], повышается пропускная способность линии, снижается потребность в напольном оборудовании и техническом обслуживании, что приводит к значительному сокращению эксплуатационных затрат.

Исходя из вышеизложенного можно утверждать, использование спутниковых навигационных систем, а также радиосвязи позволит увеличить пропускную способность железнодорожных линий и скорости движения поездов с сохранением высокого уровня безопасности движения. При этом обеспечивается возможность дистанционного управления поездами, осуществление мониторинга движения поездов и их местоположения. Все эти функциональные возможности позволяет реализовать цифровую систему управления движением поездов. Рассмотренные выше технологии способны дать ответ на поставленные вопросы: как реализуется процесс движения с использования таких систем, как осуществляется мониторинг исправности механизмов подвижного состава, как решаются вопросы обеспечения безопасности процесса движения.

Список использованных источников:

1. НИИАС URL: <http://www.vnias.ru/2011-10-04-11-18-31>
2. Лисенков, В.М, Бестемьянов, П.Ф., Леушин, В.Б. Системы управления движением поездов на перегонах: Учебник для вузов ж.-д. транспорта: часть 1. – М. : ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2009. – 160с.
3. АБТЦ-М URL: <http://scbist.com/abtc-m/436-opisanie-abtc-m.html>
4. СИРДП-Е URL: [http://ru.bombardier.com/ru/press\\_release\\_20140505.htm](http://ru.bombardier.com/ru/press_release_20140505.htm)

## **Секция 3. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ИНФОРМАЦИИ**

**И.С. Коновалов, Д.В. Кусайкин**

### **О ПРИМЕНЕНИИ АВТОКОДИРОВЩИКОВ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ**

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

Ключевые слова: модуляция, демодуляция, автокодировщик, нейросети, волоконно-оптические системы передачи

В статье рассмотрены подходы к модуляции/демодуляции оптического сигнала с помощью автокодировщиков и их смежные применения. Приведён обзор работ, содержащих описание результатов исследований этих методов и их сравнительный анализ.

**I.S. Konovalov, D.V. Kusaykin**

### **ON APPLICATIONS OF AUTOENCODERS IN OPTICAL FIBER COMMUNICATION SYSTEMS**

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

Keywords: modulation, demodulation, autoencoder, neural networks, optical fiber communication systems

The article presents approaches to modulation/demodulation of optical signals by using autoencoders as well as some of the their related applications. An overview and a comparative analysis of existing works and proposed methods is presented.

В современном мире оптические сети связи являются неотъемлемой частью нашей жизни, обеспечивая передачу данных на большие расстояния с высокой скоростью и надежностью. Пропускная способность и дальность связи в оптических сетях ограничены такими явлениями как затухание, дисперсия, шум, а также нелинейные явления. Применение методов машинного обучения, в частности нейронных сетей, в сфере связи – многообещающая и активно исследуемая на данный момент область. Так как нейронные сети считаются универсальными аппроксиматорами, системы связи могут быть реализованы в качестве сквозной нейронной сети – автокодировщика. Такой подход может быть применён к волоконно-оптическим системам передачи (ВОСП) чтобы повысить их производительность и противодействовать вышеупомянутым искажениям сигнала, вызванным распространением сигнала по оптическому волокну.

Традиционные системы связи полагаются на легко интерпретируемые математические модели, основанные на статистике, теории информации, а также приближениях физических явлений. При этом, реальные системы не идеальны и подвержены влиянию нелинейных явлений, что делает сложным их математическое моделирование и приводит к ограниченной точности этих математических моделей. С другой стороны, алгоритмы машинного обучения способны производить оптимизацию, не требуя подробной математической модели [1].

Ещё одна проблема заключается в том, что системы передачи обычно построены в виде множества независимых блоков, каждый из которых выполняет отдельную конкретную функцию. В общем случае это делает такие системы проще для анализа и управления, а также позволяет



Нейронная сеть принимает на вход сообщение, представленное в виде множества символов унитарного кода, по одному символу на разряд. Унитарный код – двоичный код фиксированной длины, содержащий только одну единицу. Далее, с помощью скрытых слоёв передатчика, сообщение преобразуется в оптический сигнал – множество дискретных отсчётов. Каждый нейрон на выходе передатчика соответствует одному отсчёту [2].

После этого оптический сигнал поступает в смоделированный оптический канал связи. В канале связи моделируются явления затухания, дисперсии и шума. Далее, оптический сигнал поступает на приёмник, который выполняет обратное преобразование оптического сигнала с помощью нескольких скрытых слоёв в информационное сообщение [2].

Авторы исследования также приводят сравнение системы на основе автокодировщика с реальной системой передачи с модуляцией PAM2 и PAM4. Система передачи на основе автокодировщика стабильно демонстрирует значения BER несколько порядков ниже, что позволяет достичь более высокой скорости передачи данных и увеличить дальность связи. Авторам удалось достичь скорости передачи данных 42 Гбит/с на расстоянии 50 км, при использовании прямого детектирования и модуляции интенсивности (IM/DD) с помощью автокодировщика [2].

В 2021 г. Жанг и др. представили улучшенный вариант автокодировщика. В проведённом исследовании, авторы применяют алгоритм обучения AdaBoost на нескольких деревьях решений для приёмника оптического сигнала вместо распознавания символов с помощью нейронной сети. Алгоритм AdaBoost используется для повышения точности классификации множества отдельных менее точных классификаторов, в роли которых выступают деревья решений. Авторы исследования смогли таким образом добиться увеличения пропускной способности и дальности связи до 48 Гбит/с и 65 км соответственно [3].

Хотя вышеупомянутые исследования [2, 3] в основном фокусировались на компенсации дисперсии в оптическом волокне, которая является линейным явлением, нелинейные явления в среднем сложнее скомпенсировать, при этом нелинейные явления тоже приводят к межсимвольной интерференции в системах передачи с плотным спектральным уплотнением (DWDM). В 2018 г. Ли и др. [4] в своей статье исследовали производительность системы передачи на основе автокодировщика с нелинейным оптическим волокном в качестве канала связи.

В статье исследователи концентрируются исключительно на нелинейных явлениях, полностью игнорируя явление хроматической дисперсии. Основная причина такого решения, как поясняют авторы, заключается в том, что такая модель канала связи легко поддаётся анализу, для неё возможно определить максимальную теоретическую пропускную способность. Это позволяет сравнить производительность автокодировщика с оптимальным передатчиком и приёмником.

Структурная схема системы представлена на рисунке 2. Как и в до этого рассмотренных системах, исходное сообщение сначала преобразуется в унитарный код, который затем обрабатывается нейронной сетью передатчика. Нейронная сеть передатчика преобразует символы сообщения в один закодированный символ на выходе, представленный в виде комплексного числа. Затем, сформированный передатчиком оптический сигнал передаётся через канал связи, в котором он испытывает нелинейные искажения. После этого, искажённый сигнал обрабатывается нейронной сетью приёмника, которая пытается восстановить исходный отправленный передатчиком символ.



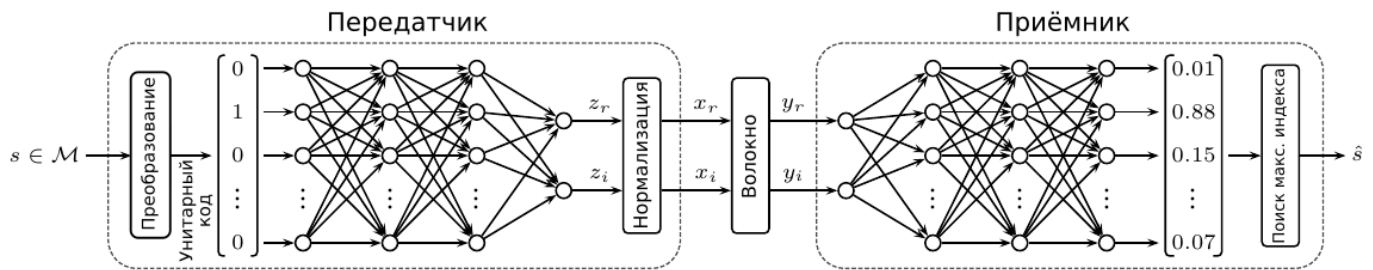


Рисунок 2 — Автокодировщик с нелинейным каналом связи

В своём исследовании авторы сравнивают производительность автокодировщика с классической системой передачи с модуляцией 16-QAM. Для сравнения использовалась частота символьных ошибок (SER). Производительность классической системы предсказуемо начинает падать после достижения определённой мощности, при которой нелинейные явления начинают проявляться гораздо сильнее. Производительность автокодировщика, с другой стороны, возрастает и превосходит классическую систему даже при сильном эффекте нелинейных явлений.

В заключении исследования авторы отмечают, что автокодировщики способны в процессе обучения определять близкие к оптимальным сигнальные созвездия, адаптироваться к особенностям канала связи. Обученный в рамках исследования автокодировщик устойчив к нелинейному фазовому шуму и превосходит классическую QAM систему по частоте символьных ошибок.

Таким образом, как показывает анализ публикаций, волоконно-оптические системы передачи с использованием автокодировщиков способны достичь близкие к оптимальным характеристики, в некоторых случаях такие системы демонстрируют превосходство над классическими, что во многом зависит от конкретной модели канала связи. ВОСП на основе автокодировщиков способны реализовывать эффективные сигнальные созвездия, а также компенсировать искажения сигнала, возникающие в процессе передачи по оптическому волокну, такие как хроматическая дисперсия, шум и нелинейные явления.

#### СПИСОК ЛИТЕРАТУРЫ:

- 1 An Introduction to Deep Learning for the Physical Layer / Т. О’Shea, J. Hoydis // IEEE Transactions on Cognitive Communications and Networking. — 2017. — Т. 3, No 4. — С. 563—575. — DOI: 10.1109/TCCN.2017.2758370.
- 2 End-to-End Deep Learning of Optical Fiber Communications / В. Karanov [и др.] // Journal of Lightwave Technology. — 2018. — Т. 36, No 20. — С. 4843—4855. — DOI: 10.1109/JLT.2018.2865109.
- 3 An Improved End-to-End Autoencoder Based on Reinforcement Learning by Using Decision Tree for Optical Transceivers / Q. Zhang [и др.] // Micromachines. — 2022. — Т. 13, No 1. — ISSN 2072-666X. — DOI: 10.3390/mi13010031. — Режим доступа: <https://www.mdpi.com/2072-666X/13/1/31>
- 4 Achievable Information Rates for Nonlinear Fiber Communication via End-to-end Autoencoder Learning / S. Li [и др.] // 2018 European Conference on Optical Communication (ECOC). — 2018. — С. 1—3. — DOI: 10.1109/ECOC.2018.8535456.

## ПРОЕКТ ИОТ СИСТЕМЫ – «АВТОНОМНЫЙ УМНЫЙ ДОМ»

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

Ключевые слова: Интернет вещей, датчики, микроконтроллер, сервер.

В статье приведено описание макета «умного» дома, нацеленного на работу в локальной сети, без подключения к Интернету. В состав макета входит следующий ряд функций: подсветка на основе датчика освещения, RFID - сканер для открывания двери, датчик температуры, «умная розетка».

I.V. Korobitsyn, O.E. Karanin, S.M. Plekhanov

## IOT SYSTEMS PROJECT – “AUTONOMOUS SMART HOME”

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

Keywords: Internet of things, sensors, microcontroller, server.

The article describes the layout of a “smart” home, aimed at working on a local network, without an Internet connection. The layout includes the following number of functions: lighting based on a light sensor, RFID scanner for opening the door, temperature sensor, smart socket.

В настоящее время многочисленные системы Интернета вещей (IoT), взаимодействующие с потребителями, функционируют на основе централизованных узлов обработки данных, которые обрабатывают входящие запросы и транслируют результаты конечным пользователям. Однако к недостаткам таких систем следует отнести риск утечки персональных данных на серверы поставщиков услуг и зависимость функциональности от подключения к Интернету. Как сказано в работе [1], создать систему умного дома используя решения мировых вендоров не составляет труда, но также придется столкнуться и последствиями в виде оплаты подписки, утечки данных и ограниченных возможностях при отсутствии подключения к сети Интернет.

Настоящий проект направлен на демонстрацию возможности создания подобных систем с использованием открытого программного обеспечения и доступных на рынке электронных компонентов, и плат. Ключевым условием проекта является обеспечение надежной работы системы в условиях отсоединения от глобальной сети.

Целью данного проекта является разработка прототипа умного дома, обладающего способностью к автономной функциональности вне зависимости от подключения к интернет-инфраструктуре, и простота реализации, которая позволит упростить реализацию подобных проектов в будущем.

Для достижения поставленной цели перед проектной группой стоят следующие задачи:

1. Разработка спецификации базового набора функций "умного" дома, предусмотренных для реализации в рамках прототипа, с акцентом на обеспечение его автономности.
2. Формирование списка аппаратных компонентов, необходимых для сборки макета, включая микроконтроллеры, датчики, исполнительные механизмы и интерфейсы взаимодействия.
3. Выбор и адаптация программного обеспечения, которое будет выполнять функции центрального узла обработки запросов и координации работы устройств макета, с учетом требований к робастности и независимости от внешних сетей.



Реализация этих задач позволит создать масштабируемую и безопасную систему, которая может служить основой для последующей разработки полноценных решений в области интеллектуальных зданий.

В процессе работы над макетом было решено заложить следующий ряд функций, которые он должен реализовывать:

1. Создать регулируемое удаленно освещение;
2. Яркость света должна реагировать на данные присылаемые с датчика света;
3. Создать имитацию системы безопасности, используя RFID-сканер, для открывания двери макета;
4. Работа «умной» розетки;
5. Измерение температуры;
6. Вывод данных и осуществление функций управления на интерфейсе удобном пользователям.

Данный набор функций, относительно простой в реализации, но позволяет наглядно показать возможности систем типа «умный» дом.

Наибольшую сложность при выполнении проекта является создание брокера запросов, в системах Алиса от Яндекса, Маруся от VK и так далее, эту функцию выполняет удаленный сервер, но использование удаленного сервера невозможно если требуется обеспечить условие автономной работы всех систем. Поэтому одной из важных проблем, которая возникла в процессе проекта, стала проблема создания своего сервера. Данный сервер должен обрабатывать все запросы, собирать данные с датчиков, а также выдавать решение исходя из данных созданными этими датчиками. Подходов для решения задачи организации сервера запросов, на сегодня, существует достаточное количество, например в статье [2], авторы предлагают использовать для этой цели мини-компьютер. Также есть и реализации сервера на основе микроконтроллеров [3].

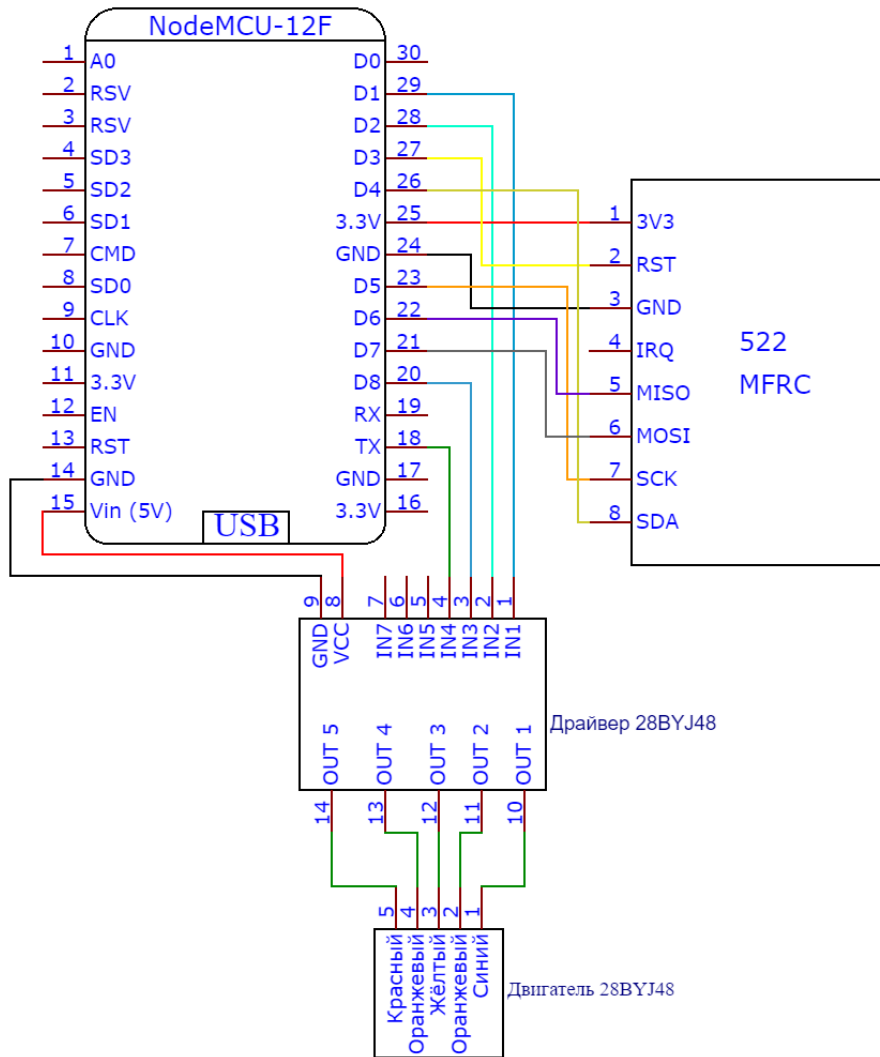
В данном проекте, в качестве сервера мы рассматривали три основных варианта: использовать микроконтроллер, использовать мини-компьютер, использовать стационарный ПК. В качестве основного варианта был выбран одноплатный компьютер Raspberry PI.

Реализация с микроконтроллером потребовала бы значительных доработок, что в свою очередь значительно усложняет проект. Ресурсы стационарного ПК просто избыточны для функций, описанных выше. Одноплатный компьютер обладает всеми необходимыми системными требованиями, также обладает портами для удобного подключения к различным системам, а также имеет в своем составе встроенный Wi-Fi адаптер, также стоит отметить, что изначально на него установлена операционная система Linux, которая является одной из самых распространенных серверных ОС мире.

Дальнейшей задачей стала разработка структурной схемы макета, а также списка элементов, которые будут отвечать за реализацию заложенных в проект функций. Ниже представлен список основных элементов:

- плата NodeMCU;
- RFID MFRC522;
- драйвер 28BYJ48;
- двигатель 28BYJ48;
- датчик освещённости BH1750;
- датчик температуры DHT11;
- релейный модуль;
- RGB WS2812B 8x1 лента;
- вилка и розетка.

На рис. 1 показана структурная схема соединения элементов.



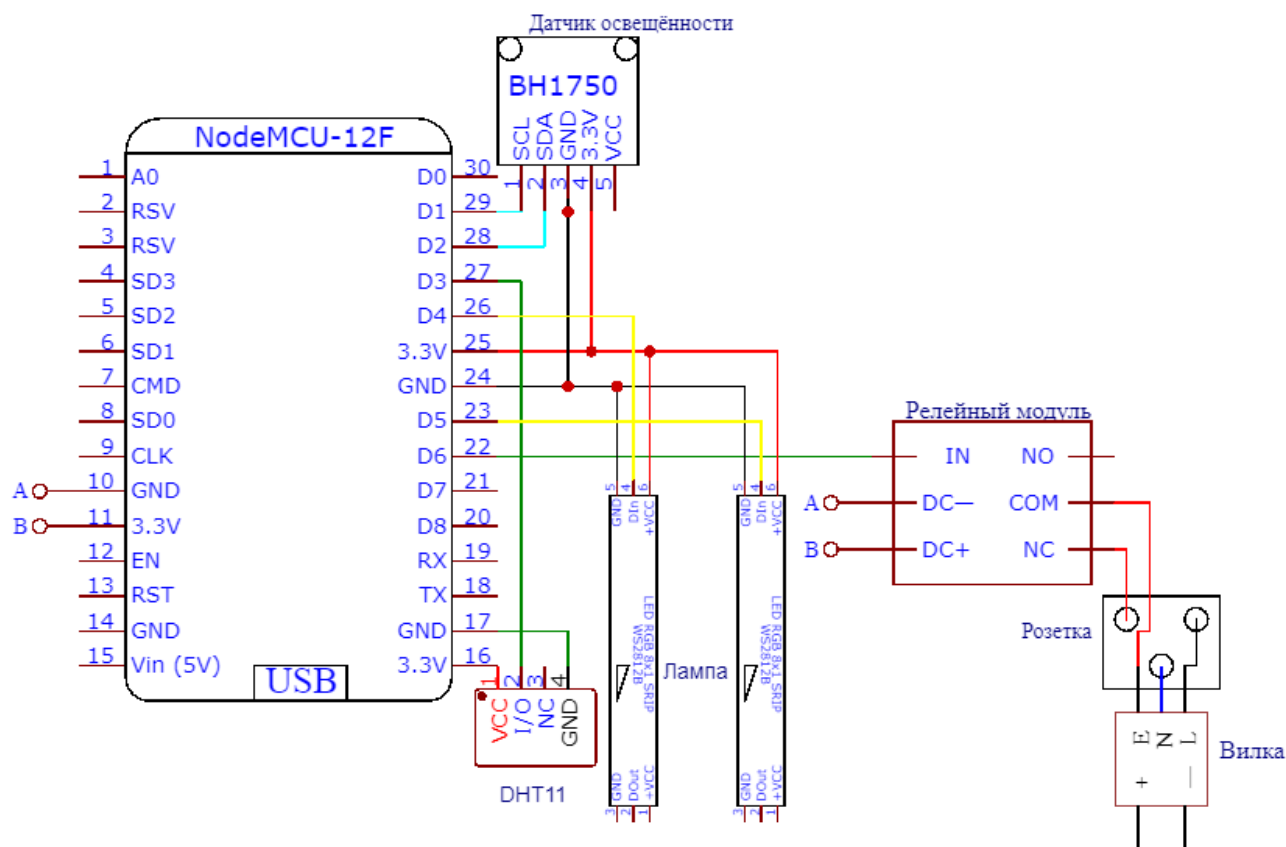


Рис. 1 структурная схема соединения элементов.

При выборе компонентов основной упор был сделан на доступность компонентов, так как одной из целей проекта была его простота реализации, как в плане электрических компонентов и датчиков, так и в плане программного обеспечения, где основной упор был сделан на продукты с открытым кодом.

При реализации нашего проекта мы остановились на ПО Vlynk, оно является полностью бесплатным, а также позволяет относительно несложно создавать свой аналог IoT приложения на смартфон, а также имеет встроенную поддержку всех основных видов мини-компьютеров и микроконтроллеров. Интерфейс ПО представлен на рис. 2.

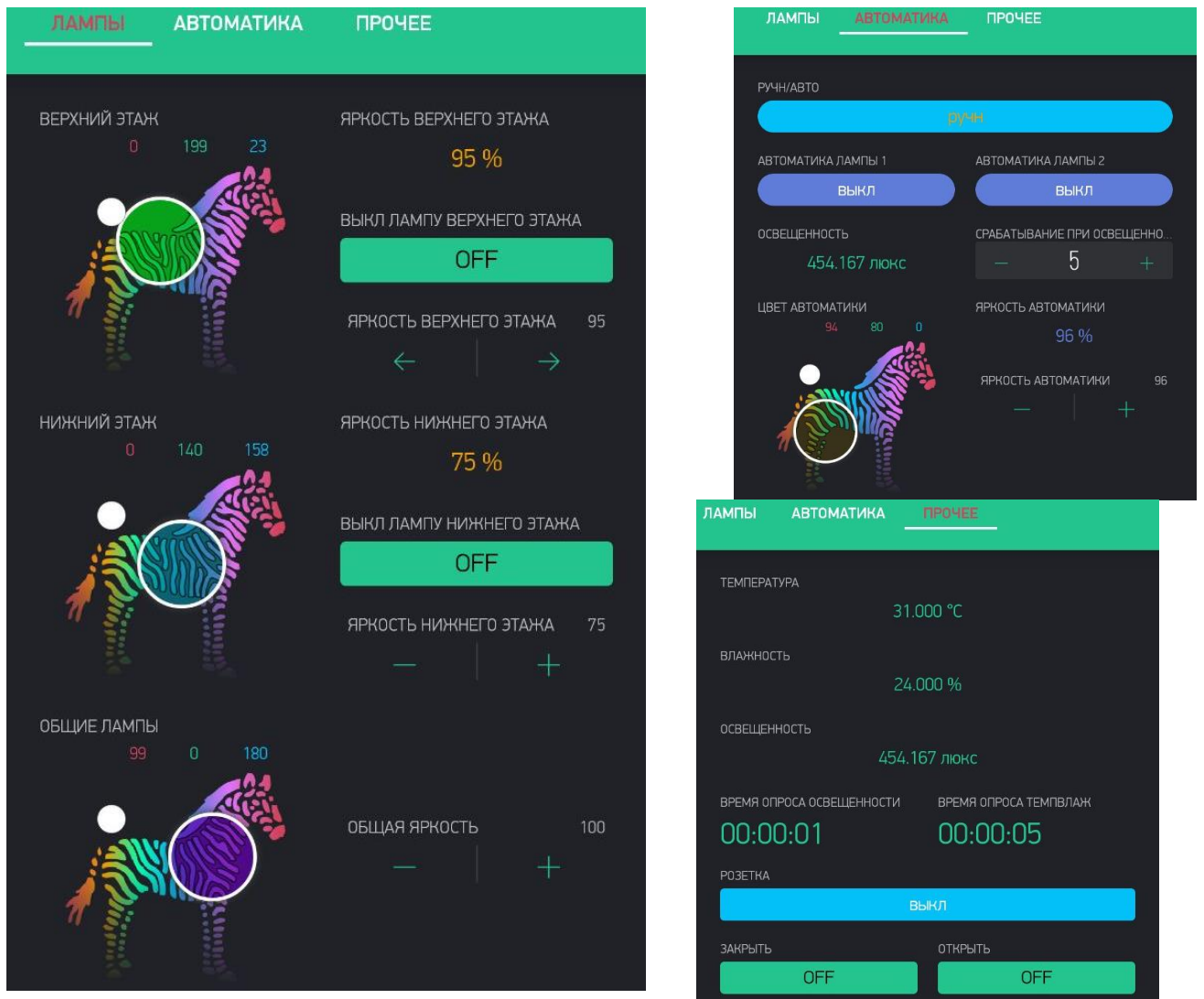


Рис 2 – Интерфейс Vlynk

Также стоит упомянуть, что корпус проекта выполнен с помощью 3D печати, с использованием PLA-пластика. Изображения 3D-моделей макета представлены на рис. 3 и 4.



Рис 3. – 3D модель макета (вид сзади)



Рис 4.- 3D модель макета (вид спереди)

#### Заключение.

В процессе реализации проекта был произведен выбор всех компонентов макета, в качестве сервера – брокера запросов был использован одноплатный компьютер Raspberry PI. Одним из условий проекта также было использование только плат, контроллеров и датчиков, находящихся в открытой продаже, а также только доступное ПО. В качестве технологии для локальной сети был выбран Wi-Fi, так как Raspberry PI имеет встроенный адаптер. Подобные проекты нацелены демонстрацию возможности реализации «умного» дома для студентов и позволяют заложить базовые навыки при работе с IoT системами.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Корнишин, М. А. «Умный дом» вместе с Яндекс Станцией Алиса / М. А. Корнишин // *Флагман науки*. – 2023. – № 9(9). – С. 446-450. – EDN VQPZDI.
2. Васильчиков, М. Г. Разработка веб-сервера для удаленного управления системой «Умный дом» / М. Г. Васильчиков, А. В. Клименко // *Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях : Материалы XXI Республиканской научной конференции студентов и аспирантов, Гомель, 19–21 марта 2018 года*. – Гомель: Гомельский государственный университет им. Франциска Скорины, 2018. – Р. 83-84. – EDN GLCOUI.
3. Сервер для системы "Умный дом" на базе микроконтроллера ESP32 / Е. Р. Захаров, А. Е. Курносенко, В. В. Леонидов, В. О. Семенякина // *Проектирование и технология электронных средств*. – 2020. – № 2. – С. 28-35. – EDN TFCENP.

## **ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В ВЕТЕРИНАРИИ**

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

Ключевые слова: нейронные сети, ветеринария.

В статье рассмотрены примеры нейронных сетей, которые могут быть использованы в ветеринарии: нейронная сеть для поиска животных, нейронная сеть для отслеживания поведения животных, нейронная сеть ChatGPT, сервис «Ветеринарный бот». Цель работы – показать, как нейронные сети могут быть применены в ветеринарии.

**I.I. Nurullin, A.V. Volynskaya**

## **THE USE OF NEURAL NETWORKS IN VETERINARY MEDICINE**

Ural State University of Railway Transport (USURT), Ekaterinburg, Russia

Keywords: neural networks, veterinary medicine.

The article discusses examples of neural networks that can be used in veterinary medicine: neural network for animal search, neural network for tracking animal behavior, ChatGPT neural network, “Veterinary Bot” service. There is also a list of how a neural network can be used in veterinary medicine. The purpose of the work is to determine how neural networks are used in veterinary medicine.

Нейросети проникли почти во все аспекты человеческой жизни. С помощью них можно упростить и ускорить множество процессов, в том числе, и в ветеринарии. Нейросеть может обрабатывать огромные пласты информации, а также вести постоянный мониторинг, позволяя, например, проводить анализ самочувствия питомца в реальном времени. Нейронные сети можно также использовать для поиска потерянных домашних животных. Этим вопросом занялись в рамках проекта PetSI (PetSearchInstrument): нейронная сеть получает на входе параметры, фото, адрес пропажи и т.д., и на основе сообщений о найденных или увиденных животных, предлагать наиболее возможные варианты нахождения питомца. Также в рамках проекта рассматривается и возможность поиска бездомным животным новых хозяев. На данный момент уже создано приложение, доступное для скачивания. Данный проект вносит вклад в ветеринарию, позволяя ускорить процесс поиска питомца, снижая вероятность болезни животного или получения им травмы [1].

Поведение животных также имеет большое значение в ветеринарии. Так, зная повадки животного, его образ жизни и предпочтения, можно составить рацион, определить особенности ухода или выявить отклонения в здоровье. Но постоянно наблюдать за животным сложно, и для этих целей можно использовать нейронные сети. Так, исследователи из Университета Дьюка и Гарвардского университета предоставили новую технологию для наблюдения за действиями животных, которая состоит из базы данных Rat 7M с использованием цветного видео и трехмерной сверточной нейронной сети. Технология заключается в том, что берутся кадры действий крыс, которые синхронизируются с цветным видео с помощью «захвата движения». Адаптация захвата проходит при помощи маркеров, прикрепленных к телам крыс. Так, нейросеть вычисляет трехмерные позиции животных из кадров, полученных с расставленных вокруг испытуемого камер захвата движения и видеокamer. По итогу исследователи добились того, что обученная нейросеть смогла на паре испытуемых без датчиков распознать движения крыс. Эту сеть можно также обучить и опознаванию других животных [2].

Использование ChatGPT может помочь не столько ветеринарам, сколько владельцам питомцев. Так, нейросеть может найти ответы на многие вопросы владельцев домашних

животных. К примеру, узнать про особенности своего питомца, что поможет в его воспитании или уходе за ним. Допустим, если у хозяина есть в доме растения, можно спросить, какие из них могут быть опасны и даже ядовиты для питомца. Также, в случае наступившей травмы или ухудшения здоровья, можно принять первые меры по оказанию помощи или подготовиться к походу к ветеринару. Дополнительно можно задать ChatGPT вопросы, касающиеся питания: выбор корма, подходящего породе, возрасту и состоянию здоровья питомца. Также ChatGPT может давать рекомендации на основании предоставленных анализов. Но результаты не всегда корректны, да и сама нейросеть может ошибочно прочесть введенные данные, особенно если загружать данные в виде картинки. Однако, использование ChatGPT не заменит поход к ветеринару, поэтому сильно полагаться в серьезных вопросах на нейросеть пока нельзя [3].

Выше уже упоминалась возможность постановки диагноза посредством предоставления нейросети анализов, но ChatGPT на этом не специализируется. Существует сервис «Ветеринарный бот», который анализирует сообщения фермеров и находит среди них самые вероятные болезни скота, но работает он только на основе текстовых сообщений, что является его главным минусом, как и то, что этот сервис предназначен только владельцам сельского скота [4].

Есть также нейронные сети для распознавания породы животного, но зачастую, пользы от них не много. Это связано с тем, что доля породистых животных мала, и зачастую, каждое такое животное имеет паспорт, который подтверждает, что данный питомец - породистый. Сама нейронная сеть, конечно, распознает ту или иную породу, но само животное может и не быть породистым, а просто иметь схожесть по внешним признакам. И в этом случае сложно говорить, присутствуют ли черты и особенности той породы, на которую похож питомец, фото которого пропускали через нейронную сеть.

Применение нейронных сетей в ветеринарии имеет огромное значение. Их использование не только облегчает процесс лечения, но и ускоряет различные времязатратные процессы. Так, использование нейронных сетей позволит:

1. Диагностировать болезни – позволит использовать нейросеть для анализа медицинских данных, к примеру, результатов кровных испытаний, изображений рентгеновских снимков;
2. Прогнозировать заболевания – можно использовать для анализа исторических данных и прогнозировать возможные риски и вероятности появления той или иной болезни;
3. Контролировать здоровье – осуществлять мониторинг здоровья и физического состояния животных, на основе собранных данных о пульсе, дыхании, активности, питания и т.д.;
4. Помогать в хирургии – нейронные сети могут проводить анализ медицинских снимков, к примеру, результатов КР. МРТ, УЗИ, с целью помощи в операциях на животных
5. Вести поддержку клиентов – позволит давать автоматические ответы на вопросы клиентов, предоставлять информацию о заболеваниях и процессе лечения животных, а также, разработке персональных планов лечения и ухода за конкретным питомцем.

В итоге, нейросети позволяют не только ускорить и автоматизировать процессы обслуживания питомцев, но и кардинально улучшить качество услуг. Сами нейронные сети тоже не стоят на месте, исследователи создают новые нейросети, что в будущем позволит усовершенствовать уже имеющиеся технологии. К примеру, тот же PetSI, сможет отслеживать питомцев по камерам в реальном времени, а не давать наводки на возможное местоположение питомца по фото. Также, можно сказать и про нейросеть по распознаванию движений, что может дополнить предыдущую, выявляя дальнейший путь по движениям и окружению животного. И если развить технологию на столько, что можно будет создать базу данных поведения каждого животного, это предоставит огромные возможности исследователям и ветеринарам, позволяя улучшить технологии лечения и ухода домашних, и даже диких животных.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Собаку съел на нейронных сетях // [Электронный ресурс] / URL: <https://habr.com/ru/articles/459988/>
2. DANNCE – сверточная нейронная сеть для характеристики поведения животных // [Электронный ресурс] / URL: <https://neurohive.io/ru/novosti/dannce-animals/>



3. Применение современных технологий для владельцев домашних животных // [Электронный ресурс] / URL: <https://dzen.ru/a/ZerE2grFsySTm3aB>
4. Редкий кейс: как мы учили нейросети определять болезни животных // [Электронный ресурс] / URL: <https://habr.com/ru/companies/rshb/articles/646179/>



## ПРИМЕНЕНИЕ ПРОТОКОЛОВ FTP, WebDAV В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОАО «РЖД»

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

Ключевые слова: информационные системы, протоколы передачи информации, протокол FTP, протокол WebDAV.

В статье представлен анализ и особенности применения протоколов передачи данных, FTP и WebDAV в информационных системах ОАО «РЖД». Целью работы было - провести обзор протоколов передачи данных, рассмотреть особенности настройки в железнодорожных информационных системах.

A.V. Rumyantseva, E.S. Bogdanova

## APPLICATION OF FTP AND WebDAV PROTOCOLS IN INFORMATION SYSTEMS OF RUSSIAN RAILWAYS

Ural State University of Railway Transport, Yekaterinburg, Russia

Keywords: information systems, information transfer protocols, FTP protocol, WebDAV protocol.

The article presents an analysis and features of the use of data transfer protocols, FTP and WebDAV in the information systems of Russian Railways. The purpose of the work was to review data transmission protocols, to consider the features of configuration in railway information systems.

Способы организации общественного производства и жизнеобеспечения определяют технологический уклад в обществе формируя закономерную последовательность технологических революций. В работах профессора А.И. Ракитова, создателя и научного руководителя центра информатизации, социально-технологических исследований и науковедческого анализа, было показано влияние информационной революции на технологическую, где информационная революция – это преобразование общественных отношений из-за кардинальных изменений в сфере обработки информации [1]. Следует отметить влияние интеграционных процессов, происходящие в информационных системах предприятия, на совершенствование информационного обмена внутри производственного процесса. Рассмотрим на примере использования протоколов FTP и WebDAV, их влияние на организацию информационного обмена между различным оборудованием, клиентами и сервисами.

FTP (File Transfer Protocol) – протокол передачи файлов по сети. Определён в RFC 959. Это стандартный механизм для копирования файла от одного хоста к другому, реализующий данную задачу при организации сетей и взаимодействия между ними. Является клиент – серверным, при этом отличается от других приложений тем, что он устанавливает два соединения между хостами. Одно соединение применяется для передачи данных, другое — для управления информацией (команды и отклики). Разделение команд и передачи управляющих данных делает FTP более эффективным. Управление соединением использует очень простые правила для связи. Нам нужна для передачи только линия команд или линия откликов. С другой стороны, соединение для данных нуждается в более сложных правилах из-за разнообразия типов данных. Имеет шесть классов команд, посылаемых клиентом для установления связи с сервером: доступа, управления файлом, определения порта, передачи файла и прочие. Отклики посылаются от сервера к клиенту в течение установления соединения. Имеет три типа файлов для передачи: копированный от сервера к клиенту, копированный от клиента к серверу. Список директорий или имена файлов, посылаемые от сервера к клиенту. Большинство операционных систем обеспечивают

дружественный пользователю интерфейс между FTP и пользователем. Анонимный FTP обеспечивает метод для общедоступного доступа к файлу на удаленных сайтах [2].

WebDAV (Web Distributed Authoring and Versioning) - это протокол файлового обмена, основанный на HTTP и XML, легко расширяемый, работающий во всех операционных системах. Позволяет пользователям удаленно управлять и совместно использовать файлы на веб-сервере. Работает по той же связи, что и FTP, и предоставляет возможность создания, изменения и удаления файлов на сервере, а также управление версиями файлов и блокировку доступа к ним для предотвращения конфликтов при одновременном редактировании. Может работать с объектами операционных систем, а не только с файлами и данными [3].

В информационных системах компании ОАО «РЖД» эти протоколы используются для ускорения процессов автоматизированной передачи данных на сервера управления информационного обмена между аппаратными средствами. Так как в настоящее время проявляется большой спрос на централизованное хранение, а также резервное копирование различного рода информации, то совместное использование данных протоколом можно рассмотреть при использовании в информационных системах ОАО «РЖД».

FTP в системах ОАО «РЖД» применяется, для обеспечения безопасной и универсальной передачи больших объемов данных между городскими подразделениями компании, а иногда между партнерами. В качестве передаваемых данных выявляют: технические и эксплуатационные чертежи различного назначения, отчеты, графики технического обслуживания как железнодорожных станций, так и самих составляющих – поездов. Пример реализации передачи информации по протоколу FTP на сервера ОАО «РЖД» представлен на рисунках 1,2.

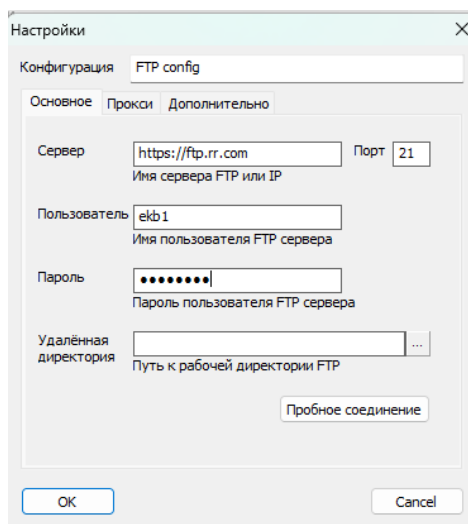


Рисунок 1. Настройки соединения сервера для передачи файлов по протоколу FTP на сервера ОАО «РЖД»

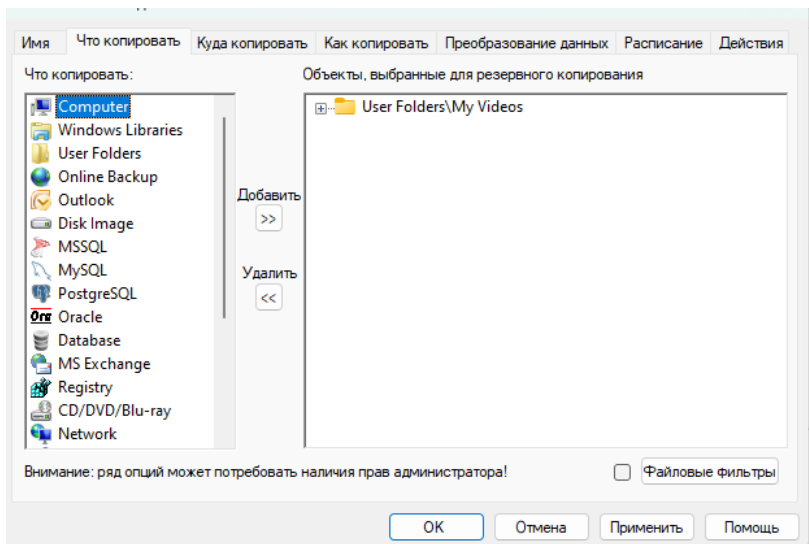


Рисунок 2. Выбор передаваемых файлов в каталоге по протоколу FTP на Сервера ОАО «РЖД»

Протокол WebDAV в информационных системах ОАО «РЖД» применяются для обеспечения совместного редактирования, использования и контроля версий документов, файлов, объектов системы. WebDAV позволяет упростить процесс создания документов в компании, а также централизацию их хранения и согласованность между всеми подразделениями внутри компании.

Пример реализации протокола WebDAV на серверах ОАО «РЖД» представлен на рисунках 3,4

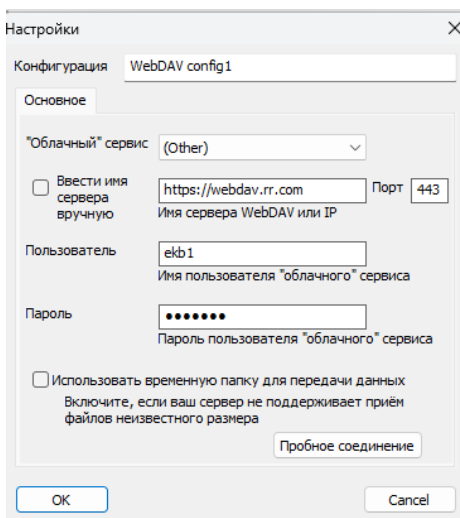


Рисунок 3. Настройки соединения сервера по протоколу WebDAV на сервера ОАО «РЖД»

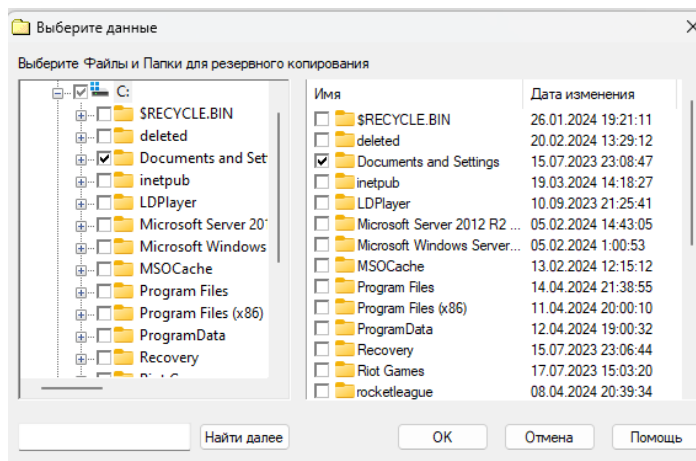


Рисунок 4. Выбор каталога/файлов для резервного копирования по протоколу WebDAV на сервера ОАО «РЖД»

В общей характеристике и применении протоколов передачи информации в информационных системах в ОАО «РЖД» является положительной стороной, это совершенствует скорость передачи и работы с файлами, объектами. Важно уточнить, что данная технология важна для их территориально разделенных подразделений, поскольку файлами могут оперировать на любой станции. Также стоит учесть, что внедрение и реализация данных протоколов не требует финансовых вложений и является легальной в стране реализации своих услуг, что является положительным фактором.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Гафнер В. В. Информационная безопасность / В. В. Гафнер. – Ростов на Дону: Общество с ограниченной ответственностью «Феникс», 2010. – 324 с. ISBN 978-5-222-17389-3.
2. Берлин, А. Н. Основные протоколы Интернет : учебное пособие / А. Н. Берлин ; А. Н. Берлин. – Москва : Интернет-Ун-т информ. технологий, 2008. – 503 с. – (Основы информационных технологий). – ISBN 978-5-94774-884-0.
3. \_WebDAV / [Электронный ресурс] – Режим доступа. <https://www.oslogic.ru/knowledge/27/webdav/#:~:text=WebDAV%20%E2%80> (дата обращения 09.04.2024).
4. Ведерников, В. К. Разработка WEBDAV сервера с деревом виртуальных свойств под управлением операционной системы Android / В. К. Ведерников // ТЕОРИЯ и ПРАКТИКА СОВРЕМЕННОЙ НАУКИ : сборник статей VIII Международной научно-практической конференции. В 2 ч., Пенза, 25 июня 2022 года. Том 1. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. – С. 55-58.

## **ИННОВАЦИИ В ОБЛАСТИ ЦИФРОВОЙ ПЕРЕДАЧИ ДАННЫХ: КВАНТОВЫЕ ТЕХНОЛОГИИ**

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

Ключевые слова: квантовые биты, квантовые технологии, квантовый интернет, угрозы цифровой передачи данных, цифровая передача данных.

В статье рассматривается актуальная тема инноваций в области цифровой передачи данных, с фокусом на использовании квантовых технологий. Описываются основные принципы квантовой передачи данных, ее преимущества по сравнению с классическими методами передачи. Также рассматриваются текущие исследования и разработки в области квантовых технологий и их потенциальное влияние на будущее развитие цифровой коммуникации.

**K.L. Kostyuchenko, M.A. Sereda**

## **INNOVATIONS IN DIGITAL DATA TRANSMISSION: QUANTUM TECHNOLOGIES**

Ural State University of Railway Transport (USURT), Ekaterinburg, Russia

Keywords: quantum bits, quantum technologies, quantum internet, threats of digital data transmission., digital data transmission.

The article deals with the current topic of innovations in the field of digital data transmission, focusing on the use of quantum technologies. The basic principles of quantum data transmission, its advantages over classical transmission methods are described. Current research and development in the field of quantum technologies and their potential impact on the future development of digital communication are also discussed.

Цифровая передача данных является неотъемлемой частью современного мира, она позволяет нам обмениваться информацией быстро и эффективно. Однако, с развитием технологий появляются новые вызовы и потребности в более продвинутых методах передачи данных. В этой статье будет рассмотрена инновация в области цифровой передачи данных – квантовые технологии.

Создание квантовых компьютеров ставит под вопрос надежность существующих методов шифрования данных, передаваемых по каналам связи. Квантовый компьютер представляет собой обычный компьютер, в котором информация обрабатывается с помощью кубитов – квантовых битов (рис. 1).

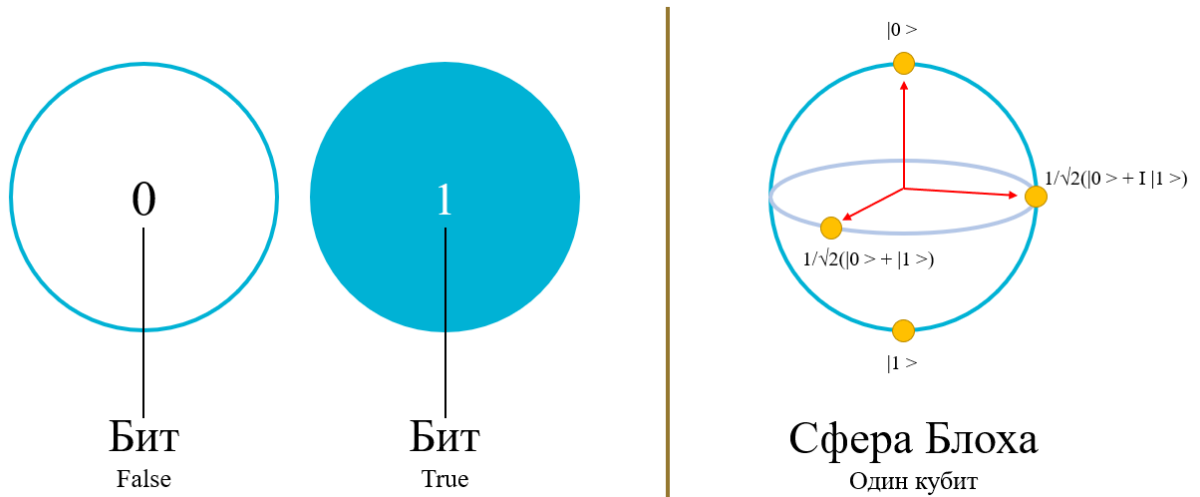


Рис. 1. Сравнение битов с кубитами.

Кубит является аналогом нулей или единиц, только квантовые биты реализованы с помощью квантовых частиц (фотонов, ионов, ядер атомов), которые находятся в суперпозиции [1]. Вычислительной мощности данных устройств хватит для взлома основного алгоритма шифрования RSA. Поэтому нынешняя защита данных, реализованная с помощью обычных компьютеров, перестанет работать. Пароли любой длины и сложности будут взломаны методом подбора за микросекунду. Данная перспектива требует поиска нового метода цифровой передачи информации и самый реалистичный вариант – квантовая связь.

Можно сделать вывод, чтобы добиться безопасной передачи конфиденциальной информации, нужно использовать те же кубиты. Особенностью данной единицы измерения информации является состояние суперпозиции до момента измерения. Данная особенность позволяет системе определять изменения в переданном сообщении, то есть при съеме информации злоумышленником кубиты выходят из состояния суперпозиции и система получает неполноценный квантовый фрагмент информации, что сигнализирует о несанкционированном доступе к каналу передачи.

Для реализации данного метода передачи информации используется квантовый интернет. Квантовый интернет является совокупностью квантовых дата-центров, которые способны обрабатывать передаваемую информацию в виде квантовых состояний [2].

В основе понимания работы квантового интернета лежит понятие «запутанность». Данный термин утверждает, что, если две частицы связаны друг с другом, они будут иметь одинаковые характеристики, даже находясь на большом расстоянии. Например, их спины, или направления вращения, будут совпадать. Причины возникновения такой «запутанности» частиц разнообразны, но в основе лежит тот факт, что поведение этих частиц описывается одной волновой функцией. Вот только до момента их измерения мы не можем предсказать, какая именно это функция. Значит, пока не будет измерена одна из частиц, нельзя точно определить состояние другой. Интересно, что характеристики одной частицы могут быть определены путем измерения параметров другой, что открывает возможности для уникальных квантовых вычислений (рис. 2).

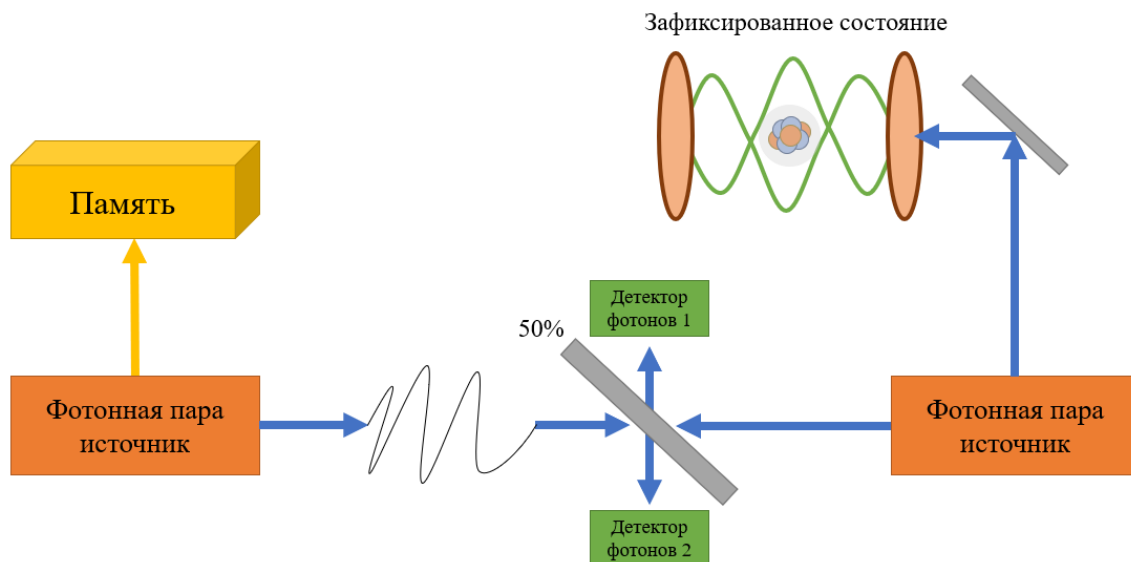


Рис. 2. Принцип работы квантового интернета

Пока обычные компьютеры передают информацию с использованием битов – нулей и единиц, квантовые компьютеры работают с кубитами. Кубиты обладают свойством квантового параллелизма, что позволяет им телепортировать данные через свои квантовые состояния. Этот принцип телепортации информации через кубиты может полностью изменить наше представление о передаче данных и обеспечении безопасности в сети.

На данный момент нельзя точно сказать, на что будет способен квантовый интернет. В отличие от обычного интернета технология на данном этапе развития не подразумевает привычные нам WEB-сайты, сервисы и приложения. Для обработки такой информации намного выгодней использовать обычный интернет. Данная инновация рассчитана на решение следующих проблем:

- Безопасность передачи данных: создание нового интернета становится все более неотложной задачей из-за необходимости обеспечить безопасность передачи данных от перехватов и дешифровки квантовыми компьютерами. QKD, технология квантового распределения ключей, предлагает несколько вариантов, таких как протокол BB84, протокол B92, протокол E91 и другие. Основная идея заключается в передаче информации по квантовому каналу, что обеспечивает проверку данных и их надежность.

- Сенсорные сети: использование квантового интернета в передаче данных между датчиками без необходимости преобразования в классический формат уже нашло свое применение в различных областях, включая исследования в области физики элементарных частиц. Усовершенствование точности научных приборов, работающих с квантовыми объектами, является значительным достижением. Также, использование квантового интернета в телескопах для создания запутанности между датчиками может значительно улучшить качество изображений, получаемых при изучении космических объектов.

- Квантовая обработка данных и вычисления: объединение квантовых компьютеров в сеть позволяет значительно увеличить вычислительную мощность без увеличения затрат на создание новых устройств. Машина, состоящая из разнообразных квантовых компьютеров, размещенных по всему миру, способна работать как единое целое. Это позволяет не только сократить издержки, но и увеличить количество кубитов, используемых в общих вычислениях.

Ученые пока еще не смогли создать надежную систему квантовой связи в целом. Однако в небольших масштабах уже имеются значительные достижения. Например, в декабре 2023 года коллектив ученых из Германии, Испании и ЮАР провели успешный эксперимент с двумя связанными фотонами, с помощью которых была передана информация через квантовую сеть, достаточная для создания изображений. Был разработан метод упаковки данных в спины и их производные, что позволяет собирать биты и даже байты информации на другом конце провода. Практическая возможность безопасной передачи картинок через интернет уже налицо, не говоря

уже о паролях, пин-кодах и небольших текстовых файлах. Впервые в истории в декабре 2023 года Россия и Китай провели успешный эксперимент по передаче информации с использованием квантовой связи на расстояние в 3800 километров [3]. Участниками проекта стали университет науки и технологий Китая и Институт физики и квантовой инженерии НИТУ МИСиС. Для этого уникального эксперимента был задействован китайский спутник Mozi, а в России был разработан и установлен первый в стране квантовый приемник, способный обрабатывать данные о поляризационных состояниях фотонов с китайского спутника.

Кроме вышеупомянутого проекта в России развиваются менее масштабные квантовые сети для связи между городами. Развитие проектов в данной области поручены ОАО «РЖД». Так в 2021 году на основе магистральных оптоволоконных каналов был создан пилотный участок квантовой сети Москва – Санкт-Петербург длиной более 700 км (самый большой в Европе). В настоящее время произошло соединение Москвы с Нижним Новгородом, заканчивается – с Казанью, Воронежем и Ростовом-на-Дону с общей протяжённостью новых сегментов 1400 км. Уже скоро РЖД планирует протестировать квантовую связь между «Ласточкой» с функцией «автоматинист» и центром управления движением на полигоне в Москве. К 2030 году РЖД планирует превысить показатель в 15 тысяч километров протяженности квантовых сетей. Высокий интерес к квантовым технологиям уже проявили Газпромбанк, Сбербанк, МТС и Ростелеком [4].

Так как быстрый и повсеместный переход на квантовую коммуникацию для организаций невозможен, ученые из России поставили цель: создать новый метод криптозащиты для устойчивости обычных сетей к взлому с использованием суперкомпьютеров. И уже в марте 2024 года кампания «Криптонит» представила криптографический механизм под названием «Кодиеум» [5]. На данный момент проект находится в разработке методических рекомендаций по стандартизации, но программная реализация данного механизма отсутствует. «Кодиеум» работает на основе невозможности решения NP задач. NP задача в криптографии представляет из себя класс сложных задач, для которого нет эффективного вычислительного алгоритма, только при наличии решения можно проверить его корректность, поэтому данный метод способен повысить криптостойкость каналов передачи информации от банального перебора вариантов суперкомпьютером.

Подводя итоги, можно сказать, что квантовые технологии – прорыв в сфере телекоммуникации, т.к. квантовые сети обеспечивают высокоскоростную, а главное защищенную передачу конфиденциальной информации. Инвестиции и стремительный темп развития данной технологии показывает, что квантовая передача данных является востребованной как для государства, так и для предприятий. Достижение квантового превосходства становится необходимым элементом развития страны.

#### СПИСОК ЛИТЕРАТУРЫ:

1. Как устроен и зачем нужен квантовый компьютер [Электронный ресурс]. – Режим доступа: <https://thecode.media/quantum/> .
2. От кванта до сети [Электронный ресурс]. – Режим доступа: <https://ria.ru/20231120/internet-1909895277.html> .
3. Физики из России и Китая впервые совместно использовали квантовый спутник связи [Электронный ресурс]. – Режим доступа: [https://nauka.tass.ru/nauka/19433401?utm\\_source=yandex.ru&utm\\_medium=organic&utm\\_campaign=yandex.ru&utm\\_referrer=yandex.ru](https://nauka.tass.ru/nauka/19433401?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru) .
4. Магистральная квантовая сеть РЖД: к 2030 году будет построено 15 тысяч км [Электронный ресурс]. – Режим доступа: <https://rzddigital.ru/events/k-2030-godu-rzhd-postroit-15-tys-km-kvantovykh-setey/> .
5. В России разработан криптографический механизм, способный выдерживать атаки квантовых компьютеров [Электронный ресурс]. – Режим доступа: [https://www.cnews.ru/news/top/2024-03-25\\_kriptologi\\_rabotayut\\_na\\_operezhenie](https://www.cnews.ru/news/top/2024-03-25_kriptologi_rabotayut_na_operezhenie) .



## СТЕГАНОГРАФИЯ В СОВРЕМЕННЫХ КИБЕРАТАКАХ

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

Ключевые слова: стеганография, сокрытие данных, защита информации, информационная безопасность.

В статье приведена теоретическая часть по стеганографии, приведены примеры использования стеганографии, рассмотрены стеганографические методы и алгоритмы, примеры современных программ и инструментов для кибершпионажа.

К.М. Tupitsyn

## STEGANOGRAPHY IN CONTEMPORARY CYBERATTACKS

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

Keywords: steganography, data concealment, information protection, information security.

The article provides a theoretical part on steganography, provides examples of the use of steganography, considers steganographic methods and algorithms, examples of modern programs and tools for cyber espionage.

Стеганография – это практика отправки данных в скрытом формате, при которой сам факт отправки данных скрывается. Слово стеганография представляет собой комбинацию греческих слов *στεγανή* (стеганос), означающих «покрытый, скрытый или защищенный», и *γράφειν* (графейн), означающих «письмо» [1].

В отличие от криптографии, которая скрывает содержание секретного сообщения, стеганография скрывает сам факт передачи сообщения. Концепция стеганографии была впервые представлена в 1499 году, но сама идея существует с древних времен. Есть истории о методе, который применялся в Римской империи, когда рабу, выбранному для передачи секретного послания, выбривали наголо голову и вытатуировывали на коже послание. Когда волосы гонца отрастали, его отправляли на задание. Получатель снова побрил посылному голову и прочитал сообщение.

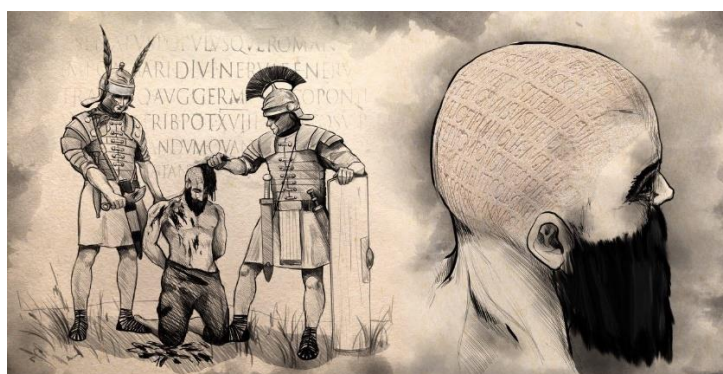


Рисунок 1 – Пример секретного послания

При стеганографии используются следующие определения:

– полезная нагрузка: информация, которая должна быть скрыта и тайно отправлена, или данные, передаваемые скрытым образом;

- носитель (стего–контейнер): любой объект, в который тайно встроена полезная нагрузка;
- стего–система: методы и средства, используемые для создания скрытого канала передачи информации;
- канал: канал передачи данных, по которому передается носитель;
- ключ: ключ, используемый для извлечения полезной нагрузки из носителя (применяется не всегда).

Стеганография активно развивалась на протяжении всего 20–го века, как и стеганоанализ, или практика определения факта передачи скрытой информации внутри носителя. Однако сегодня наметилась новая опасная тенденция: стеганография все чаще используется субъектами, создающими вредоносные программы и инструменты кибершпионажа. Большинство современных решений для защиты от вредоносных программ практически не обеспечивают защиту от стеганографии, в то время как любой носитель, на котором можно тайно перевозить полезную нагрузку, представляет потенциальную угрозу. В нем могут содержаться данные, утекающие с помощью программ–шпионов, связь между вредоносной программой и ее C&C или новое вредоносное ПО.

Научно разработаны и протестированы различные стеганографические методы и алгоритмы. Описание некоторых из них приведено ниже.

В LSB–стеганографии полезная информация кодируется и передается в одном или нескольких младших битах несущей. Чем меньше количество битов, используемых для передачи полезной информации, тем меньше влияние на исходный сигнал несущей.

Стеганография с дискретным косинусным преобразованием или на основе DCT – это подтип LSB–стеганографии, который часто применяется на носителях формата JPEG (т.е. когда изображения в формате JPEG используются для передачи полезной нагрузки). В этом методе передаваемые данные тайно кодируются в коэффициентах DCT. При прочих равных условиях этот метод обеспечивает несколько меньшую пропускную способность для передачи данных; одна из причин этого заключается в том, что значения коэффициентов 0 и 1 не могут быть изменены, поэтому никакие данные не могут быть закодированы всякий раз, когда коэффициенты принимают эти значения.

Стеганография изображений на основе палитры – это, по сути, еще один подтип LSB–стеганографии, при котором передаваемые данные кодируются в младшие разряды палитры изображений, а не в разряды носителя. Очевидным недостатком этого метода является его низкая пропускная способность.

Использование служебных полей в форматах данных. Это относительно простой метод, при котором полезная информация встраивается в служебные поля заголовков перевозчика. Недостатками, опять же, являются низкая пропускная способность и низкая защита полезной нагрузки: встроенную полезную нагрузку можно обнаружить с помощью обычного программного обеспечения для просмотра изображений, которое иногда может отображать содержимое служебных полей.

Внедрение полезной нагрузки – это метод, при котором полезная нагрузка кодируется в носитель и после доставки декодируется с использованием алгоритма, известного обеим сторонам. Несколько полезных грузов могут быть независимо закодированы в один и тот же носитель при условии, что методы их внедрения ортогональны.

Широкополосные методы делятся на следующие типы:

- метод псевдослучайной последовательности, в котором секретный несущий сигнал модулируется псевдослучайным сигналом.

- метод скачкообразной перестройки частоты, в котором частота несущего сигнала изменяется в соответствии с определенным псевдослучайным законом.

- метод наложения – строго говоря, это не является правильной стеганографией и основано на том факте, что некоторые форматы данных содержат размер данных в заголовке, или на том факте, что обработчик таких форматов считывает файл до тех пор, пока он не достигнет отметки конца данных. Примером может служить хорошо известный метод RAR/JPEG, основанный на объединении файла изображения таким образом, что он состоит из раздела формата JPEG, за которым следует раздел архива RAR. Программа просмотра файлов в формате JPEG прочитает его до границы, указанной в заголовке файла, в то время как программа архивирования файлов в

формате RAR проигнорирует все, что находится до RAR! подпись, обозначающая начало архива. Таким образом, если такой файл открыть в программе просмотра файлов изображений, он отобразит изображение, а если открыть в RAR-архиваторе, то отобразится содержимое RAR-архива. Недостатком этого метода является то, что наложение, добавленное к сегменту носителя, может быть легко идентифицировано аналитиком, визуально просматривающим файл.

Стеганография используется в следующих вредоносных программах и инструментах кибершпионажа:

- Microcin (ОН же six little monkeys);
- NetTraveler;
- Zberp;
- Enfal (новый загрузчик называется Zero.T);
- Shamoon;
- KinS;
- ZeusVM;
- Triton (Fibbit).

Итак, почему авторы вредоносных программ все чаще используют стеганографию в своих разработках? Три основных причины:

- помогает им скрывать не только сами данные, но и тот факт, что данные загружаются и скачиваемый контент;
- помогает обойти системы DPI, что актуально для корпоративных систем;
- использование стеганографии может помочь обойти проверки безопасности продуктов anti-APT, поскольку последние не могут обрабатывать все файлы изображений (корпоративные сети содержат их слишком много, а алгоритмы анализа довольно дороги).

Для конечного пользователя обнаружение полезной нагрузки в носителе может оказаться нетривиальной задачей. В качестве примера давайте рассмотрим два изображения ниже. На одном изображен пустой носитель, а на другом - носитель с полезной нагрузкой. Мы будем использовать стандартное тестовое изображение Lenna. [2]



Рисунок 2 – Lenna

Размер обоих изображений составляет 786 486 байт, однако правое изображение содержит первые 10 глав романа Набокова «Лолита». [3]

Внимательно посмотрите на эти два изображения. Видите ли вы разницу? Они идентичны как по размеру, так и по внешнему виду. Однако одним из них является носитель, содержащий встроенное сообщение.

Проблемы очевидны:

Стеганография в настоящее время очень популярна среди разработчиков вредоносных и шпионских программ;

Средства защиты от вредоносных программ в целом и средства защиты периметра в частности мало что могут сделать с носителями, содержащими полезную информацию. Такие

носители очень трудно обнаружить, поскольку они выглядят как обычные файлы изображений (или файлы других типов).;

Все современные программы обнаружения с помощью стеганографии, по сути, являются проверенной концепцией, и их логика не может быть реализована в коммерческих средствах обеспечения безопасности, поскольку они работают медленно, имеют довольно низкую скорость обнаружения и иногда даже содержат математические ошибки (мы видели несколько случаев, когда это имело место).

#### СПИСОК ЛИТЕРАТУРЫ:

- 1 Steganography in contemporary cyberattacks [Электронный ресурс] // Режим доступа: <https://securelist.com/steganography-in-contemporary-cyberattacks/79276/>
- 2 The Lenna Story [Электронный ресурс] // Режим доступа: <http://www.lenna.org>
- 3 Стеганография в современных кибератаках [Электронный ресурс] // Режим доступа: <https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/>

## АВТОРЫ СТАТЕЙ

- БАИМОВ** Роман Ирекович студент ФГАОУ ВО «Южно-Уральский государственный университет (Национальный исследовательский университет)» (ФГАОУ ВО ЮУрГУ (НИУ)), г. Челябинск, Россия, [baimov.roman@internet.ru](mailto:baimov.roman@internet.ru)
- БАЙТЯКОВ** Никита Александрович студент Уральского государственного университета путей сообщения (УрГУПС), Россия, [Tekken25.04@mail.ru](mailto:Tekken25.04@mail.ru)
- БАТЕНКОВ** Кирилл Александрович д.т.н., профессор РТУ МИРЭА, г. Москва, Россия, [pustur@yandex.ru](mailto:pustur@yandex.ru)
- БАРАНОВ** Сергей Анатольевич к.т.н., доцент Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, [oda@urtisi.ru](mailto:oda@urtisi.ru)
- БАРБИН** Николай Михайлович д.т.н., 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](mailto:nmbarbin@mail.ru)
- БОГДАНОВА** Елена Сергеевна к.т.н., доцент Уральского государственного университета путей сообщения (УрГУПС), Россия, [ebogdanova@usurt.ru](mailto:ebogdanova@usurt.ru)
- БУДЫЛДИНА** Надежда Вениаминовна к.т.н., доцент, 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](mailto: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](mailto:bdi@urtisi.ru)
- ВОЛЫНСКАЯ** Анна Владимировна к.т.н., доцент Уральского государственного университета путей сообщения (УрГУПС), Россия, [Anna@usurt.ru](mailto:Anna@usurt.ru)
- ВОРОБЬЕВ** Алексей Андреевич студент магистратуры Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, [rcebod@gmail.com](mailto:rcebod@gmail.com)
- ГОРЛОВ** Николай Ильич д.т.н., профессор ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ), г. Новосибирск, Россия, [gorlovnik@yandex.ru](mailto:gorlovnik@yandex.ru)
- ГОНЧАРОВ** Даниил Андреевич магистрант кафедры инфокоммуникационных систем и сетей ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ), г. Новосибирск, Россия, [denn102@bk.ru](mailto:denn102@bk.ru)
- ЗЕЛЕНЦОВ** Борис Павлович д.т.н., профессор ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ), г. Новосибирск, Россия, [zelentsovb@mail.ru](mailto:zelentsovb@mail.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](mailto:zemsckov.alexander2016@yandex.ru)
- КАЗАНЦЕВ** преподаватель Уральского технического института связи и  
Михаил Юрьевич информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [m-kazantsiev@mail.ru](mailto:m-kazantsiev@mail.ru)
- КАМЕНСКОВ** преподаватель Уральского технического института связи и  
Александр Евгеньевич информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [sashakamenskov@mail.ru](mailto:sashakamenskov@mail.ru)
- КАРАНИН** студент Уральского технического института связи и  
Олег Евгеньевич информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [olkaranin@gmail.com](mailto:olkaranin@gmail.com)
- КВИТКОВА** старший преподаватель кафедры инфокоммуникационных  
Ирина Геннадьевна систем и сетей ФГБОУ ВО «Сибирский государственный  
университет телекоммуникаций и информатики», г.  
Новосибирск, Россия, [irin.creme@yandex.ru](mailto:irin.creme@yandex.ru)
- КОВАЛЕНКО** к.т.н., доцент Уральского государственного университета  
Владимир Николаевич путей сообщения (УрГУПС), Россия [VKovalenko@usurt.ru](mailto:VKovalenko@usurt.ru)
- КОРОБИЦЫН** студент магистратуры Уральского технического института  
Иван Владимирович связи и информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [kiv@urtisi.ru](mailto:kiv@urtisi.ru)
- КОНОВАЛОВ** студент Уральского технического института связи и  
Иван Сергеевич информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [mec@urtisi.ru](mailto:mec@urtisi.ru)
- КОСТЮЧЕНКО** к.т.н., доцент Уральского государственного университета  
Константин Леонидович путей сообщения (УрГУПС), Россия, [kkost2@yandex.ru](mailto:kkost2@yandex.ru)
- КРАСНЫХ** старший преподаватель Уральского технического института  
Сергей Юрьевич связи и информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [seregakrasnyh@yandex.ru](mailto:seregakrasnyh@yandex.ru)
- КУАНЫШЕВ** к.ф.-м.н., доцент Уральского технического института связи  
Валерий Таукенович и информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [kuan06@mail.ru](mailto:kuan06@mail.ru)
- КУДРЯВЦЕВА** студентка Уральского государственного университета путей  
Ксения Николаевна сообщения (УрГУПС), Россия,  
[Kseniakudruavtseva21@gmail.com](mailto:Kseniakudruavtseva21@gmail.com)
- КУЛИКОВ** стажер-исследователь кафедры инфокоммуникационных  
Иван Михайлович систем и сетей ФГБОУ ВО «Сибирский государственный  
университет телекоммуникаций и информатики», г.  
Новосибирск, Россия, [i9428020@yandex.ru](mailto:i9428020@yandex.ru)
- КУСАЙКИН** к.т.н., доцент кафедры многоканальной электросвязи  
Дмитрий Вячеславович Уральского технического института связи и информатики

(филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, [Kusaykin@mail.ru](mailto:Kusaykin@mail.ru)

**ЛОБУНЕЦ**  
Олег Дементьевич

д.т.н., 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](mailto:lod@urtisi.ru)

**МАЛКОВА**  
Ирина Андреевна

старший преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, [mia@urtisi.ru](mailto:mia@urtisi.ru)

**МЕЛЕНТЬЕВ**  
Олег Геннадьевич

д.т.н., профессор кафедры инфокоммуникационных систем и сетей ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики», г. Новосибирск, Россия, [melog@sibguti.ru](mailto:melog@sibguti.ru)

**МИНИНА**  
Елена Александровна

к.т.н., 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, [mea@urtisi.ru](mailto:mea@urtisi.ru)

**МИХЕЕВА**  
Светлана Валерьевна

студентка Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), Россия, [Mixeeva.svetlana@mail.ru](mailto:Mixeeva.svetlana@mail.ru)

**МУХАЧЕВ**  
Сергей Валентинович

к.ф.-м.н., доцент Уральского государственного университета путей сообщения (УрГУПС), Россия, [smuhachev@usurt.ru](mailto:smuhachev@usurt.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](mailto:Biveralexey@yandex.ru)

**НУРУЛЛИН**  
Ильнур Ильдусович

студент магистратуры Уральского государственного университета путей сообщения (УрГУПС), Россия, [ilnur.nurullin@list.ru](mailto:ilnur.nurullin@list.ru)

**ОВЧИННИКОВ**  
Дмитрий Александрович

старший преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, [oda@urtisi.ru](mailto:oda@urtisi.ru)

**ПЛЕХАНОВ**  
Савелий Михайлович

старший преподаватель Уральского технического института связи и информатики (филиала) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г. Екатеринбург, Россия, [saveli3898@gmail.com](mailto:saveli3898@gmail.com)

**РАГОЗИН**  
Андрей Николаевич

к.т.н., доцент ФГАОУ ВО «Южно-Уральский государственный университет (Национальный исследовательский университет)» (ФГАОУ ВО ЮУрГУ (НИУ)), г. Челябинск, Россия, [ragozinan@susu.ru](mailto:ragozinan@susu.ru)

**РУМЯНЦЕВА**  
Анастасия Валерьевна

студентка Уральского государственного университета путей сообщения (УрГУПС), Россия, [UserIT2020@yandex.ru](mailto:UserIT2020@yandex.ru)

- СЕРЕДА** студент Уральского государственного университета путей  
Максим Андреевич сообщения (УрГУПС), Россия, [masereda@mail.ru](mailto:masereda@mail.ru)
- СИДОРОВ** студент Уральского технического института связи и  
Владимир Сергеевич информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г.  
Екатеринбург, Россия, [wowa0904@yandex.ru](mailto:wowa0904@yandex.ru)
- ТАРАСОВ** доцент кафедры инфокоммуникационных технологий и  
Евгений Сергеевич мобильной связи 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](mailto:tes@urtisi.ru)
- ТАШКИНОВ** студент магистратуры Уральского технического института  
Илья Владимирович связи и информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г.  
Екатеринбург, Россия, [Ilyatkv@vk.com](mailto:Ilyatkv@vk.com)
- ТУПИЦЫН** преподаватель Уральского технического института связи и  
Константин Михайлович информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г.  
Екатеринбург, Россия, [kaillytop@gmail.com](mailto:kaillytop@gmail.com)
- ЧАДАЕВ** студент Уральского технического института связи и  
Дмитрий Валерьевич информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г.  
Екатеринбург, Россия, [htrd63@gmail.com](mailto:htrd63@gmail.com)
- ШЕСТАКОВ** старший преподаватель Уральского технического института  
Иван Игоревич связи и информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ), г.  
Екатеринбург, Россия, [ivansche2007@rambler.ru](mailto:ivansche2007@rambler.ru)
- ШУВАЛОВ** д.т.н., профессор ФГБОУ ВО «Сибирский государственный  
Вячеслав Петрович университет телекоммуникаций и информатики», г.  
Новосибирск, Россия, [shvp04@mail.ru](mailto:shvp04@mail.ru)
- ЮРЧЕНКО** старший преподаватель Уральского технического института  
Евгения Владимировна связи и информатики (филиала) ФГБОУ ВО «Сибирский  
государственный университет телекоммуникаций и  
информатики» в г. Екатеринбурге (УрТИСИ СибГУТИ),  
Россия, [jena23@mail.ru](mailto:jena23@mail.ru)
- ЯКОВЛЕВ** старший преподаватель ФГБОУ ВО «Сибирский  
Артём Сергеевич государственный университет телекоммуникаций и  
информатики», г. Новосибирск, Россия, [yakovlev-  
as@sibguti.ru](mailto:yakovlev-as@sibguti.ru)



**АВТОРСКИЙ УКАЗАТЕЛЬ  
THE AUTHOR'S INDEX**

Баимов Р.И.	6	Куликов И.М.	48
Байтяков Н.А.	11, 14	Кусайкин Д.В.	108
Батенков К.А.	18	Лобунец О.Д.	82
Баранов С.А.	100	Малкова И.А.	31
Барбин Н.М.	20, 71, 100	Мелентьев О.Г.	48
Богданова Е.С.	121	Минина Е.А.	58
Будылдина Н.В.	40, 44, 77	Михеева С.В.	58
Бурумбаев Д.И.	20	Мухачев С.В.	11
Вольнская А.В.	53, 118	Никитин А.С.	77
Воробьев А.А.	23	Нуруллин И.И.	118
Горлов Н.И.	67	Овчинников Д.А.	100
Гончаров Д.А.	48	Плеханов С.М.	112
Зеленцов Б.П.	28	Рагозин А.Н.	6
Земсков А.В.	31	Румянцева А.В.	121
Казанцев М.Ю.	37	Середа М.А.	125
Каменсков А.Е.	86	Сидоров В.С.	40
Каранин О.Е.	112	Тарасов Е.С.	77
Квиткова И.Г.	28, 62	Ташкинов И.В.	44
Коваленко В.Н.	103	Тупицын К.М.	129
Коробицын И.В.	112	Чадаев Д.В.	91
Коновалов И.С.	108	Шестаков И.И.	23, 58
Костюченко К.Л.	14, 125	Шувалов В.П.	28, 62
Красных С.Ю.	71	Юрченко Е.В.	86, 91
Куанышев В.Т.	71, 100	Яковлев А.С.	96
Кудрявцева К.Н.	53		