НАУЧНЫЙ ЖУРНАЛ

ТЕЛЕКОММУНИКАЦИИ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

№1-2021

(*Дата издания: апрель 2021 г.*)

Редакционная коллегия

Орлов Владимир Георгиевич (*Главный редактор*)
к.т.н., Главный специалист отдела организации научно-исследовательской работы студентов Московского технического университета связи и информатики «МТУСИ», Москва, Россия

Андреев Владимир Александрович
д.т.н., профессор, Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия

Зимин Игорь Викторович
к.т.н., доцент, заведующий кафедрой Телекоммуникаций института Электроники и Телекоммуникаций при Кыргызском государственном технический университете имени И.Раззакова, Бишкек, Кыргызстан

Маркосян Мгер Вардкесович
к.т.н., доцент, Ереванский НИИ средств связи, Ереван, Армения

Самойлов Александр Георгиевич
д.т.н., профессор, заместитель директора института информационных технологий и радиоэлектроники Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), Владимир, Россия

Рогачев Александр Александрович
д.т.н., в.н.с., Гомельский государственный университет имени Франциска Скорины, Гомель, Республика Беларусь

Суржиков Анатолий Петрович
д.ф.-м.н., профессор, Национальный исследовательский Томский политехнический университет, Томск, Россия

Титов Евгений Вадимович
к.т.н., профессор, Московский технический университет связи и информатики, Москва, Россия

УЧРЕДИТЕЛЬ:

ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ» (МТУСИ)

РЕДАКЦИОННАЯ ПОДГОТОВКА:

Отдел организации научно-исследовательской работы студентов (ОНИРС МТУСИ)

СОДЕРЖАНИЕ №1-2021

«Цифровые технологии радиосвязи и телерадиовещания»

«Сетевые технологии и системы телекоммуникаций»

«Информационные технологии и автоматизация процессов в системах связи»

СПОСОБ ПЕРЕХВАТА GSM-СИГНАЛОВ С ПОМОЩЬЮ SDR-ПЛАТФОРМЫ HACKRF ONE

Николаев Владимир Владимирович,
студент МТУСИ, Москва, Россия,
fredfred9033@mail.ru

Михайлов Вячеслав Эдуардович,
ассистент базовой кафедры ЦУиСЗИ института Кибернетики, РТУ МИРЭА, Москва, Россия,
vmikhaylov95@yandex.ru

Аннотация

В статье представлено описание характеристик устройства SDR HackRF One. В первой части статьи проведен анализ функциональных возможностей данного устройства, предложены меры предосторожности при использовании SDR HackRF One. Во второй части рассмотрены различные области применения данного устройства. В третьей части статьи обозначены проблемы стандарта GSM, в частности, алгоритма шифрования A5/1, приведен пример перехвата и расшифровки SMS-сообщения с помощью SDR-платформы HackRF One и специального программного обеспечения, написанного для данного устройства. Целью статьи является рассмотрение современных подходов к анализу радиосигналов при помощи технологии SDR.

Ключевые слова*: GSM, SDR, анализ трафика, зашифрованные данные, шифрование, злоумышленник, перехват, радиосигнал.*

SDR (программно-определяемая радиосистема) - это процесс создания/генерирования в компьютере характеристик будущей радиоволны (например, её частоты). После формирования в компьютерной программе сигнал отправляется на внешнюю плату, чтобы в дальнейшем быть переданным в качестве радиоволны [1]. Благодаря применению SDR-технологии возможно достичь большую гибкость в работе по сравнению с привычными аналоговыми устройствами формирования/демодуляции радиосигналов.

На этапах развития SDR-технологии можно выделить 3 поколения устройств:

1. SDR на базе звуковой карты. На сегодняшний день это самая старая модель на рынке, данный SDR передает сигнал на линейный вход по аудио кабелю, оцифровка же происходит на компьютере. Левый канал используется в качестве синфазного канала, правый – в качестве квадратурного канала, благодаря этому отсутствует необходимость в установке дополнительных драйверов. SDR определяется операционной системой компьютера как звуковая карта, но для приема радиосигналов требуется установка специализированного программного обеспечения.
2. SDR со встроенным АЦП. Такой тип SDR преобразует принятый аналоговый сигнал в цифровой вид для его последующей обработки на компьютере.
3. SDR со встроенным сверхбыстрым АЦП. Данный тип SDR имеет частоту семплирования входного аналогового сигнала порядка 100 млн семплов/с, что позволяет иметь ширину полосы пропускания, равную половине частоты дискретизации (согласно теореме Котельникова/Шеннона).

SDR переводит на новый уровень оборудование, которое раньше имело только аппаратную реализацию и нерегулируемую аппаратуру, в программно-определяемое [2].

Платформа SDR предоставляет широкие возможности по конфигурированию параметров и режимов работы. К примеру, для прослушивания радиоэфира на определенной частоте достаточно выбрать несущую частоту и смешать её с входным сигналом, остальные преобразования выполнятся программным обеспечением.

Цель SDR – получить аналоговый сигнал, преобразовать его в цифровой вид и передать на компьютер для последующей обработки. Для этого сигнал необходимо дискретизировать и квантовать.

Работать с SDR можно при помощи программы GNU Radio Companion. Данное ПО имеет интерфейс, алгоритмы в котором реализуются посредством соединения блоков, выполняющих заданные функции (например, функции модуляции/демодуляции) [2].

Пример окна программы GNU Radio Companion представлен на рисунке 1.

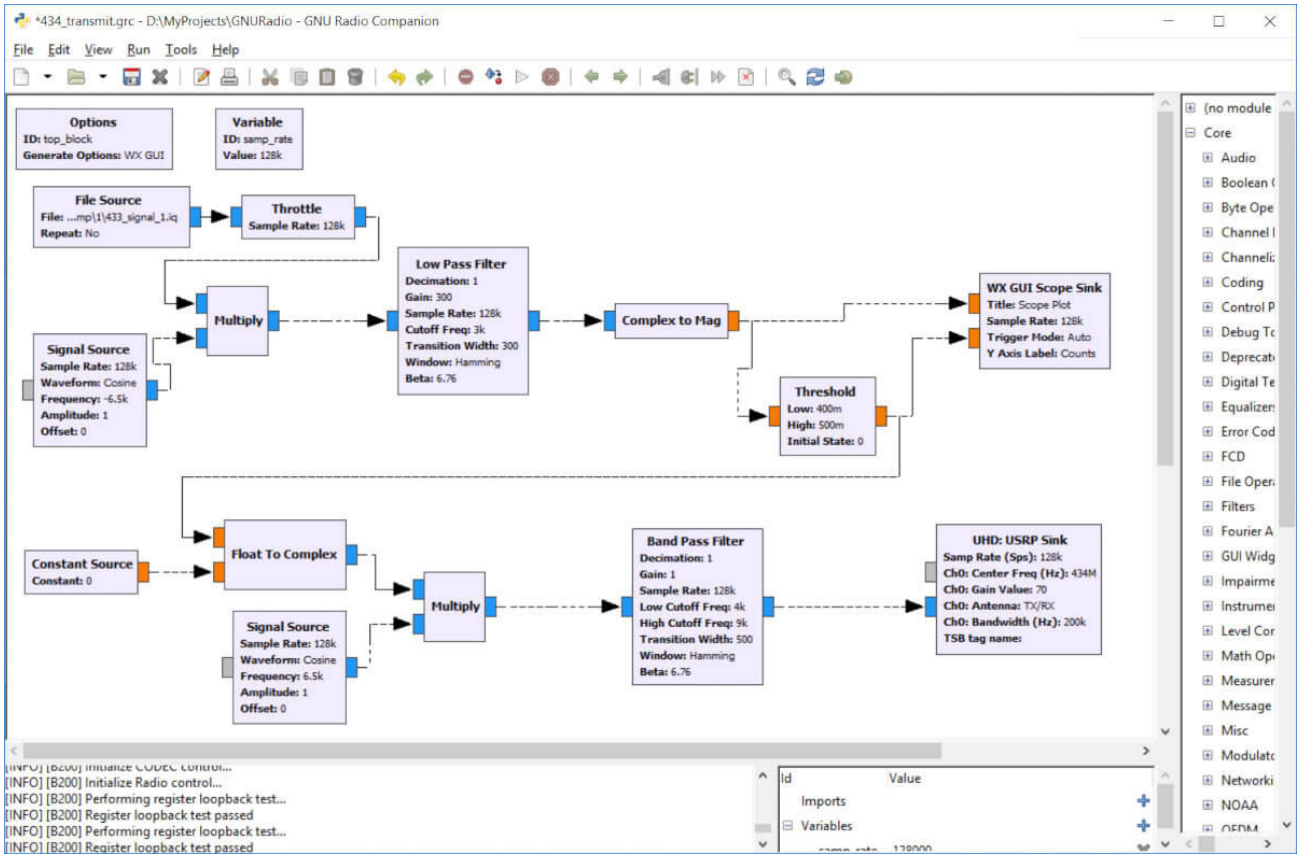


Рис. 1. Окно программы GNU Radio Companion

В GNU Radio Companion также предусмотрена возможность декодирования входных сигналов. Результат декодирования будет выводиться в нижнюю часть интерфейса программы.

HackRF One

Выбор платформы HackRF One для анализа радиосигналов обусловлен ее относительной дешевизной и сочетанием большого спектра возможностей.

HackRF One — это платформа Software Defined Radio с открытым исходным кодом [3]. Устройство является полудуплексным трансивером.

Характеристики HackRF One

HackRF One имеет следующие характеристики:

- **Диапазон частот**: 1 МГц ÷ 6 ГГц;
- **Ширина полосы пропускания**: 20 МГц;
- **Количество бит на входе/выходе**: 8 бит;
- **Гнездо антенны**: SMA-female;
- **Частоты дискретизации**: 8 ÷ 20 Msps;
- **Программно-контролируемая мощность порта антенны**: 50 мА на 3.3 В;
- **Штырьевой разъём** для подключения дополнительных плат для расширения функциональности;
- **Интерфейс хоста**: USB 2.0;

- **Совместимость с операционными системами**: Windows, Linux, Mac;
- **Мощность передатчика:** 30 мВт

Недостатки данного устройства:

1) Низкоскоростной интерфейс USB 2.0;
2) Ширина полосы захвата 20 MHz;
3) Встроенный передатчик может обеспечить передачу сигнала на расстояние не более 50 метров. Для передачи сигнала на большее расстояние необходимо дополнительно приобретать специальный усилитель, что приведет к дополнительным финансовым вложениям.

Преимущества данного устройства:

1) Дешевизна;
2) Доступность.
3) Прием аналоговых сигналов любой формы;
4) Открытые исходные коды ПО;
5) Совместимость с большим количеством ПО;
6) Совместимость с основными операционными системами: Windows, Linux, Mac.

Значение кнопок и индикаторов HackRF One

Устройство HackRF One имеет на плате 6 индикаторов, сигнализирующих о текущих режимах работы.

1) **3V3**
2) **1V8**
3) **RF**

Индикаторы отвечают за элементы питания схемы. При активной работе HackRF One все индикатора должны работать. Если один из них не работает, это значит, что в схеме имеется проблема, которую стоит устранить. Индикаторы могут отключаться при включении режима экономии энергии; 1V8 и RF отключаются, если HackRF One находится в режиме сна.

4) **USB** — указывает на то, что компьютер взаимодействует с HackRF One как с USB-устройством.
5) **RX** — операция приёма данных;
6) **TX** — операция передачи данных;

Индикаторы USB, RX, TX находятся под управлением ПО. Имеется возможность установить пользовательскую прошивку и переназначить функции индикаторов.

Устройство HackRF One имеет на плате 2 кнопки.

1) **RESET** — перезагрузка микроконтроллера;
2) **DFU** — режим обновления прошивки. HackRF имеет возможность обновлять свою прошивку без перехода в этот режим. Основная функция кнопки — вывод устройства из состояния покоя или восстановления прошивки после неудачной перепрошивки. Кнопка функциональна только при включении устройства или нажатии кнопки **RESET**. Остальное время она не выполняет функций, при необходимости её функционал можно изменить.

Меры предосторожности при работе с HackRF One

При работе с HackRF One необходимо соблюдать меры, направленные на безопасность пользователя и самого устройства. Не допускается запуск приёма/передачи сигналов без подключённой антенны. При приеме/передаче данных без подключенной антенны существует риск выхода устройства из строя. В бескорпусном варианте изготовлении HackRF One возможно короткое замыкание при контакте платы с металлической поверхностью.

Область применения

HackRF One применяется в следующих случаях:

- при проверке WI-FI сети на устойчивость к подавителям сигнала или перехвате пакетов;
- при перехвате специальных сигналов со спутников;
- при перехвате информации, выведенной на монитор по кабелю, через электромагнитные наводки, излучаемые монитором;
- при перехвате звонков и СМС-сообщений;
- при прослушивании радио или радиолюбительских переговоров;
- при проверке на защищённость автомобильной сигнализации;
- при перехвате сигнала с беспроводной мыши или клавиатуры.

Перехваченный сигнал хранится в памяти компьютера в цифровом виде. Большая часть злоумышленников используют SDR-платформу для перехвата личной информации.

Проблемы защищенности стандарта GSM

GSM — это стандарт цифровой мобильной связи, разработанный в 1980-х годах, который считается надежно защищенным от различного рода злоумышленников и их возможных атак. Ассоциация GSMA официально утверждает, что прослушать разговор в GSM-канале возможно только с позволения одной из сторон:

- на стороне оператора;
- на стороне абонента.

К сожалению, даже такая технология имеет свои недостатки. 29 декабря 2009 года, немецкий инженер Керстин Нол сообщил всему миру об уязвимостях алгоритма шифрования «A5/1» К.Нол заявил, что система шифрования в GSM имеет основополагающие уязвимости и написанный им и его командой эксплойт это подтверждает [4].

Цели К.Нола заключались в следующем:

- продемонстрировать телекоммуникационным компаниями фундаментальные недочеты в алгоритме «A5/1» [4];
- призывать разработчиков к исправлению фундаментальных ошибок в алгоритме [4].

Таким образом, разработчик хотел показать, что действующие системы защиты GSM совершенно не соответствуют современным требованиям.

Свою разработку инженер представил в рамках конференции «Всемирный конгресс хакеров», которая проходила в Германии в г. Берлине.

«Ассоциация GSMA» после заявления К.Нола сообщает, что организации уже удалось изучить код, который им был предоставлен, и они передали образцы кода представителям сотовых операторов [4].

В ассоциации GSMA к разработке К.Нола отнеслись крайне неоднозначно: с одной стороны, её считали незаконной, а с другой отмечали, что разработчик значительно завысил возможную опасность своих разработок. Возможность дать всем желающим прослушивать разговоры абонентов К.Нол не рассматривал.

По мнению представителя ассоциации GSMA Клэр Крентон, взлом теоретически был возможен, но на практике это маловероятно, так как пока никому не удалось взломать систему шифрования сетей GSM, вдобавок К.Крентон отметила, что в ряде стран такие разработки носят незаконный характер [4].

Многие эксперты напротив, придерживались иной позиции. По их мнению, предоставленный код эксплойта можно модернизировать, и что при его компиляции на современных многоядерных, многопроцессорных вычислительных системах код может быть вполне эффективным и нести в себе вредоносную угрозу.

К.Нола часто обвиняли в незаконности своей разработки, в ответ на обвинения, он заявлял, что его разработка носит исключительно научный интерес и никаких зловредных действий он не совершал. Все тестирования эксплойта проходили на специальных программных симуляторах, которые воспроизводили режимы работы сети [4].

Достаточно авторитетная исследовательская компания в сфере мобильных развлечений и бизнеса «ABI Research» утверждала, что заинтересованным «сторонам» следует уделить большее внимание к данной проблеме, так как в ближайшее время может появится улучшенная версия программного кода. Важно отметить, что образцы кода эксплойта уже были в открытом доступе.

Разработка эксплойта проводилась К.Нолом и группой заинтересованных энтузиастов, которых он встретил в Амстердаме, на одном из форумов, посвященных вопросам информационной безопасности. Над созданием эксплойта трудилось порядка 25 человек из разных стран Европы [4].

На тот момент система GSM работала на 64-битном алгоритме шифрования «A5/1», в котором команда К.Нола нашла фундаментальную уязвимость. Этот алгоритм использует комплексный генератор потока ключей и 64-битный закрытый ключ, это позволяет защититься от большинства базовых атак и уязвимостей, например от атаки «грубая сила» («brute force»). Сегодня большая часть современных ПК работает с ключами длиной от 128 до 512 бит, использование которых является приоритетным при сравнении с длиной ключей шифрования в стандарте «A5/1» [4]. К сожалению, любую систему шифрования рано или поздно можно будет взломать, для этого требуется время и необходимый объем данных с оборудованием. На взлом современного алгоритма шифрования у злоумышленника должно уходить неизмеримое количество времени, тогда алгоритм можно рассмотреть для дальнейшего использования. На данный момент систему шифрования «A5/1» можно взломать за 9 секунд.

В 2007 году «Ассоциация GSMA» закончила разработку нового алгоритма шифрования под названием «KASUMI» или «A5/3», в данном алгоритме ключ имеет размер 128 бит, размер блока 64 бит. На момент выпуска алгоритма лишь незначительная часть операторов сотовой связи согласились поддержать технологию [4]. Причина достаточно очевидна: это технически сложная задача, невыгодная с точки зрения финансовых затрат, требуются значительные инвестиции - телекоммуникационным компаниям придется менять до 60 несущих частот на всех своих станциях. Большая часть сотовых операторов используют почти 100% своих радиочастотных ресурсов [5], следовательно, техническая возможность по оказанию услуг связи значительно снизится.

Практическая часть

При рассмотрении способа перехвата данных, передаваемых по протоколу GSM, стоит отметить, что процесс перехвата трафика в публичных сетях является незаконным и разрешен только в случае применения рассматриваемого способа в отношении свой собственной сети либо при наличии специального разрешения на данный вид деятельности. Далее рассматривается перехват данных, зашифрованных с помощью алгоритма шифрования A5/1.

Для перехвата используется:

- Устройство HackRF One;
- Операционная система Linux (дистрибутив Kali или Ubuntu);
- ПО GNU Radio, Wireshark, gqrx;
- Программный пакет airprobe.

С целью анализа перехваченного трафика используется инструмент gr-gsm – расширение для GNU Radio Companion, которое использует программный пакет airprobe в качестве модуля для работы с GSM-данными [6]. Для анализа различных сетевых протоколов используется ПО Wireshark, которое позволяет выводить и анализировать данные сетевых пакетов различных уровней моделей OSI, TCP/IP [6].

Для осуществления перехвата необходимо:

1) Определить рабочую частоту анализируемой GSM-станции. Для этого используется gqrx – ПО, которое позволяет работать с получаемыми через SDR данными. Программа имеет графический интерфейс, что значительно упрощает процесс эксплуатации. Результат анализа частот в диапазоне 890 ÷ 1000 МГц представлен на рис. 2 [7], где можно заметить присутствие постоянных сигналов в диапазоне частот 944.2 - 952 МГц [7], что позволяет сделать вывод о наличии в данном диапазоне частот каналов анализируемой станции;

2) Использовать программу airprobe – модуль для работы с GSM [6]. Для приема GSM-сигнала достаточно использовать программы gsmdecode и gsm-receiver, входящие в состав airprobe;

3) Запустить ПО Wireshark и в качестве приемного устройства выбрать интерфейс «lo», на-

строив фильтр на ключевое слово «gsmtap».

4) Запустить модуль airprobe для захвата GSM-трафика;

В окне модуля задать максимальное значение усиления. В качестве центральной частоты следует использовать среднюю частоту рабочего диапазона станции, определенного на шаге 1. В опциях трассировки (рис. 3) следует выбрать отображение пиковых и усредненных значений принимаемого сигнала [7].

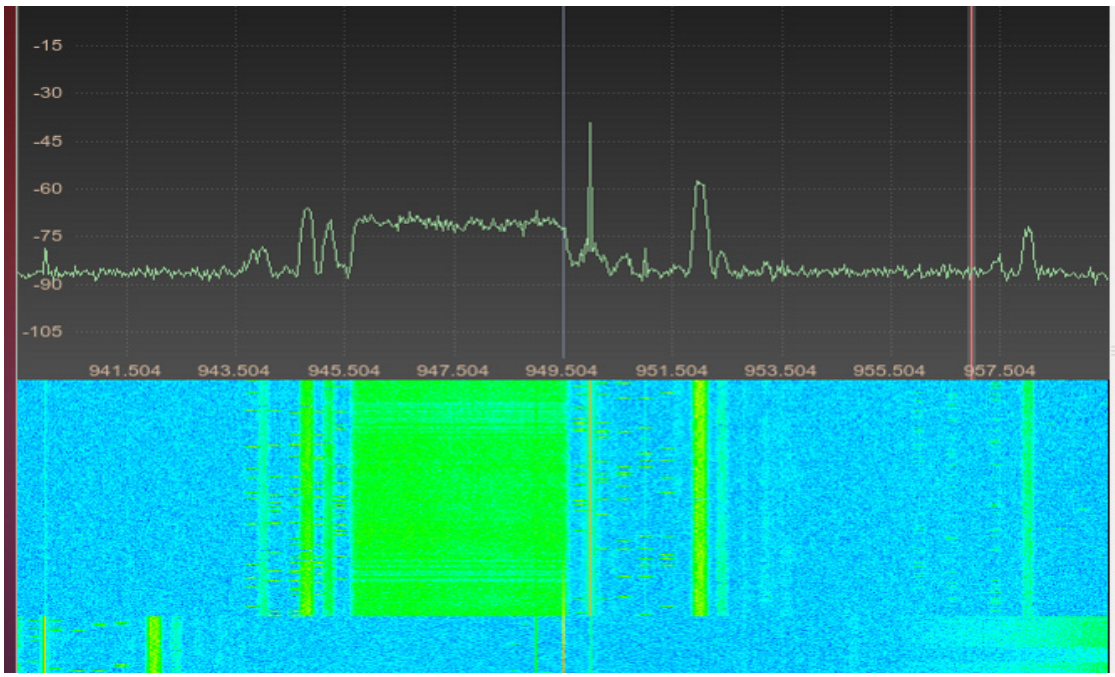


Рис. 2. Программа gqrx

Рис. 3. Настройка модуля airprobe для захвата GSM-трафика

Для декодирования сигнала необходимо выбрать частоту с максимальным значением амплитуды однократным нажатием кнопкой мыши.

5) Перенаправить GSM-данные в ПО Wireshark (рис. 4). Для поддержания частоты, заданной на шаге 5, необходимо повторять нажатия [8].

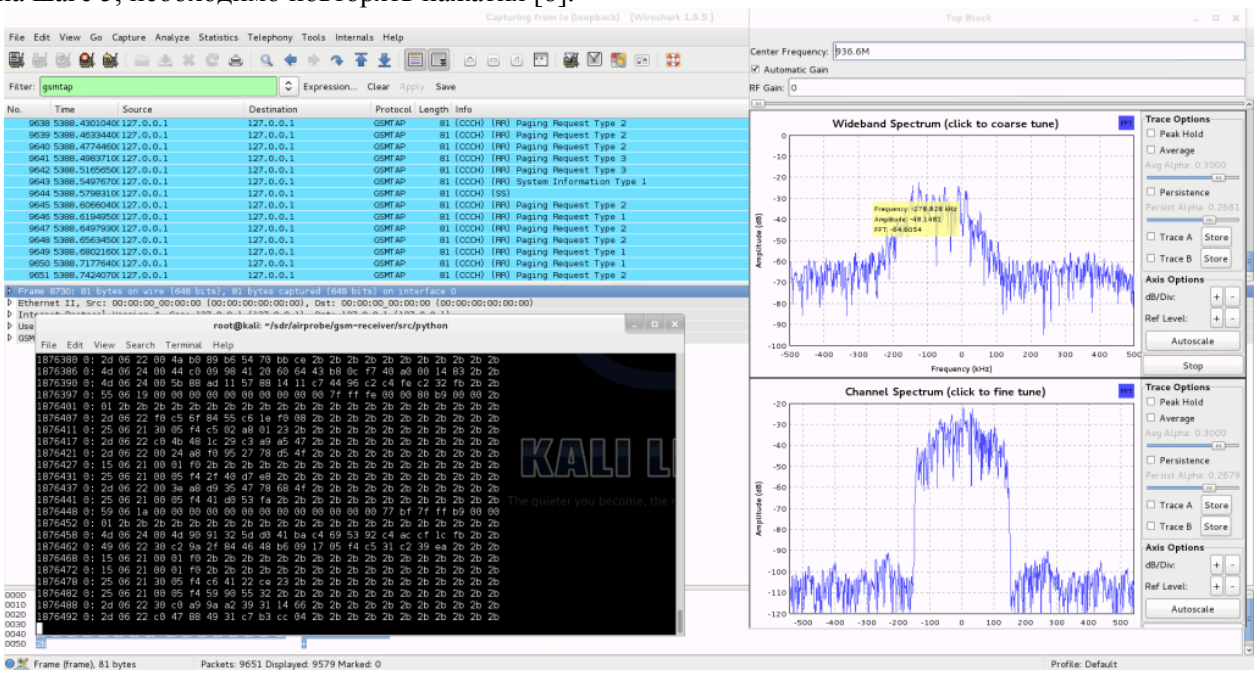


Рис. 4. Перехват GSM-трафика

6) Полученный после декодирования сигнал зашифрован с помощью алгоритма A5/1 [4]. Дешифратор из программы airprobe позволяет получить информацию в открытом виде. На рис. 5 приведен пример расшифровки SMS-сообщения [8].

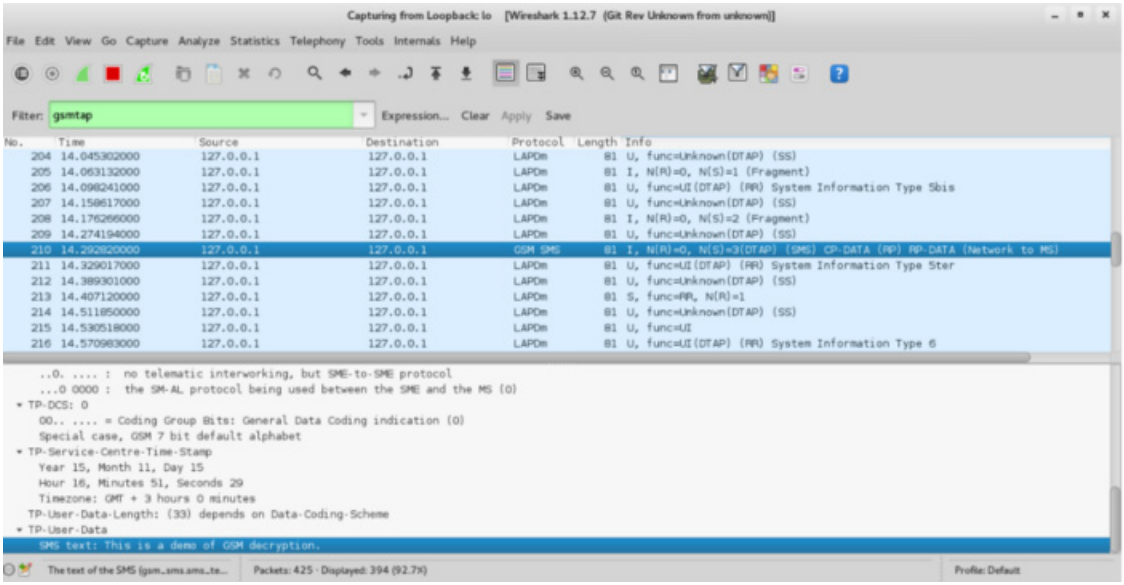


Рис. 5. Пример расшифровки SMS-сообщения

Заключение

Благодаря использованию HackRF One совместно с ПО GNU Radio, Wireshark и программным пакетом airprobe была продемонстрирована возможность перехвата трафика сети GSM, в результате которого были декодированы и расшифрованы передаваемые внутри сети данные.

Рассмотренный способ перехвата трафика демонстрирует широкие возможности SDR-платформы HackRF One. За счёт своей доступности и простоты использования SDR-устройства становятся востребованным инструментом решения инженерных и исследовательских задач.

Литература

1. *Силин А.* Технология Software Defined Radio. Теория, принципы и примеры аппаратных платформ // Беспроводные технологии. 2007. №2. С. 22-27.
2. *Плетнева И.Д.* Программно-определяемое радио: лабораторный практикум для подготовки магистров. М.: МИЭТ, 2016. Т.6. №2. С. 260-263.
3. *Шевелёв А.Е., Завьялов С.В.* Реализация модема для метеорной радиосвязи на основе SDR платформы HACKRF ONE. НЕДЕЛЯ НАУКИ СПБПУ, 2016. С. 79-82.
4. Взломана система шифрования стандарта GSM [www.iksmedia.ru] – URL: https://www.iksmedia.ru/news/3065166-Vzlomana-sistema-shifrovaniya-stand.html (дата обращения: 11.10.2020).
5. *Шетько Николай.* Взлом сотовых сетей GSM: расставляем точки над «i» // ET CETERA – серия цифровых журналов, распространяемых по подписке № 32. 2013.
6. *Будников С.А., Стешковой А.С., Бондаренко В.С.* Использование программно-определяемого радио для исследования трафика беспроводной сети. ОХРАНА, БЕЗОПАСНОСТЬ, СВЯЗЬ. 2017. №1. С. 225-231.
7. Прослушивание GSM с помощью HackRF – [www.securitylab.ru] URL: https://www.securitylab.ru/analytics/448062.php (дата обращения 11.10.2020).
8. RTL-SDR TUTORIAL: ANALYZING GSM WITH AIRPROBE/GR-GSM AND WIRESHARK [www.rtl-sdr.com/] – URL: https://www.rtl-sdr.com/rtl-sdr-tutorial-analyzing-gsm-with-airprobe-and-wireshark/ (дата обращения: 11.10.2020).

METHOD OF INTERCEPTING GSM SIGNALS BY THE USE OF HACKRF ONE SDR PLATFORM

Vladimir V. Nikolaev,
Student MTUCI, Moscow, Russia,
fredfred9033@mail.ru

Vyacheslav E. Mikhaylov,
Assistant of the Department of DD&ISS of the Institute Cybernetics, RTU MIREA, Moscow, Russia,
vmikhaylov95@yandex.ru

Abstract

The article provides a description of the characteristics of the SDR HackRF One device. The first section of the article represents the analysis of the functional capabilities of the device and suggests precautions. In the second section there are considered various areas of application of the device. The third section of the article defines problems of the GSM in terms of A5/1 encryption algorithm and provides an example of intercepting and decrypting SMS messages by the use of HackRF One SDR platform and special software written for this device. The aim of the article is to consider a modern approach in radio signals analysis by means of SDR technology.

Key words*: GSM, SDR, traffic analysis, encrypted data, encryption, intruder, intercepted, radio signal.*

ОЦЕНКА ВЛИЯНИЯ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ СЕТЕЙ 5G НА ЧЕЛОВЕКА

Сизов Дмитрий Викторович,
инженер Сахалинского ОРТПЦ, ФГУП РТРС, г. Углегорск, Россия,
deeemon8@mail.ru

Панкратов Денис Юрьевич,
доцент кафедры СиСРТ, к.т.н., МТУСИ, Москва, Россия,
dpankr@mail.ru

Аннотация

В последнее время завершается стандартизация сетей 5G, которые представляют собой дальнейшее развитие и расширение уже действующих сетей четвёртого поколения. В сетях 5G применяется как сантиметровый, так и миллиметровый частотные диапазоны, благодаря чему становится возможным применение антенных решеток с большим числом элементов (технология Massive MIMO). Указанные причины вызывают обеспокоенность научного сообщества и общественности влиянием излучения сетей 5G на человека. В данной статье рассматриваются новые технологии 5G и проблемы оценки биологического воздействия сетей 5G на человека с точки зрения существующих норм на излучение. Приведены нормы на излучение для различных стран, а также рассмотрены нормы на излучение, действующие на территории Российской Федерации. Рассмотрены основные организации, занимающиеся вопросами нормирования излучений электромагнитных полей. В статье рассматриваются и анализируются результаты семинара Международного союза электросвязи (ITU), проходившего в 2020 году и посвященного текущей ситуации по оценке безопасности сетей 5G для человека в мировом сообществе.

Ключевые слова: *сети 5G, ICNIRP, неионизирующие излучения, технология Massive MIMO, Beamforming, безопасность электромагнитных полей, нормы на неионизирующее излучение, санитарные нормы для электромагнитных полей.*

1. Введение

Стремительными темпами происходит развитие и модернизация технологий систем радиодоступа общего пользования. Недавно вошедшим в строй сетям 4G на смену приходят сети стандарта 5G [1,2,3, 12-18]. Технологии 5G - это дальнейшее развитие и значительное расширение возможностей уже введённых в эксплуатацию сетей поколения 4G, однако применение новых диапазонов частот и новых технологий вызвало обеспокоенность в мировом сообществе.

В рамках Семинара для стран Европы и СНГ по управлению спектром и вещанию [4], проходившего 1-2 июля 2020 года в дистанционном режиме на электронной площадке Международного союза электросвязи (ITU-D), рассматривались проблемы оценки влияния электромагнитных полей сетей 5G на человека. На Семинаре ITU, в частности, рассматривались как технические (новые технологии и новые диапазоны частот), так и биологические (оценка влияния излучения на человека, международные нормы, основные сомнения и направления для исследований) аспекты сетей 5G.

Использование в сетях 5G сантиметровых и миллиметровых диапазонов частот даёт возможность использовать антенны меньших размеров, чем в действующих сетях четвертого поколения. В системах пятого поколения рассматривается использование многоэлементных антенных массивов, распложенных на базовой станции, а также на абонентских устройствах. В сантиметровом диапазоне значительное повышение емкости сетей 5G планируется обеспечить за счет применения многопользовательской технологии MIMO в режиме направленной передачи (Beamforming) [1, 2].

В сетях 5G заявлены следующие ключевые показатели: пиковая скорость передачи данных до 10 Гбит/с, гарантированная скорость передачи для абонента 100 Мбит/с, задержка величиной в 1мс, возможность стабильной связи на скоростях движения абонентов около 500 км/ч. Также планиру-

ется увеличить эффективность использования спектра в 10-15 раз по сравнению с сетями 4G, для чего потребуются новейшие технологии для генерирования и обработки сигналов [3].

2. Новые технологи физического уровня сетей 5G

Основными нововведениями, реализуемыми на физическом уровне систем 5G, являются следующие технологии [1, 2]:

- технология неортогонального множественного доступа (NOMA) и другие альтернативные методы множественного доступа;
- системы MIMO с большим количеством антенн (Massive MIMO);
- применение направленной передачи (Beamforming).
- полный дуплекс (Full Duplex);
- использование фемтосот (Femtocell).

Важной особенностью технологии сетей пятого поколения является применение адаптивных антенных систем, построенных на основе следящих антенных решёток с применением технологий MIMO и Beamforming [2,4]. Такие антенные системы позволяют формировать узкие направленные лучи в сторону абонентского устройства в целях повышения скорости передачи данных (так называемый режим направленной передачи). При этом увеличивается излучаемая мощность в направлении абонента (см. рис. 1).

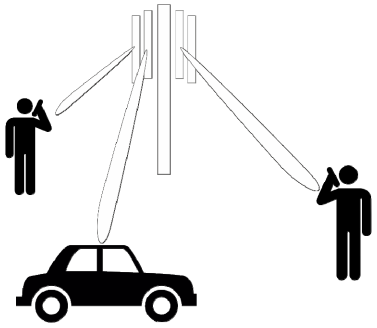


Рис 1. Принцип технологии направленной передачи (Beamforming)

Применение антенн меньшего размера (для диапазонов выше 6 ГГц) позволяет реализовать системы MIMO с большим количеством антенн (Massive MIMO). Благодаря этой технологии, возможно, обеспечить более высокую спектральную эффективность и энергетическую эффективность системы связи [4]. С помощью технологии Massive MIMO возможна узконаправленная передача в направлении конкретных абонентов внутри соты, благодаря этому удаётся значительно уменьшить взаимные помехи между соседними сотами, а также и внутри соты. В сетях 5G предполагается размещать на базовых станциях многоэлементные антенны (построенные на основе антенных решёток), которые будут состоять более чем из 128 элементов.

Использование технологи Beamforming позволит обеспечить узконаправленную передачу и, соответственно, энергетический выигрыш благодаря передачи сигналов в направлении абонентских станций. Также использование этой технологии даёт возможность снизить внутрисистемные помехи. В отличие от режима пространственного мультиплексирования (более эффективен для диапазонов до 6 ГГц), в котором формируется несколько пространственных потоков, режим Beamforming при использовании адаптивных антенных решеток позволяет излучать основную часть энергии сигналов в нужных направлениях и адаптироваться к условиям радиоканала [4].

Сети пятого поколения используют два частотных диапазона [2, 3], первый из которых включает частоты от 0,4 ГГц до 7,125 ГГц, а второй - частоты от 24 ГГц до 52,6 ГГц. В частотном диапазоне выше 6 ГГц для обеспечения покрытия сетей 5G и качества обслуживания необходимо увеличивать количество базовых станций, что неминуемо приводит к увеличению совокупной излучаемой мощности. Следует подчеркнуть, что именно использование диапазона частот СВЧ, особенно миллиметровых волн, вызывает тревогу у населения.

В связи с опасением негативного воздействия электромагнитных полей сетей 5G на человека, как в научном мире, так и в обществе, остро встала проблема излучения влияния излучений, фор-

мируемого при помощи технологий, применяемых в сетях 5G, на человеческий организм. В мире существует множество организаций, национальных и международных, которые занимаются вопросами безопасности электромагнитных полей при их воздействии на человека [5].

В процессе изучения негативного влияния излучения электромагнитных полей (ЭМП) на человека полученные результаты исследований и нормы были опубликованы в различных международных и российских документах [4,5,6]. В данной статье основное внимание уделяется оценке влияния излучений базовых станций 5G, при этом безопасность использования абонентских устройств также вызывает обеспокоенность общественности, о чем свидетельствуют публикации в средствах массовой информации [7].

3. Безопасность электромагнитных полей и международные спецификации

Одна из основных организаций, занимающихся вопросами безопасности электромагнитных излучений, это Международная комиссия по защите от неионизирующего излучения (МКЗНИ или англ. – ICNIRP). Комиссия МКЗНИ существует в целях изучения негативных эффектов для здоровья человека, связанных с воздействием на него неионизирующих излучений электромагнитных полей (ЭМП) и создания обоснованных норм по ограничению воздействия ЭМП на человека.

При построении сетей 5G одним из основных регулирующих документов МКЗНИ является «Руководящие принципы МКЗНИ по организации воздействия ЭМП (до 300 ГГц)» [5]. Следует отметить, что приведённые в этом документе нормы приняты и являются базовыми во многих странах мира. Руководящие принципы МКЗНИ включают в себя основные ограничения и контролируемые уровни, которые далее рассматриваются подробнее. Все значения допустимых величин в вышеупомянутом документе [5] основаны на проведённых научных медико-биологических исследованиях.

Основные ограничения включают в себя ограничения воздействия переменных ЭМП, при этом оценка этих ограничений проводится по измеряемым параметрам, которые оказывают воздействие на человека [5]. Известно, что частоты ЭМП полей существенно влияют на процессы взаимодействия ЭМП с биологическими организмами. Кроме того, для формирования ограничений на излучения нормируют следующие величины: плотность потока энергии (ППЭ) и индукционного тока, а также удельная поглощенная мощность. В реальных условиях измерение этих физических параметров ЭМП является трудоёмкой задачей. Поэтому основным измеряемым параметром вне тела человека является плотность потока энергии, измерить которую относительно просто.

4. Контролируемые уровни излучений

На практике при проведении санитарного контроля с целью оценки влияния ЭМП на человеческий организм, используются контролируемые уровни. Эти уровни нормируют следующие величины: плотность магнитного потока и напряженность поля, плотность потока энергии, сила тока в конечностях.

При соответствии измеряемой величины нормам контролируемых уровней, эта величина также будет соответствовать и нормам основных ограничений. При этом превышение значения контролируемого уровня не всегда говорит о том, что не выполняется основное ограничение. В таких случаях необходимо обеспечить соответствие основным ограничениям, а также использовать дополнительные защитные меры [5].

Для ЭМП частотных диапазонов от 0,1 МГц до 10 ГГц, как правило, ограничения приводятся на основании удельной поглощаемой мощности (Specific Absorption Ratio, SAR) для защиты тканей тела человека от перегрева. В частотных диапазонах от 10 ГГц до 300 ГГц основные ограничения приводятся на основании величины плотности потока мощности (ППМ) в целях исключения повышенного нагрева тканей на поверхности тела человека. В таблице 1 приведены значения величин для ограничений МКЗНИ, которые обеспечивают защиту от негативного воздействия ЭМП на человека [5].

Таблица 1

Значения величин для ограничений МКЗНИ, которые обеспечивают защиту от негативного воздействия ЭМП на человека

Диапазон частот	Средн. знач. SAR (тело человека) (мВт/кг$^{-1}$)	Лок. знач. SAR (туловище, голова) (мВт/кг$^{-1}$)	Лок. знач. SAR (конечности) (мВт/кг$^{-1}$)	ППМ (мВт/см^2)
0,1 МГц-10 ГГц	80	2000	4000	-
10 ГГц-300 ГГц	-	-	-	10^{-3}

Кроме основных ограничений и контролируемых уровней существует два типа норм – для защиты населения и для производственных условий. Нормы для производства предъявляют менее жёсткие требования к уровням излучений ЭМП.

Вопросами изучения негативного воздействия электромагнитных полей на человека также занимается Международный союз электросвязи (МСЭ). МСЭ разрабатывает рекомендации по измерению уровней излучения ЭМП, особенно в случае внедрения новых технологий в области современных систем радиосвязи, а также при создании специального программного обеспечения для прогнозирования уровней ЭМП.

Данную работу обеспечивает рабочая группа «EMC, lighting protection, EMF» сектора стандартизации электросвязи (ITU-T). Международный союз электросвязи (сектор – Телекоммуникации) опубликовал множество документов по оценке воздействия ЭМП на человеческий организм, которые представляют собой руководства и рекомендации по методам и мерам обеспечения ограничений на излучения ЭМП при воздействии на человеческий организм [7, 8].

Исследования и работы ITU-T проводятся в сотрудничестве с такими международными и национальными организациями, как например, ICNIRP, Институт инженеров электротехники и электроники (IEEE), Международная электротехническая комиссия (IEC), Всемирная организация здравоохранения (ВОЗ) и другие организации, выполняющие задачи стандартизации систем электросвязи и радиосвязи.

5. Нормы на НИИ в различных странах и в России

Можно заметить, что в соответствие с рекомендациями международных организаций уровни излучения ЭМП в нормативных документах многих стран в целом имеют схожие значения. При этом многие страны используют свои предельно допустимые уровни излучений, которые существенно отличаются от общепринятых. В таблице 2 в качестве примера указаны нормы на НИИ для диапазонов сотовой связи ниже и выше 6 ГГц.

Сопоставив данные таблицы 2 можно заметить насколько сильно отличаются нормы на НИИ в различных странах мира. Самые жёсткие нормы используются в Швейцарии (9,5 мкВт/см^2), а в ряде таких стран, как Россия, Китай, Италия, они составляют 10 мкВт/см^2. Это примерно в сто раз жёстче в сравнении с международными стандартами ICNIRP. При этом самые мягкие предельные уровни используются в США, и менее мягкие – в Канаде.

В Российской Федерации нормы на излучение ЭМП регламентируется документами СанПиН, например – "Гигиенические требования к средствам сухопутной подвижной радиосвязи" [6].

Таблица 2

Нормы разных стран на НИИ для диапазонов сотовой связи для диапазонов ниже 6 ГГц и выше 6 ГГц [8]

Страна	Плотность потока мощности (мкВт/см^2) для защиты населения	
	ниже 6 ГГц	выше 6 ГГц
Россия	10	10
Швейцария	9,5	9,5
Италия	10	10
Китай	10	10
Канада	440	1000
США	1000	1000
МКЗНИ	900	

Требования СанПиН [6] определяют уровни излучения ЭМП в целях снижения неблагоприятного воздействия на здоровье человека излучений, создаваемых базовыми станциями систем подвижной связи. Как производство, так и применение оборудования систем подвижной связи регулируются с помощью санитарно-эпидемиологических испытаний, проводимых по определённой методике. По результатам таких исследований выдаётся заключение, в котором указывается каким нормам соответствует данное оборудование.

Ввод в эксплуатацию и эксплуатация оборудования базовых станций, а также уровни излучений ЭМП от базовых станций строго регулируются законодательством и контролируются уполномоченными государственными органами. При этом размещение базовых станций планируется так, чтобы минимизировать воздействие ЭМП на население.

Для оценки влияния излучений ЭМП на человека при использовании оборудования систем подвижной связи в соответствии с нормами СанПиН в зависимости от диапазонов рабочих частот измеряются следующие параметры. Для диапазонов частот от 27 МГц до 0,3 ГГц осуществляется измерение напряженности поля (В/м), а для диапазонов частот от 0,3 ГГц до 2,4 ГГц осуществляется измерение величины ППЭ (мВт/см, мкВт/см).

Допустимые значения уровней излучения ЭМП в пределах жилой застройки, а также внутри помещений (жилых, общественных, производственных), составляют не более: 10 В/м для диапазонов частот от 27 МГц до 30 МГц; 3 В/м для диапазонов частот 30 МГц до 0,3 ГГц и 10 мкВт/см^2 для диапазонов частот от 0,3 ГГц до 2,4 ГГц.

В Российской Федерации для контроля по соблюдению Санитарных норм и правил на излучение соответствующие государственные регулирующие органы (Роспотребнадзор, Роскомнадзор) осуществляют измерения уровней излучений ЭМП и оценивают его соответствие допустимым уровням на излучение. Требования на излучения для защиты населения приведены в таблице 3.

Сопоставляя данные таблиц 2 и 3 для сантиметровых и миллиметровых диапазонов, нетрудно заместить, что нормы на излучения ЭМП в России на данный момент устанавливают довольно жёсткие требования к излучениям по сравнению с другими странами (нормы введённые для защиты населения по ППМ в США примерно в 100 раз мягче), но уступают нормам в Швейцарии.

Таблица 3

Максимальные значения и измеряемые параметры ЭМП для защиты населения [6,7]

Диапазоны частот	< 0,3 МГц	от 0,3 до 3 МГц	от 3 до 30 МГц	от 30 МГц до 0,3 ГГц	от 0,3 до 300 ГГц
Измеряемые параметры	Напряженность поля, (В/м)				ППМ (мкВт/см^2)
Максимальные значения	25	15	10	3	10 *
* 25 мкВт/см^2 - при измерении облучения от антенн в режиме сканирования					

6. Современные проблемы при оценке влияния ЭМП сетей 5G

Технологии 5G позволят обеспечить существенное усовершенствование существующих систем радиосвязи. Этому способствует также использование новых частотных диапазонов (как около 3,5 ГГц, так и до нескольких десятков ГГц). Более высокие частоты являются новыми для сетей мобильной связи (ранее они использовались в основном для систем радиорелейной связи и систем спутниковой связи). При этом в сетях 5G на более высоких частотах будут работать больше базовых станций, и обеспечиваться больше подключенных абонентских устройств. В сетях 5G будет дополнительно использоваться технология направленной передачи (Beamforming) для более эффективной передачи сигналов на конкретные абонентские устройства [3,4].

В связи с указанными выше обстоятельствами Комиссия ICNIRP предложила продолжить разработку и расширить научно обоснованные рекомендации по ограничению воздействия НИИ, относящихся к сетям 5G [9]. Это некоммерческая и независимая от телекоммуникационной отрасли международная организация, которая помимо взаимодействия с ВОЗ и Международной организацией труда осуществляет разработку рекомендаций по ограничению воздействия радиочастотных ЭМП на человека.

В докладе [9] в рамках секции по сетям 5G Международного семинара ITU [3] была показана необходимость проведения такой работы и оценки влияния ЭМП на человека, а также рассмотрены возникающие в связи с этим вопросы безопасности сетей 5G. Четкие правила важны, чтобы контролировать безопасность сетей 5G в различных странах, а ясная и точная информация имеет ключевое значение для информирования о рисках для здоровья человека. Всем известно о вреде курения и связанных с этим рисках для здоровья человека – на соответствующей продукции указывается предупреждение. Также мы встречаем предупреждение на электрических приборах, работающих от электросети.

На Семинаре ITU было показано, как в мировом сообществе обеспечивается безопасность сетей 3G / 4G / 5G. Кроме того, безопасность обеспечивается с помощью обновляющихся норм, разработанных комиссией ICNIRP (ЭМП для частот от 100 кГц до 300 ГГц). Новые Рекомендации ICNIRP по ограничению воздействия ЭМП охватывают аспекты защиты, которые не были так актуальны 20 лет назад – ранее для систем мобильной связи основное внимание вопросам безопасности уделялось частотам до 6 ГГц. В настоящее время больше внимания уделяется аспектам защиты для частот от 6 до 100 ГГц – это диапазоны частот 5G и будущих систем мобильной связи. Было сделано замечание о ненадлежащем использовании показателя SAR в диапазонах частот от 6 до 10 ГГц, а также о необходимости уменьшения площади пространственного усреднения с 20 до 4 $см^2$ для диапазонов частот > 6 ГГц. Новые ограничения позволят обеспечить более адекватную защиту от воздействий импульсных или непрерывных сигналов сетей 5G.

На семинаре ITU также были затронуты актуальные вопросы безопасности сетей 5G и рассмотрены возможные заблуждения при неправильном толковании подходов оценки влияния ЭМП на человека. В частности, в средствах массовой информации встречаются сообщения об опасности систем мобильной связи для человека в связи с тем, что нормы и принципы защиты учитывают только тепловое воздействие. По заявлениям специалистов в нормах ICNIRP учтены все возможные эффекты независимо от механизма воздействия на здоровье человека. В то же время, если механизм воздействия известен (например, тепловой), это позволяет использовать больший объем научных данных для обеспечения соответствующих ограничений излучений.

Следует отметить, что есть указания на то, что ЭМП могут вызывать болезни, например, рак, хотя нет прямых доказательств этого (ВОЗ). При этом Международное агентство по изучению рака (осуществляющее свою деятельность в рамках ВОЗ) в 2011 году классифицировало радиочастотные излучения как потенциально канцерогенные. Специалисты ICNIRP утверждают, что при разработке норм учитываются все эффекты, рассматриваются все аспекты негативного влияния излучений ЭМП на человека. Однако, исходя из последних данных, не отрицается негативное влияние ЭМП на человека и «нельзя с абсолютной уверенностью сказать, что это оно безопасно» [4,8,9].

В качестве примера обоснования негативного влияния также указывается воздействие курения на здоровье человека. Хорошо известно, что оно вредит здоровью и вызывает рак, но также известно, что некоторые люди могут курить всю свою жизнь и никогда не заболеть раком. При том важно знать процент людей заболевающих раком от курения, а также факторы, которые могут изменить этот прогноз к лучшему или к худшему.

Довольно часто у населения возникает беспокойство в связи с установкой вышек мобильной связи на крыше зданий в городе и вблизи населенных пунктов в сельской местности. Конечно, это может быть не безопасно, так как 5G – это новое явление, и пока нет достоверных исследований его воздействий на людей. С другой стороны, как утверждают специалисты ICNIRP, при соблюдении норм защиты от ЭМП можно с достаточной уверенностью сказать, что сети 5G не причинят вреда населению. Кроме того, не следует ассоциировать негативное воздействие только с названием «5G», так как на безопасность людей влияет только физическое воздействие ЭМП.

7. Заключение

Подведя итог сказанному выше, с учетом недавних публикаций [3,9,10], можно сказать, что вопрос, связанный с безопасностью ЭМП, излучаемых базовыми станциями 5G, для здоровья человека однозначно не решён. На это также указывает то, что в разных странах используются различные нормы на допустимые уровни излучений ЭМП, то есть существуют разногласия, и у специалистов нет единого мнения. Более тщательные исследования воздействия ЭМП диапазонов выше 6 ГГц продолжаются.

Исследования оценки вреда от использования оборудования сетей подвижной сотовой связи (в основном базовых станций) на здоровье человека продолжаются более 20 лет. Специалисты не могут с достаточной уверенностью сказать, насколько вредно воздействие оборудования подвижной связи на человека, и каков потенциальный риск для его здоровье с учётом сравнительно небольшого периода подобных исследований. До настоящего времени было проведено незначительное количество конкретных исследований на частотах, которые будут использоваться в 5G. На настоящий момент неблагоприятных последствий для здоровья человека при использовании данного оборудования не было выявлено [9,11].

Следует отметить, что по данным ВОЗ воздействия ЭМП современных технологий 5G приводят к незначительному повышению температуры в организме человека. При условии, что общий уровень воздействия остается ниже международных норм, никаких последствий для общественного здравоохранения не ожидается [9,11]. Однако исследования негативного влияния излучения ЭМП при использовании оборудования систем подвижной связи активно ведутся как на международном, так и на государственном уровне различных стран, что отражается в различие норм и требовани в разных странах [8,9,10] и планировании проведения регулярных семинаров ITU в этой области. Ужесточение норм на излучение ЭМП необходимо для минимизации его негативного влияние на человеческий организм.

Литература

1. *Ali Zaidi, Frederik Athley, Jonas Medbo, Ulf Gustavsson, Giuseppe Durisi, Xiaoming Chen.* 5G Physical Layer Principles, Models and Technology Components. Elsevier Ltd, 2018. 314 p.
2. *Wei Xiang, Kan Zheng, Xuemin (Sherman) Shen.* 5G Mobile Communications.Switzerland: Springer International Publishing, 2017. 692 p.
3. https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2020/Spectrum_EUR_CIS/Remote.aspx.
4. *Бакулин М. Г., Крейнделин В. Б., Панкратов Д. Ю.* Технологии в системах радиосвязи на пути к 5G. М.: Горячая линия – Телеком, 2018. 280 с.
5. Руководства ICNIRP по ограничению воздействия переменных электрических, магнитных и электромагнитных полей (до 300 ГГЦ). https://www.who.int/peh-emf/publications/ICNIRP_Guidelines_rus_final.pdf?ua=1.
6. СанПиН 2.1.8/2.2.4.1190-03 "Гигиенические требования к размещению и эксплуатации средств сухопутной подвижной радиосвязи".
7. https://www.comnews.ru/content/121089/2019-08-01/trebovaniya-sanpin-v-rf-tormozyat-5g-chast-2-igor-guryanov-generalnyy-direktor-ooo-spektrum-menedzhment.
8. *Dr. Emilie van Deventer*, Head of EMF Project, Radiation Programme, Department of Environment, Climate Change and Health, Geneva, Switzerland, Radiofrequency Electromagnetic Fields and Health, Presentation, 2 July 2020.
9. *Mr. Rodney Croft, Chair,* International Commission on Non-Ionizing Radiation Protection (ICNIRP); University of Wollongong, Australia, Presentation, 2 July 2020.
10. *Dr. Fryderyk Lewicki*, ITU-T SG5, Chairman of WP1, Orange Polska, Poland, Electromagnetic Fields and 5G Implementation, Presentation, 2 July 2020.
11. https://www.who.int/ru.
12. *Панкратов Д.Ю., Степанова А.Г.* Компьютерное моделирование технологии MIMO для систем радиосвязи // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 12. С. 33-37.
13. *Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К.* Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 24-30.
14. *Крейнделин В.Б., Старовойтов М.Ю.* Повышение помехоустойчивости системы связи MIMO с пространственным мультиплексированием методом додетекторного сложения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 4-13.
15. *Крейнделин В.Б., Усачев В.А.* LTE-advanced pro как основа для новых сценариев M2M // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 28-32.
16. *Бакулин М.Г., Крейнделин В.Б.* Проблема повышения спектральной эффективности и емкости в перспективных системах связи 6G // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 25-31.
17. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Анализ пропускной способности канала mimo в условиях замираний // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 2. С. 13-20.
18. *Крейнделин В.Б., Панкратов Д.Ю.* Вероятностная модель радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 1. С. 103-107.

ASSESSMENT OF ELECTROMAGNETIC FIELDS IMPACT OF 5G NETWORKS ON HUMANS

Denis Y. Pankratov,
Associate Professor of the Department of NaSRCaTRB, Ph.D., MTUCI,
dpankr@mail.ru

Dmitry V. Sizov,
Engineer of Sakhalin Regional Broadcasting Center, FGUP RTRS, Uglegorsk, Russia,
deeemon8@mail.ru

Abstract

Recently, the standardization of 5G networks is being completed, which represent the further development and expansion of already existing fourth-generation networks. In 5G networks, both centimeter and millimeter frequency bands are used, which makes it possible to use antenna arrays with large number of elements (Massive MIMO technology). These reasons cause concern of the scientific community and the public about 5G networks radiation impact on humans. This article briefly examines new 5G technologies and the problem of assessing the biological impact of 5G networks on humans from the point of existing radiation regulations. The electromagnetic fields radiation standards for various countries are given, and the standards in force in the territory of the Russian Federation are considered. The main organizations dealing with the issues of standardization of electromagnetic fields radiation are considered. However, the issue of assessing the impact of radiation of 5G networks has not been unequivocally resolved, further research continues.

Keywords: *5G networks, ICNIRP, non-ionizing radiation, Massive MIMO technology, Beamforming, safety of electromagnetic fields, norms for non-ionizing radiation, sanitary standards for electromagnetic fields radiation.*

ТЕКУЩЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СЕТИ 5G

Ермакова Анастасия Всеволодовна,
магистрант МТУСИ, Москва, Россия,
msikisylia@gmail.com

Бабенко Ксения Андреевна,
магистрант МТУСИ, Москва, Россия,
kcbabenko@yandex.ru

Мирошникова Наталия Евгеньевна,
доцент кафедры РТС, к.т.н., МТУСИ, Москва, Россия,
n.e.miroshnikova@mtuci.ru

Аннотация

В статье рассматривается текущее состояние и перспективы развития сетей пятого поколения. Приведено сравнение методов модуляции, являющихся кандидатами в технологии физического уровня сетей 5G, рассматривается перспектива использования концепции когнитивного радио в системах пятого поколения, а также способы решения проблемы доступа в частотному ресурсу.

***Ключевые слова**: 5G, системы мобильной связи, методы модуляции, интернет вещей, когнитивное радио, динамический доступ к спектру*

Введение

В 2015 году состоялось первое собрание 3GPP по разработке нового стандарта, обозначенного как 5G. По результатам собрания был разработан план, согласно которому развитие стандарта должно было проходить в два этапа, первый из которых завершился в 2018 году, второй этап – в 2019-м, а первая коммерческая эксплуатация состоялась в 2020-м году. Данный план подробно описан в Рекомендации МСЭ М.2083-0 [8-16].

В рекомендации говорится, что системы мобильной связи нового поколения должны обладать следующими свойствами:

- Предоставлять пользователям широкий спектр приложений и услуг, от информационно-развлекательных услуг до новых промышленных и профессиональных приложений.
- Способствовать появлению интегрированных отраслей ИКТ. Некоторые возможные области включают: накопление, агрегирование и анализ больших данных; предоставление настраиваемых сетевых услуг для корпоративных и социальных групп в беспроводных сетях. Доступные, устойчивые и простые в развертывании системы мобильной и беспроводной связи могут способствовать достижению этой цели, одновременно эффективно экономя энергию и повышая эффективность.
- Обеспечивать обмен любым типом контента в любое время, в любом месте и через любое устройство. Пользователи будут создавать больше контента, и делиться им без ограничений по времени и местоположению.
- Обеспечивать легкий доступ к электронным учебникам или облачному хранилищу знаний в Интернете, расширяя возможности таких приложений, как электронное обучение, электронное здравоохранение и электронная коммерция.
- Обеспечивать энергоэффективность в ряде секторов экономики, поддерживая межмашинную связь и такие решения, как интеллектуальные сети, телеконференции, интеллектуальная логистика и транспорт.

Большинство мобильных сетей 4G работает на макросотах. Однако макросоты, охватывающие большие географические области, не всегда смогут обеспечить плотное покрытие, низкую задержку

и высокую пропускную способность, необходимые для некоторых приложений 5G, поэтому операторы сейчас вкладывают средства в уплотнение своих сетей радиодоступа (RAN) - особенно в густонаселенных городских районах - путем развертывания небольших сот. Маленькие соты, обслуживая гораздо меньшую географическую зону, чем макросота, увеличивают покрытие сети, пропускную способность и качество обслуживания.

К 2020 году услуги систем пятого поколения предоставляются 1155 операторами в Японии, Корее, Китае и США, тестовые сети развернуты в Европе и России [1]. Основные нововведения касаются физического уровня сети и алгоритмов обработки сигналов в приемных и предающих устройствах.

Технологии физического уровня

Технологии физического уровня систем 5G должны обеспечивать высокую помехоустойчивость системы передачи и спектральную эффективность. В качестве кандидатов в методы модуляции для физического уровня систем 5G выбраны следующие: модуляция на основе синтезированного банка фильтров FBMC, OFDM с дополнительной фильтрацией (f-OFDM), обобщенное мультиплексирование с частотным разделением (GFDM) и мультиплексирование с частотным разделением и универсальной фильтрацией (UFMC). Каждая из этих технологий имеет свои преимущества и недостатки, и среди них F-OFDM и FBMC использовались в тестовых версиях разрабатываемых систем.

F-OFDM (Filtered OFDM) представляет собой модификацию технологии OFDM. Суть технологии F-OFDM представлена на рисунке 1. В технологии F-OFDM, полоса спектра, выделенная для передачи OFDM сигнала, разделяется на несколько частотных поддиапазонов, каждый из которых фильтруется для уменьшения интерференции. Каждая из полос может иметь разную ширину, а значит, возможна организация каналов с различной пропускной способностью, в зависимости от вида предаваемого трафика. Каждый поддиапазон состоит из нескольких поднесущих, и частотный интервал между поднесущими может различаться для каждого поддиапазона. Это позволяет создать очень гибкую структуру подкадра, которая может переносить различные типы служебных данных в одном подкадре, что является одним из требований, предъявляемым к структуре кадра в 5G.

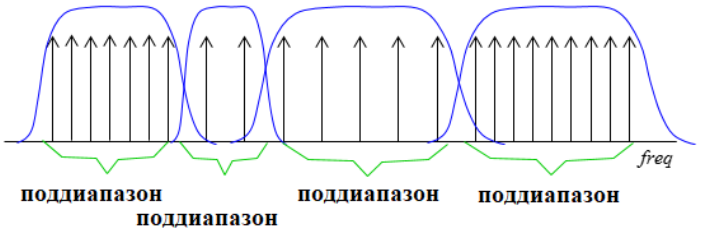


Рис. 1. Разделение на поддиапазоны в F-OFDM

Сравнение структурных схем формирователей сигналов F-OFDM и OFDM представлено на рисунке 2. В F-OFDM разнесение поднесущих в каждом поддиапазоне различно (например, разнесение поднесущих для поддиапазона N_1 равно $\Delta f / 2$, а разнесение поднесущих для поддиапазона N_k равно $4\Delta f$), также длина циклического префикса для каждого поддиапазона может варьироваться и к каждому поддиапазону применяется отдельный фильтр.

Очевидно, что основным преимуществом такой технологии является возможность адаптации к условиям в канале и виду трафика, а основным недостатком – сложность технической реализации [4].

В технологии FBMC для разбиения на частотные поддиапазоны используется синтезированный на основе фильтра прототипа банк фильтров. Система FBMC предлагает большую устойчивость к сдвигу времени и частоты, чем OFDM, и не использует циклический префикс, что повышает спектральную эффективность, но усложняет синхронизацию. За счет фильтрации обеспечивается малый уровень боковых лепестков и, тем самым, малая интерференция между поддиапазонами. На рисунке 3 показан принцип разбиения на частотные поддиапазоны с помощью банка фильтров в технологии FBMC [5].

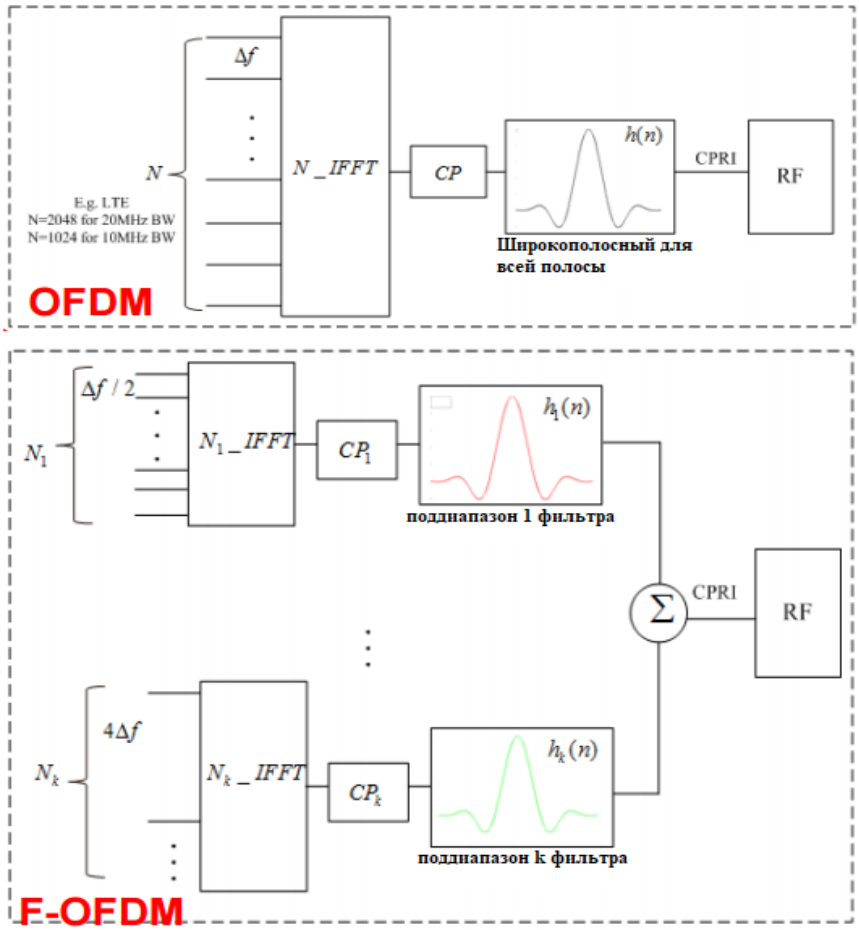


Рис. 2. Структурная схема формирователя сигнала F-OFDM

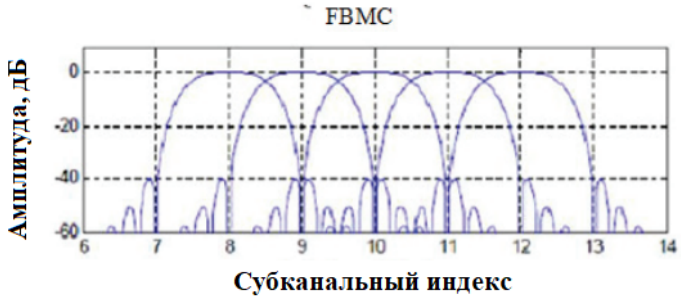


Рис. 3. Разбиение на частотные поддиапазоны с помощью банка фильтров в технологии FBMC

Также стоит отметить, что системы FBMC сравнительно более устойчивы к воздействию узкополосного шума, чем системы с OFDM.

На рисунке 4 показана структурная схема передатчика FBMC, на рисунке 5 – структурная схема стандартного приемника FBMC. В передатчике высокоскоростной входной сигнал будет демультиплексирован на N ветвей (поддиапазонов). В каждом поддиапазоне может быть выбран либо одинаковый, либо различный тип модуляции поднесущих. Далее, в каждом из поддиапазонов производится передискретизация. Данные с повышенной частотой дискретизации поступают на вход банка фильтров синтеза gk (n), k = 0,1,…., N-1. Затем, сигналы с выхода всех фильтров суммируются. В приемнике, чтобы получить N поднесущих с разными центральными частотами, принятый сигнал r(n) будет передан на набор фильтров анализа fk (n), k = 0,1,…., N-1. Сигнал в каждой ветви обработки подвергается понижению частоты дискретизации на N, демодулируется и мультиплексируется для получения оценки исходного сигнала Xr (n). [6]

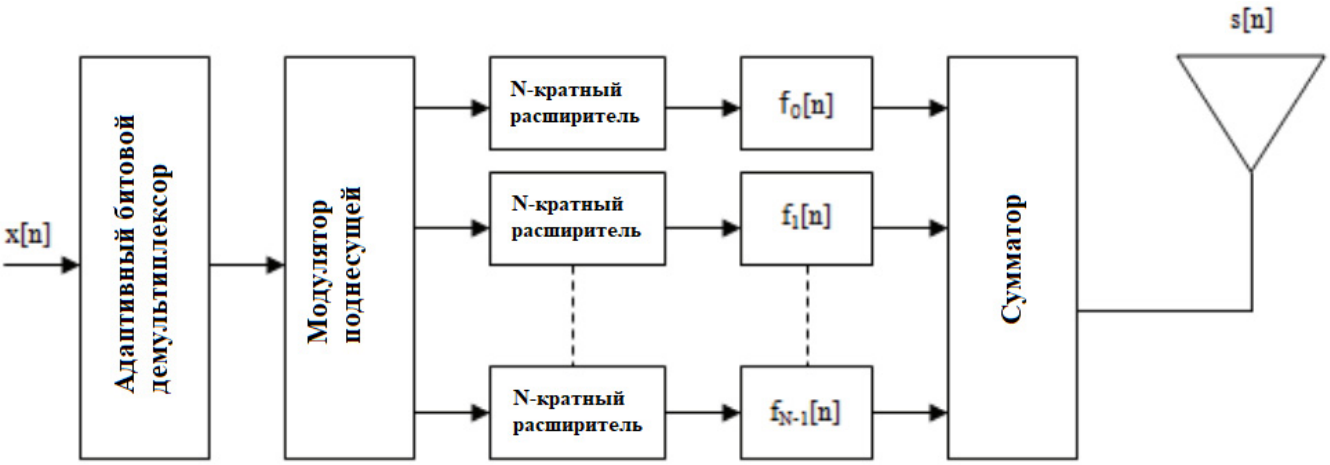


Рис. 4. Структурная схема передатчика FBMC

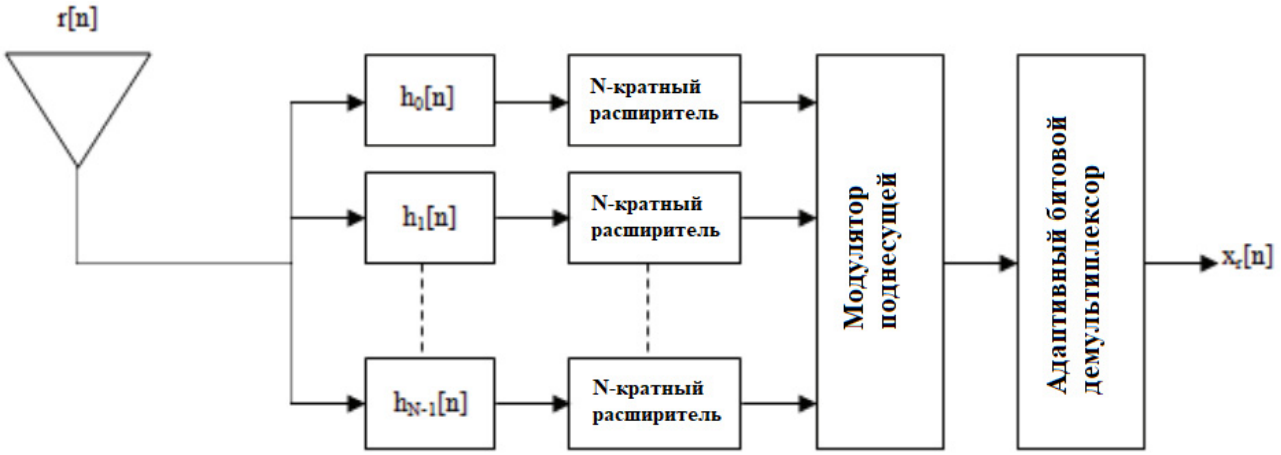


Рис. 5. Структурная схема типового приемника FBMC

Система когнитивного радио для 5G

Важным этапом в развитии систем 5G является реализация возможности работы интернет-сервисов в системах, как нового стандарта, так и существующих в настоящее время системх 4G, то есть реализации “мобильного интернета” в гетерогенных сетях (HetNets) с очень высокими скоростями подключения. Реализация гетерогенных систем возможна с использованием принципов когнитивного радио.

Цель когнитивного радио (cognitive radio, CR) состоит в том, чтобы производить мониторинг радиоэфира в режиме реального времени и обнаруживать неиспользуемые участки спектра. Когнитивным радио можно назвать радиоустройство, в котором программно реализована возможность мониторинга условий своей работы, накопления данных по результатам мониторинга, и возможность принимать решения о параметрах своей работы для наиболее эффективной работы системы. К условиям работы относятся такие данные как: географическое положение абонента, помеховая обстановка, загрузка спектрального диапазона, качество передачи, вид траффика. По результатам анализа и с учетом накопленных данных, может быть принято решение о смене скорости передачи, мощности, типа модуляции и т.д., вплоть до перехода в иной стандарт связи. Технология когнитивного радио может обеспечить совместную работу устройств различных стандартов связи, которые в силу условий применения и требований пользователей не могут использовать общие для всех методы модуляции, единые методы разделения каналов, скорость передачи данных и т.д.

В своих рекомендациях Международный Союз Электросвязи (МСЭ-Р) определил следующие

задачи систем когнитивного радио:

1. Повышение эффективности использования имеющегося радиочастотного спектра и частичное решение проблемы перегруженности сетей за счет непрерывного мониторинга свободных участком спектра.
2. Работа когнитивных устройств не должна налагать какие-либо дополнительные ограничения на другие радиослужбы, совместно использующие соответствующую полосу частот.
3. Любая система, использующая технологии когнитивного радио в некоторой распределенной соответствующей радиослужбе полосе частот, должна функционировать в соответствии с положениями Регламента радиосвязи и другими административными правилами, регулирующими использование полос частот и критерии защиты.

Когнитивный цикл можно разделить на четыре этапа:

1. Мониторинг условий работы

Можно выделить следующие виды мониторинга:

- энергетический мониторинг (этот способ хорош для грубой оценки);
- циклостационарный мониторинг, основанный на предположении о периодичности используемых сигналов;
- мониторинг с помощью согласованной фильтрации.

2. Сканирование частотного диапазона:

- определение свободных участков спектра;
- определение свободных временных интервалов;
- установка правил взаимодействия между лицензированными и нелицензированными пользователями.

3. Адаптация характеристик.
4. Установление соединения и обмен информацией между узлами.

На упрощенном уровне понимания когнитивным радио можно считать радиосистему, которая сканирует эфир, обычно используя в качестве аппаратной платформы программно-определяемое радио (software-defined radio, SDR), и выбирает наиболее эффективную архитектуру работы в нем. Радиосистема может проверять наличие сигналов 2G GSM, 3G UMTS и сигнала Wi-Fi, а затем конфигурировать себя для использования соединения, которое будет предоставлять оптимальный диапазон частот.

Реализация 3GPP динамического управления частотным ресурсом в сетях 5G

Управление сетью - одна из важнейших задач любой коммуникационной технологии. Учитывая множество существующих услуг и дополнительных услуг, которые будут предлагаться в новом экономическом секторе с использованием технологии 5G, срочно необходимы интеллектуальные средства эффективного управления сетью. Автономные NM, обладающие свойствами самосознания, самонастройки, самооптимизации и самовосстановления, необходимы дляуменьшения затрат и экономии энергии.

Ключевые проблемы при применении UDN в 5G были определены следующим образом: сетевая архитектура и усовершенствования процедур протокола, предотвращение помех и межсотовая координация, EE и SON. Для решения одной из этих ключевых проблем UDN был проведен опрос о том, как решения машинного обучения могут принести пользу управлению 5G SON с точки зрения сквозной перспективы [5]. Ключевым улучшением SON является его способность настраивать, оптимизировать и «лечить» себя. Также была представлена эволюция SON в 3GPP вместе с подробными реализациями SON на различных архитектурах. Были подробно обсуждены элементы, которые способствовали развитию SON, включая самоконфигурацию, самооптимизацию, самовосстановление, самосогласование, минимизацию тестов привода, основные сети и SON в виртуализированной и программно управляемой архитектуре 5G. Обзор соответствующей литературы NM на основе ML, основанной на этих элементах, также был представлен всесторонне в [5]. Возможности множественного доступа и мультисервиса, предусмотренные в 5G, могут быть реализованы путем разделения одной физической сети на несколько изолированных логических сетей. Проблемы, которые необходимо решить, прежде чем полностью реализовать концепцию разделения сети на ос-

нове мультисервисной программной архитектуры мобильной сети 5G, включают виртуализацию RAN, композицию услуг с детализированными сетевыми функциями, а также сквозную оркестровку и управление срезами.

Распределение спектра для 5G подразделяется на три основных диапазона, а именно: низкий, высокий и очень высокий. Спектр на частотах ниже 1 ГГц, особенно на 700 МГц [3,4], обеспечивает покрытие 5G на больших территориях и глубокое покрытие внутри помещений. Спектр на высоких частотах с относительно большой полосой пропускания ниже 6 ГГц (от 3,4 до 3,8 ГГц) [3,4] обеспечивает необходимую емкость для поддержки множества подключенных устройств и высокую скорость для одновременно подключенных устройств. Этот спектр обеспечивает наилучший компромисс между пропускной способностью и покрытием. На очень высоких частотах выше 24 ГГц (например, от 24,25 до 27,5 ГГц) с очень большой полосой пропускания спектр обеспечивает сверхвысокую пропускную способность и очень низкую задержку [3,4]. Ячейки на этих частотах имеют небольшое покрытие (от 50 до 200 м). Создание сетей 5G в диапазонах mmWave первоначально будет сосредоточено на областях с высоким спросом на трафик или определенных местах или помещениях, требующих услуг с чрезвычайно высокими скоростями передачи данных (в Гбит/с). Этот «новаторский» диапазон mmWave также обеспечивает сверхвысокую пропускную способность для новых инновационных услуг, что позволяет новым бизнес-моделям и секторам экономики пользоваться преимуществами 5G.

С-диапазон спектра, который находится в диапазоне от 3300 до 5000 МГц, определен как основная полоса частот для внедрения 5G в 2020 году. Полоса пропускания канала, предоставляемая для 5G, должна составлять не менее 100 МГц на сеть, чтобы соответствовать всем требованиям. Реализация очень рентабельна, поскольку пропускная способность канала может быть увеличена без затрат на уплотнение сети. Использование С-диапазона в 5G может быть реализовано путем внедрения массивного MIMO из-за его приемлемой сложности и способности увеличивать пиковую, среднюю и граничную пропускную способность. Низкая частота, используемая для мобильных устройств, также может быть использована путем комбинирования частот от 3300 до 3800 МГц в качестве одной из функций 5G в стандартах 3GPP за счет использования сосуществующего восходящего канала LTE/NR.

Проблемы развертывания сети 5G.

Самая главная сложность связана с огромными возможностями 5G-сетей. Интеграция большого количества сервисов и услуг, а значит и разного вида трафика, с разными требованиями в качестве обслуживания, делает развертывание сети сложной задачей. Такие сети требуют постоянной оптимизации и мониторинга, что требует больших вычислительных мощностей и подключения таких технологий как машинное обучение и нейронные сети. Другой важной проблемой становится необходимость эффективного технического обслуживания гетерогенных сетей, так как сети нового поколения должны обеспечивать работу с сетями 2G, 3G и 4G. С многократным усложнением рабочих процессов и повышением затрат должны помочь справиться автоматизация процессов и применение искусственного интеллекта.

Мобильные сети работают в сетевой инфраструктуре, которая не ограничивается только электронными компонентами, но также включает пассивные элементы, такие как вышки, необходимые для работы сети. Совместное использование сетевой инфраструктуры становится все более популярным. И ожидается, что это продолжится в эпоху 5G, когда сети будут еще более уплотнены. Совместное использование пассивной инфраструктуры – это совместное использование неэлектронной инфраструктуры в узле сотовой связи, такой как система электропитания и управления, и физических элементов, таких как транспортные сети. Совместное использование активной инфраструктуры - это совместное использование электронной инфраструктуры сети, включая сеть радиодоступа (состоит из антенн/приемопередатчиков, базовой станции, транзитных сетей и контроллеров) и базовой сети (серверы и основные сетевые функции). Эта форма может быть далее классифицирована в MORAN (Multi-Operator Radio Access Network), где сети радиодоступа используются совместно, а выделенный спектр используется каждым оператором совместного использования, в MOCN (Multi-Operator Core Network), где совместно используются сети радиодоступа и спектр, а также в совместное использование основной сети, где используются общие серверы и основные сетевые функции. Совместное использование сетевой инфраструктуры позволяет значительно сократить

расходы операторов. Совместное использование сетевой инфраструктуры может препятствовать конкуренции между операторами мобильной связи.

Когда сетевая инфраструктура является совместно используемой, по своей сути трудно дифференцировать или подтверждать собственную сетевую инфраструктуру, чтобы конкурировать с партнерами по совместному использованию. Несмотря на то, что на основе услуг можно конкурировать, нормативные обязательства мобильных сетей имеют тенденцию сосредотачиваться на возможности подключения к сети и, следовательно, на инфраструктуре. Эту проблему можно свести к минимуму, если совместное использование ограничивается областью пассивной инфраструктуры. Поскольку активные компоненты можно дифференцировать, оптимизируя стоимость пассивной инфраструктуры, конкуренция между операторами совместного использования все еще может быть активной. Кроме того, очень сложно консолидировать существующую сетевую инфраструктуру для совместного использования. Существующая сеть является результатом этапов планирования и эксплуатации, основанных на конкретных требованиях оператора, и консолидация существующих сетей, вероятно, будет затруднена, если какие-либо требования противоречат друг другу. Совместное использование сетевой инфраструктуры может быть более осуществимо с вариантом, когда и радиодоступ, и базовые сети будут развернуты заново, при условии, что операторы будут сотрудничать на этапе планирования.

Собственное решение по эксплуатации сетей 5G предложила компания Huawei. «Решение нацелено на обеспечение умной эксплуатации и обслуживания сетей 5G и включает в себя возможности работы в режиме онлайн, полной автоматизации и применения технологий на базе ИИ, чтобы операторы могли успешно решать задачи по эксплуатации и обслуживанию сетей нового поколения», — пишет Фред Чжао (Fred Zhao), руководитель департамента по управлению сервисами и обеспечению их надежности компании Heavy Reading. [2]

Заключение

Разработка нового стандарта 5G началась с физического уровня будущей сети. Среди возможных кандидатов на технологию физического уровня: FBMC, F-OFDM, GFDM и UFMC. Наиболее привлекательными для разработчиков оказались F-OFDM и FBMC, которые использовались в тестовых версиях разрабатываемых систем. Использование на физическом уровне технологии Massive MIMO позволяет обеспечить низкую задержку в сети и высокие скорости передачи данных. Следующим вопросом при разработке систем нового поколения является осуществление одновременной работы нескольких стандартов связи, что требует возможности сопряжения работы устройств разных стандартов. Для решения этой задачи может использоваться концепция когнитивного радио, позволяющая перестраивать параметры передатчика, и тем самым адаптировать его для работы в другом стандарте или новой полосе частот. Третья важная задача - задача доступа к частотному ресурсу, может быть решена посредством динамического перераспределения спектра за счет его мониторинга, а также использования машинного обучения.

Литература

1. *Батуев Б.* Технологии 5G: поэтапное внедрение и элементная база для абонентского оборудования // Беспроводные технологии. №4. 2020. С. 15-27.
2. Какие задачи 5G ставит перед телеком-операторами и как их решать [Электронный ресурс] - URL:https://www.cnews.ru/articles/2020-07-16_kakie_zadachi_5g_stavit_pered_telekomoperatorami (дата обращения: 07.11.2020).
3. *Тихвинский В.О.* Динамическое управление радиочастотным ресурсом сетей 5G для различных видов доступа к РЧС // Электросвязь. №7. 2019. С. 18-22.
4. *Shaat, Musbah and F. Bader.* “Low complexity power loading scheme in cognitive radio networks: FBMC capability.” 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications (2009): 2597-2602.
5. *Tensubam, B.D., Chanu, N.L. and Singh, S.* Comparative Analysis of FBMC and OFDM Multicarrier Techniques for Wireless Communication Networks. International Journal of Computer Applications, 2014, 100, 27-31.
6. *Kansal P., Shankhwar A.K.* (2017). FBMC vs OFDM Waveform Contenders for 5G Wireless Communication System. Wireless Engineering and Technology, 8. С. 59-70.
7. *Akyildiz F., Kak A., Nie S.,* "6G and Beyond: The Future of Wireless Communications Systems," in IEEE Access, vol. 8, pp. 133995-134030, 2020, doi: 10.1109/ACCESS.2020.3010896.

8. *Панкратов Д.Ю., Степанова А.Г.* Компьютерное моделирование технологии MIMO для систем радиосвязи // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 12. С. 33-37.

9. *Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К.* Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 12. С. 24-30.

10. *Крейнделин В.Б., Старовойтов М.Ю.* Повышение помехоустойчивости системы связи MIMO с пространственным мультиплексированием методом додетекторного сложения // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 4-13.

11. *Крейнделин В.Б., Усачев В.А.* LTE-advanced pro как основа для новых сценариев M2M // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 3. С. 28-32.

12. *Бакулин М.Г., Крейнделин В.Б.* Проблема повышения спектральной эффективности и емкости в перспективных системах связи 6G // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 25-31.

13. *Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю.* Анализ пропускной способности канала mimo в условиях замираний // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 2. С. 13-20.

14. *Крейнделин В.Б., Панкратов Д.Ю.* Вероятностная модель радиоканала MIMO с учетом взаимной корреляции передающей и приемной сторон // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 1. С. 103-107.

15. *Крейнделин В.Б., Григорьева Е.Д.* Реализация банка цифровых фильтров с пониженной вычислительной сложностью // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 7. С. 48-53.

16. *Крейнделин В.Б., Григорьева Е.Д.* Модификация метода билинейного преобразования для синтеза цифровых фильтров // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 1. С. 4-9.

CURRENT STATE OF THE 5G NETWORK, PROSPECTS FOR DEVELOPMENT AND DEPLOYMENT 5G NETWORKS

Anastasia V. Ermakova,
Graduate MTUCI, Moscow, Russia,
msikisylia@gmail.com

Ksenia A. Babenko,
Graduate MTUCI, Moscow, Russia,
kcbabenko@yandex.ru

Natalia E. Miroshnikova,
Associate Professor of the Department of the RES, Ph.D., MTUCI, Moscow, Russia,
n.e.miroshnikova@mtuci.ru

Abstract

The article examines the current state and development prospects of fifth generation networks. A comparison of modulation methods that are candidates for the physical layer technology of 5G networks is given, the prospect of using the concept of cognitive radio in fifth-generation systems is considered, as well as ways to solve the problem of access to the frequency resource.

Keywords: *5G, mobile communication systems, modulation methods, internet of things, cognitive radio, dynamic spectrum access*

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДОВ ВИЗУАЛИЗАЦИИ ОДНОКОНАЛЬНЫХ ИЗОБРАЖЕНИЙ В УСЛОВНЫХ ЦВЕТАХ

Кремлева Элина Александровна
инженер кафедры ТиЗВ, МТУСИ, Москва, Россия,
krehlina@gmail.com

Власюк Игорь Викторович,
доцент кафедры ТиЗВ к.т.н., МТУСИ, Москва, Россия,
ru3dlp@yandex.ru

Аннотация

В работе рассмотрены этапы представления черно-белых изображений в условных цветах для систем прикладного телевидения. Изложены принципы выбора условных цветов и их обхода с учетом необходимости сохранения представления об исходной яркости объекта и оптимизации его визуального контрастирования. Представлены результаты проведенной цветовой обработки изображений, расчет эффективности выбранных алгоритмов и результаты повышения динамического диапазона изображения с помощью технологии HDR.

Ключевые слова: *одноканальные изображения, цветовая обработка изображения, псевдоцвета, квантование по яркости, преобразование яркости в цвет, динамический диапазон, технология HDR, Tone Mapping.*

В настоящее время одноканальные малоконтрастные изображения используются во многих областях таких как: промышленность, медицина, астрономия, правоохранительная деятельность, метеорология и многие другие (рис. 1), в каждой из которых используются различные источники формирования изображений (рентгеновские, радиоволновые, оптические, ультразвуковые и т.п.) [1]. После получения изображения необходимо представить его в виде, удобном для зрительного наблюдения и анализа.

Когда изображение отображается на устройстве вывода, человек может приступить к анализу данных, но не всегда легко работать с одноканальными изображениями. С какими же трудностями встречаются сотрудники различных организаций, при работе с одноканальными малоконтрастными изображениями?:

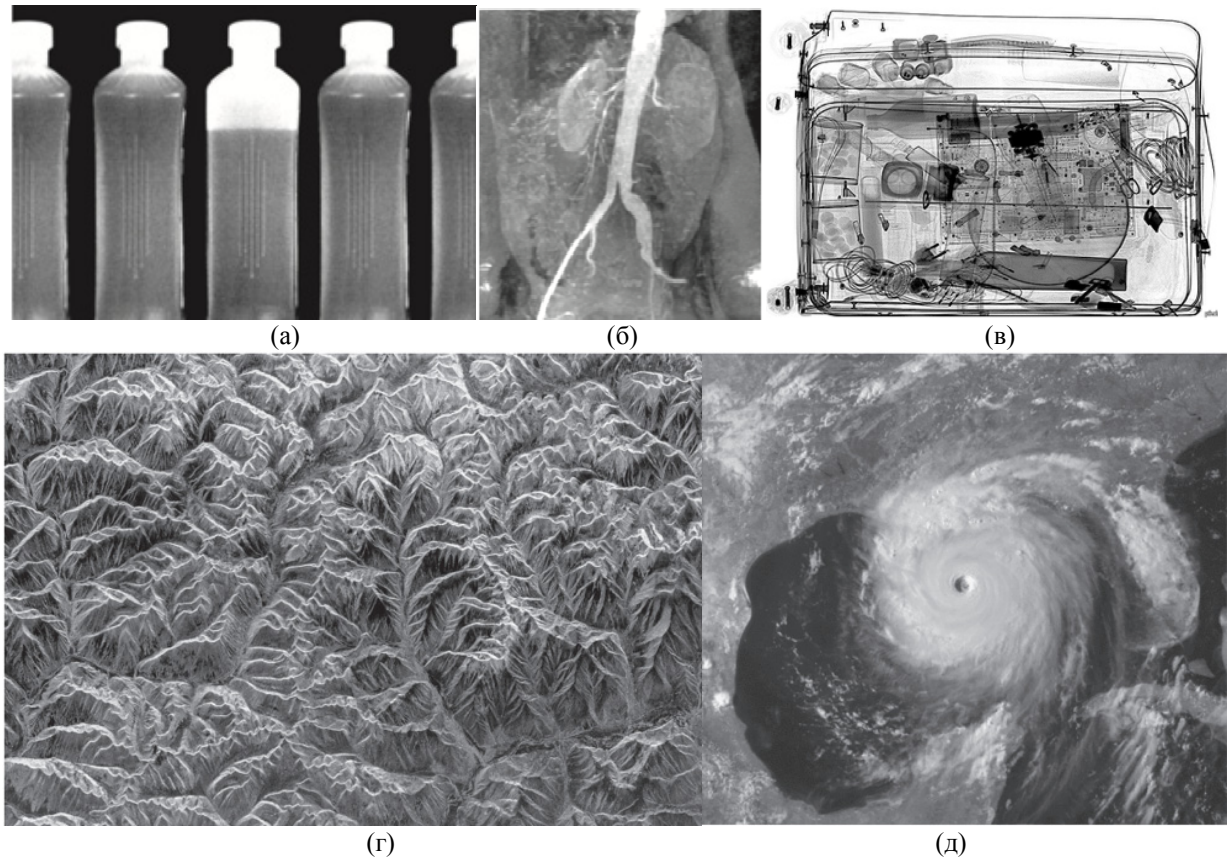
- Трудно заметить необходимую деталь. На рисунке 1(а) не составляет труда увидеть, что одна из бутылок недостаточно заполнена, в тоже время, чтобы найти на рисунке 1(в) необходимый предмет нужно потрудиться.
- Обработка большого количества малоконтрастных изображений за рабочий день.
- Человеческий глаз способен различить около двухсот градаций яркости [1].
- Утомление глаз. При длительной работе с компьютером, изображениями, содержащими мелкие детали, бумагами и выполнении процедур, требующих сосредоточенности взгляда, человек может ощущать быстрое утомление глаз. Напряжение в глазах может привести к ухудшению качества зрительных функций и снижению остроты зрения.

Применение цветовой обработки изображений может облегчить работу с одноканальными малоконтрастными изображениями. Как уже было сказано, человеческий глаз различает около двух сотен градаций яркости, но при этом в состоянии различить тысячи различных оттенков цвета. Еще одним преимуществом изображений, к которым была применена цветовая обработка, является то, что при работе с цветными изображениями проще распознавать и выделять объекты на изображении [2, 5-8].

Существуют два приёма цветовой обработки изображений:

- Обработка в натуральных цветах. Формирование изображения цветными устройствами регистрации изображения.

- Обработка в псевдоцветах (условных цветах). Присвоение цветов значениям пикселям монохромного изображения.



(а) (б) (в)

(г) (д)

Рис. 1. Примеры областей применения одноканальных малоконтрастных изображений: (а) Промышленность. Контроль выпускаемой продукции; (б) Медицина. Ангиограмма аорты; (в) Правоохранительная деятельность. Досмотр багажа; (г) Радиолокация. Горный массив на юго-востоке Тибета; (д) Метеорология. Ураган Катрина

В данной работе рассматривается обработка изображений в условных цветах, которые применяются для визуализации и интерпретации информации, содержащейся в полутоновых изображениях. Интенсивность черно-белого пикселя может быть задана 256 градациями серого, столько же градаций существует для каждого цвета. Квантование по яркости и преобразование яркости в цвет – основные методы обработки изображений.

Метод квантования по яркости и цветового кодирования является простейшим из методов обработки изображений в условных цветах. При работе этого метода пикселям присваиваются цвета в качестве уровней квантования. Изображение рассматривается как поверхность в трехмерном пространстве. Данный метод основывается на проведении плоскостей, каждая из которых параллельна координатной плоскости изображения и разделяет поверхность по области пересечения (рис. 2) [1].

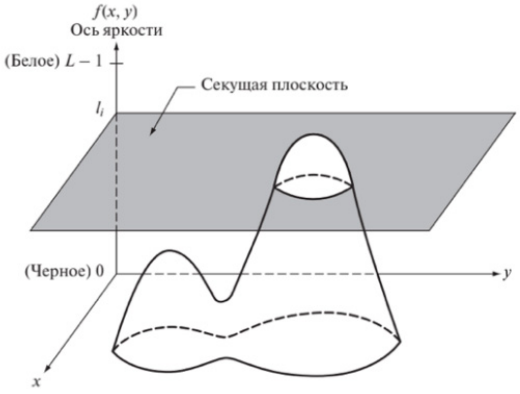


Рис. 2. Геометрическое объяснение метода квантования

Каждой стороне плоскости присваивается свой цвет. Пиксели, лежащие выше секущей плоскости, кодируются в один цвет, а в другой цвет кодируются пиксели, которые лежат ниже плоскости. Пикселям, находящимся на пересечении плоскости и поверхности, присваивается любой из использованных цветов. В итоге получается двуцветное изображение. При движении плоскости вдоль оси яркости вверх или вниз, меняется вид полученного изображения.

Метод преобразования яркости в цвет. Основная идея данного метода заключается в осуществлении трех независящих друг от друга преобразований значений яркости для каждого пикселя изображения (рис. 3). Полученные изображения подаются в красный, зеленый и синий каналы монитора, затем формируется составное изображение. Преобразования обычно не зависят от положения пикселя на изображении, а затрагивают только значения яркости.

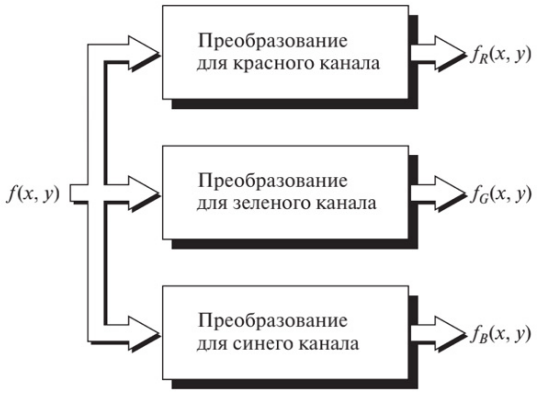


Рис. 3. Функциональная блок-схема формирования изображения в псевдоцветах. Величины f_R, f_G и f_B подаются в качестве входных сигналов соответственно в красный, зеленый и синий каналы цветного RGB-монитора

Но необходимо не только провести цветовую обработку изображения, но и подобрать такую цветовую гамму, которая была бы комфортна человеку, а глаза не перенапрягались. Например, длительное воздействие красного цвета на глаз приводит к чрезмерной усталости, какое же воздействие оказывает и синий цвет. Зеленый цвет оказывает благотворное влияние на зрение, понижает давление внутри глаза, позволяет расслабиться и успокоиться.

Учитывая, что методы преобразования изображений в псевдоцветах предназначены для улучшения визуального распознавания градаций изображения, эффективных и объективных параметров для оценки качества работы алгоритмов раскраски нет. В данной работе с целью повышения адекватности оценки качества раскраски и получения количественных результатов ее эффективности, помимо субъективных оценок окраски изображений, предлагается использовать тестовый шаблон, содержащий два смежных градационных клина, смещенных друг от друга на целое число градаций так, чтобы, например, уровень черного одно клина соответствовал темно-серой градации другого и т.д. Функция зависимости яркости от координаты пикселя определяется следующим образом [2]:

(2)

где и - координаты пикселя, L - яркость пикселя, N - количество битов, w и h - ширина и высота тестового изображения соответственно, δ - смещение между яркостями клиньев, *floor(x)* - целая часть числа (округленное в меньшую сторону).

Чтобы гарантировать отсутствие интерполяционных искажений, ширина и высота тестового изображения должны удовлетворять следующим критериям:

(3)

Под клиньями отображается шкала, делящая ширину изображения на 10 равных частей [2].

Оценка преимущества цветовой обработки будет проходить на основе тестового изображения (рис. 4), метод формирования которого описан выше.

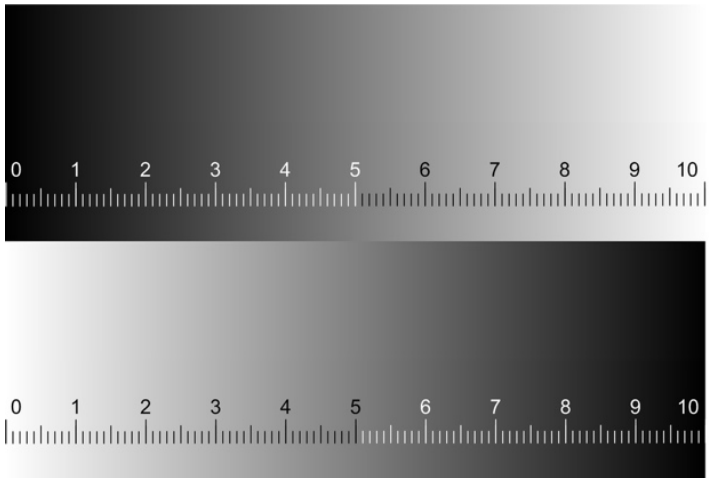


Рис. 4. Тестовое изображение

Алгоритмы цветового кодирования изображений могут иметь множество вариантов реализации. Например, спирально-треугольный алгоритм кодирования (рисунок 5(а)) дает постепенное увеличение яркости при приближении к центру. Недостатками данного алгоритма являются:

- Цвета внутренних треугольников близки между собой и плохо отличаются. Данный недостаток может привести к ошибкам в интерпретации оператором информации, содержащейся в полутоновом изображении.
- Уменьшение информативности цветокодированного изображения из-за уменьшения динамического диапазона сигналов от внутренних треугольников.
- Различия в яркости чистых спектральных цветов не учитываются, что может создать проблемы восприятия.

Пытаясь решить проблему с разницей в яркости, был создан стигмаобразный алгоритм (рисунок 5(б)). Алгоритм следует яркости спектральных цветов, начиная путь цветового кодирования в области самых «темных» цветов (синего), затем резко меняет путь в строну пурпурных цветов, далее движется в сторону зеленых, а заканчивается в области желтых цветов (самой яркой). При этом алгоритм «обходит» точку белого.

Данный алгоритм дает более равномерное изменение условных цветов, но изменение яркости при прохождении пути кодирования внутри треугольника RGB неравномерно, также плохо охватывается красная часть спектра.

Круговой алгоритм цветового кодирования (рисунок 5(в)) обеспечивает равномерный охват каждого цвета. Путь алгоритма начинается в начальной точке, затем движется по кругу вокруг точки белого и завершается в конечной точке.

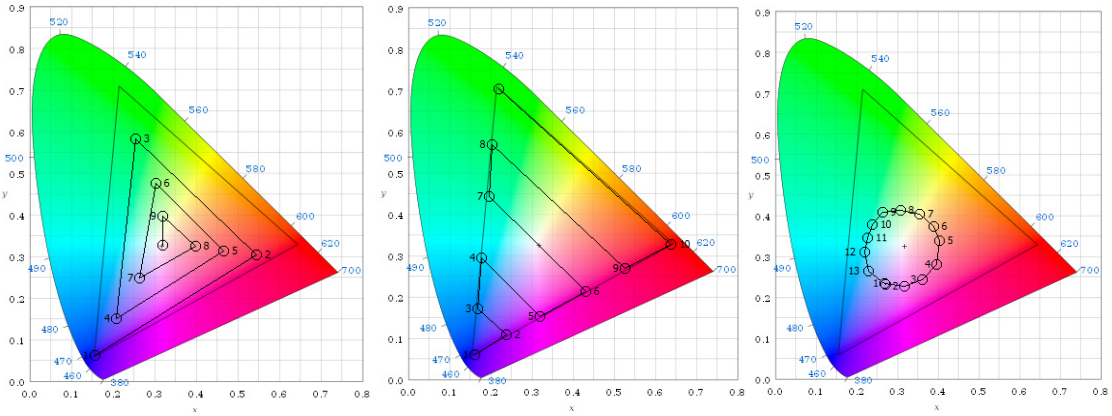
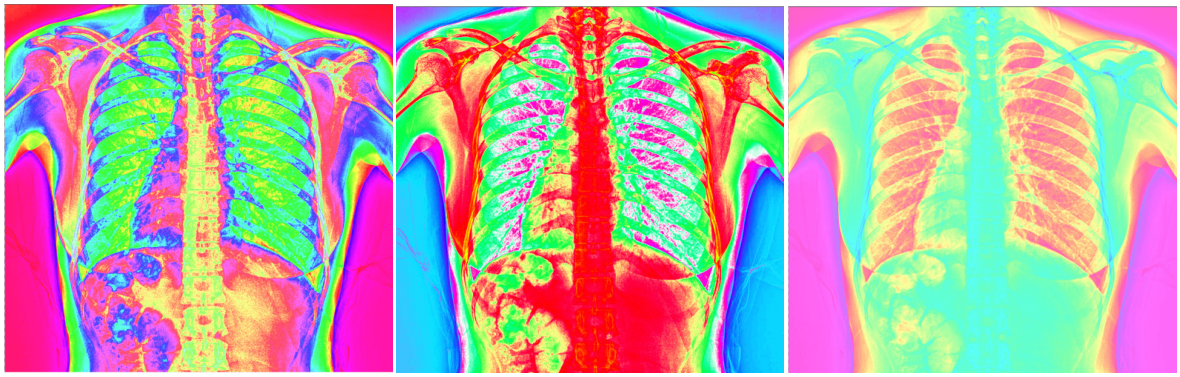


Рис. 5. Алгоритмы цветного кодирования изображений:
(а) - Спирально-треугольный алгоритм; (б) - Стигмаобразный алгоритм; (в) - Круговой алгоритм

При выборе алгоритма цветового кодирования необходимо основываться на поставленной задаче и подобрать такой алгоритм, который наилучшим образом справится с ней.

Результаты применения вышеперечисленных алгоритмов на рентгеновском снимке грудной клетки представлены на рисунке 6 (а-в).



а) б) в)

Рис. 6. Рентгеновский снимок грудной клетки после цветового кодирования.
(а) - Спирально-треугольный алгоритм, (б) - Стигмаобразный алгоритм, (в) - Круговой алгоритм

Основываясь на полученных изображениях после цветовой обработки (рис. 6 а-в), можно сделать вывод, что ни один из представленных методов не подходит для выполнения нашей задачи. Поэтому был выбран другой алгоритм обработки (рис. 7) и после этого была произведена раскраска изображения (рис. 8). На полученном изображении становятся заметны перепады между клиньями, а на исходном изображении – это незаметно.

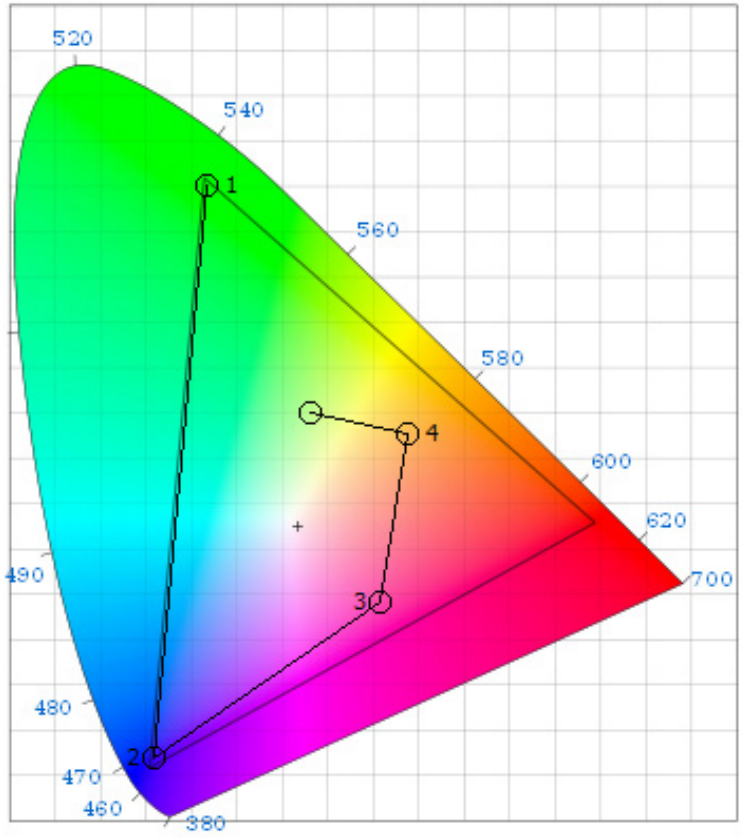


Рис. 7. Алгоритм цветовой обработки изображения

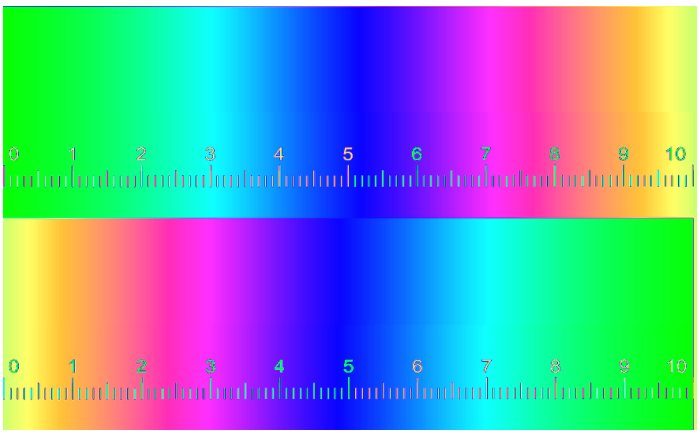


Рис. 8. Изображение, полученное после цветовой обработки

После проведения цветовой обработки можно оценить эффективность выбранного алгоритма. Она оценивается, как отношение количества делений шкалы (находящихся в нижней части изображения), на которых заметен перепад, к общему числу делений [3]:

—— (1)

На основе формулы (1) была рассчитана эффективность выбранного алгоритма:

—

Для получения более высокого значения эффективности был выбран другой алгоритм обработки (рис. 9 и 10).

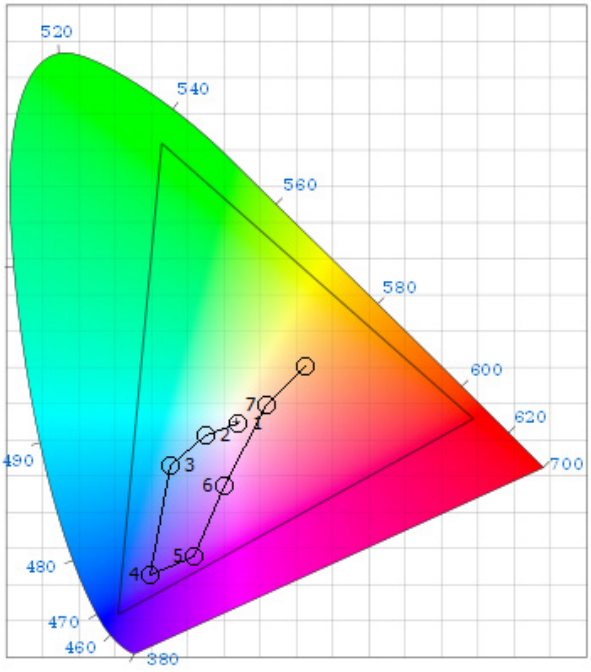


Рис. 9. Алгоритм цветовой обработки изображения

Оценка эффективности второго алгоритма:

—

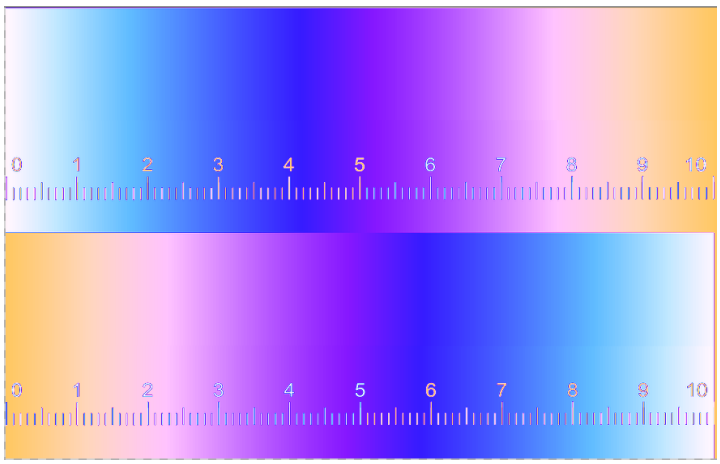


Рис. 10. Изображение, полученное после цветовой обработки

После сравнения полученных значений эффективности двух алгоритмов, было установлено, что эффективность второго алгоритма почти в два раза выше, чем у первого.

На рисунке 11 представлены результаты использования ранее упомянутых алгоритмов на рентгеновском снимке грудной клетки. Проанализируем изображение, полученное с помощью первого алгоритма (рис. 11а):

- Выбранный алгоритм достаточно плохо выделил кости. Почти невозможно рассмотреть позвоночник, плечевые суставы и грудную клетку немного проще рассмотреть.
- Силуэт хорошо выделен на общем фоне.
- Очень яркие цвета, может возникнуть чувство дискомфорта в глазах. Гистограмма рисунка 11(а) представлена на рисунке 12.

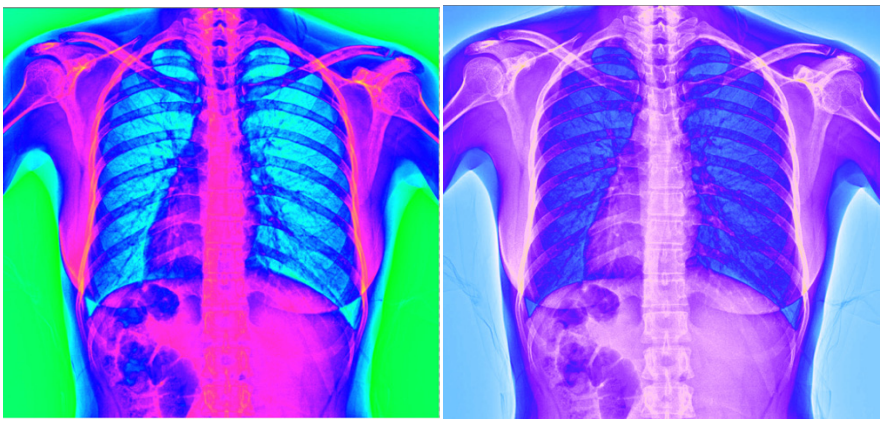


Рис. 11. Рентгеновский снимок грудной клетки:
(а) - После цветовой обработки с помощью первого алгоритма;
(б) - После цветовой обработки с помощью второго алгоритма

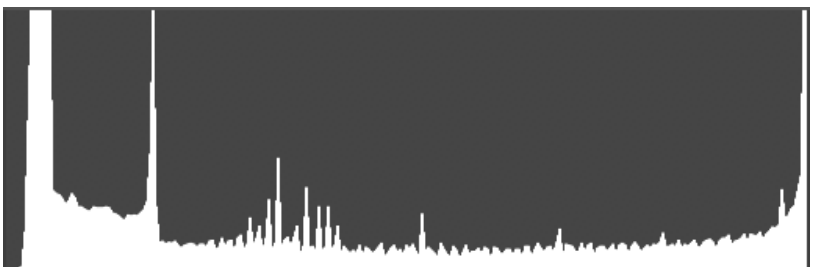


Рис. 12. Гистограмма рентгеновского снимка после обработки с помощью первого алгоритма

Анализ результатов обработки рентгеновского снимка с помощью второго алгоритма (рис. 11б):

- Хорошо различимы плечевые суставы.

- Легко распознать позвоночник и каждый позвонок в отдельности.
- Заметны некоторые внутренние органы: кишечник и легкие.
- Не очень хорошо выделены ребра, трудно определить их состояние.
- Границы между фоном и силуэтом хорошо определены.
- На изображении преобладают оттенки синего цвета. Свет, поступающий в глаза, будет холодным, что может способствовать утомляемости глаз.

Каждый из выбранных алгоритмов имеют свои недостатки и преимущества, которые могут серьезно повлиять на результаты анализа изображения.

Помимо цветовой обработки распознаваемость деталей можно повысить путем увеличения динамического диапазона изображения. Динамический диапазон – отношение между максимальным и минимальным уровнями яркости. Для реализации данной идеи можно использовать уже имеющуюся технологию HDR (High Dynamic Range). Принцип её работы таков: создается несколько изображений с различными уровнями экспозиции, далее они накладываются друг на друга и объединяются с помощью специальных алгоритмов, после чего получается изображение с хорошей детализацией в тенях и в более светлых участках [4]. Далее изображение подвергается цветовой обработке и выводится на специальные мониторы, способные отображать изображения с расширенным динамическим диапазоном. В ином случае, чтобы при выводе изображения на устройства сохранить полезную информация, необходимо преобразовывать изображения к модели LDR, которая используется на большинстве дисплеев, с помощью процесса Tone Mapping (тональное отображение). Данный процесс корректирует общую овещенность изображения, опираясь на яркость средних тонов, а чтобы войти в выходной динамический диапазон яркость светлых пикселей уменьшается, а темных – увеличивается. Потеря некоторой информации неизбежна, но при правильном выборе алгоритма Tone Mapping и предварительной цветовой обработке изображения большая часть полезной информации сохраняется.

Заключение

Исходя из проделанных экспериментов видно, что при выборе алгоритма цветового кодирования нужно отталкиваться от поставленной задачи. Использование изображений с расширенным динамическим диапазоном, к которым была применена цветовая обработка, может существенно облегчить анализ изображений, так как несёт в себе больше информации. Чтобы сохранить большую часть полезной информации при отображении изображений на любых мониторах необходимо использовать алгоритмы Tone Mapping.

Литература

1. *Р.Гонсалес, Р.Вудс, С.Эддинс.* Перевод с английского *В.В.Чепыжова. А.И.Солонина, С.М.Арбузов.* Цифровая обработка изображений в среде MATLAB // Техносфера. 2006. 618 с.
2. *Potashnikov A.M., Vlasuyk I.V., Ivanchev V.V., Balobanov A.V.* The method of representing grayscale images in pseudo color using equal-contrast color space // 2020 Systems of signals generating and processing in the field of on board communications. Institute of Electrical and Electronics Engineers Inc. 2020. 9078584.
3. *Балобанов А.В. Врагова М.В. Фаблов Д.А.* Методические указания к лабораторной работе №63. Исследование обработки изображений в псевдоцветах. 2010. 15 с.
4. *Francesco Banterle, Alessandro Artusi, Kurt Debattista, Alan Chalmers.* Advanced High Dynamic Range Imaging: Theory and Practice // A K Peters/CRC Press. 2011. 352 с.
5. *Поташников А.М., Власюк И.В*. Метод построения равноконтрастного цветового пространства для заданной системы отображения информации и условий контроля // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 15-22.
6. *Пушкина Е.В., Фролова М.М., Власюк И.В*. Исследование и разработка метода реставрационной обработки сигналов для систем цифрового телевидения // Телекоммуникации и информационные технологии. 2016. Т. 3. № 1. С. 55-58.
7. *Valitskaya N.S., Vlasyuk I.V., Potashnikov A.M*. Video compression method on the basis of discrete wavelet transform for application in video information systems with non-standard parameters // T-Comm. 2020. Т. 14. № 3. С. 47-53.
8. *Власюк И.В., Любецкая В.Ю.* Анализ методов подавления артефактов звона, возникающих на изображениях в процессе кодирования с wavelet-преобразованием // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 4. С. 53-58.

EVALUATION OF THE EFFECTIVENESS OF VISUALIZATION TECHNIQUES FOR SINGLE CHANNEL IMAGES IN A CONDITIONAL COLORS

Elina A. Kremleva,
Engineer of the Department of T&SB, MTUCI, Moscow, Russia,
krehlina@gmail.com

Igor V. Vlasuyk,
Associate Professor of the Department of the T&SB, PhD., MTUCI, Moscow, Russia,
ru3dlp@yandex.ru

Abstract

The paper considers the stages of presenting black-and-white images in conventional colors for applied television systems. The principles of selecting conditional colors and bypassing them are shown, taking into account the need to preserve the idea of the original brightness of the object and optimize its visual contrast. The results of color image processing, calculation of the efficiency of the selected algorithms, and results of increasing the dynamic range of the image using HDR technology are presented.

Keywords*: single-channel images, color image processing, pseudo-colors, brightness quantization, brightness-to-color conversion, efficiency, dynamic range, HDR technology, Tone Mapping.*

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ РАБОТ В ПРЕПОДАВАНИИ ДИСЦИПЛИНЫ «ОСНОВЫ КОМПЬЮТЕРНОГОАНАЛИЗА ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ»

Казина Елизавета Владимировна,
студент МТУСИ, Москва, Россия,
lizakazinamtuci@gmail.com

Тупиков Илья Владиславович,
студент МТУСИ, Москва, Россия,
worst.angr@gmail.com

Каретина Марина Александровна,
студент МТУСИ, Москва, Россия,
m-karetina@mail.ru

Шманев Антон Олегович,
студент МТУСИ, Москва, Россия,
aoshmanev@gmail.com

Григорьева Елена Дмитриевна,
доцент кафедры ТЭЦ, к.т.н., МТУСИ, Москва, Россия,
e.d.grigoreva@mtuci.ru

Аннотация

Современный процесс обучения строится на основе использования передовых технологий разработки телекоммуникационных устройств. Соответственно встаёт вопрос разработки совершенно новых пособий для студентов, в частности таковыми пособиями являются виртуальные лабораторные работы, позволяющие упростить и ускорить процесс изучения нового материала. Основными плюсами подобного подхода является наглядность и гибкость в применении для исследования различных задач в области электрических цепей. Современный специалист в первую очередь должен чётко понимать и представлять физические основы процессов, протекающих в электронных цепях, так как в силу существования специализированного программного обеспечения ручной расчёт давно потерял свою актуальность. Однако использование специализированного программного обеспечения в процессе обучения студентов затруднено в силу дороговизны подобного проприетарного программного обеспечения. В свою очередь создание пользовательского приложения позволяет избавиться от ручных расчётов и сделать акцент на самой задаче и наглядном представлении её решения в формате графиков. Помимо того, разработка аналогичных программ или усовершенствование уже существующих является простой задачей, так как существует возможность использования ранее созданных DLL-библиотек, содержащих основные универсальные функции, в качестве основы для решения новых задач.

Ключевые слова*: виртуальная лабораторная работа, полосковые линии, среда программирования, программное обеспечение Visual C++, проприетарное программное обеспечение.*

Представлены результаты разработки узкоспециализированных пользовательских приложений. В качестве объекта исследования была выбрана задача расчёта конструкции фильтра нижних частот на полосковых линиях передачи, используемого в диапазоне СВЧ. В качестве среды программирования избран Visual C++ в силу того, что данное программное обеспечение обладает требуемой гибкостью. Все расчёты и графики, полученные в созданной программе, проверялись в среде Mathcad [4-10].

Постановка задачи разработки ФНЧ на полосковых линиях

Радиотехнические устройства, работающие в диапазоне ультракоротких волн, как правило, не содержат катушек индуктивности и конденсаторов, то есть индуктивных и ёмкостных элементов с сосредоточенными параметрами. Геометрические размеры этих элементов оказываются очень малыми, что усложняет их изготовление. Ещё более важным фактором является то, что в элементах с сосредоточенными параметрами в диапазоне сверхвысоких частот проявляются паразитные параметры элементов, вызываемые излучением энергии. Поэтому, при разработке радиотехнических устройств для работы в диапазоне ультракоротких волн, в большинстве случаев, используются отрезки линий передачи, которые эквивалентны индуктивным и ёмкостным элементам [1].

Величина и характер (индуктивный или ёмкостный) сопротивления отрезка полосковой линии передачи зависят от длины отрезка l и волнового сопротивления $Z_в$. Формулы (1) и (2) получены из уравнений передачи цепей с распределёнными параметрами в режимах короткого замыкания и холостого хода соответственно [1]:

$$X_L = 2\pi \cdot f \cdot L = Z_в \cdot tg\left(\frac{2\pi \cdot l_{кз}}{\lambda}\right) \quad (1)$$

$$X_C = \frac{1}{2\pi \cdot f \cdot C} = \frac{Z_в}{tg\left(\frac{2\pi \cdot l_{xx}}{\lambda}\right)} \quad (2)$$

где l – длина отрезка полосковой линии в режимах короткого замыкания или холостого хода; $\lambda = \frac{v_ф}{f}$ – длина волны, $v_ф$ – фазовая скорость, f – частота, $Z_в$ – волновое сопротивление.

На основании формул (1) и (2) длины отрезков полосковых линий в режимах короткого замыкания или холостого хода выражаются через параметры реактивных элементов следующим образом:

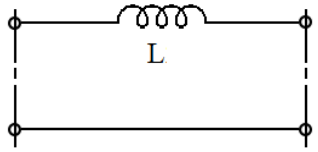
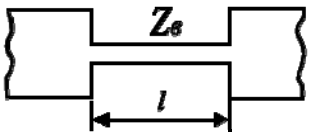
$$l_{\text{инд(кз)}} = \frac{\lambda}{2\pi} \cdot arctg\left(\frac{2\pi f_1 \cdot L}{Z_в}\right) \quad (3)$$

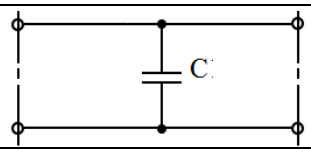
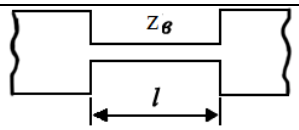
$$l_{\text{емк(xx)}} = \frac{\lambda}{2\pi} \cdot arctg\left(2\pi f_1 \cdot C \cdot Z_в\right) \quad (4)$$

Характеристики элементов с сосредоточенными параметрами и элементов с распределёнными параметрами связаны соотношениями, представленными в таблице 1.

Таблица 1

Представление цепей на элементах с сосредоточенными параметрами с помощью элементов с распределёнными параметрами.

Звено фильтра на элементе с сосредоточенными параметрами	Звено фильтра на элементы с распределёнными параметрами	Расчётные формулы при условии $\left(l < \frac{\lambda}{8}\right)$
		$l_{кз} = \frac{\lambda}{2\pi} \cdot arctg\left(\frac{2\pi f_1 \cdot L}{Z_в}\right)$

		$l_{xx} = \frac{\lambda}{2\pi} \cdot arctg\left(2\pi f_1 \cdot C \cdot Z_в\right)$

Если короткий отрезок линии передачи с достаточно высоким волновым сопротивлением $Z_в$ подключить в разрыв линии со значительно меньшим волновым сопротивлением (эквивалентным режиму короткого замыкания) $z_в \ll Z_в$, то согласно формулы (3), такой отрезок линии передачи будет эквивалентен четырёхполюснику с индуктивным элементом в продольной ветви.

Аналогично, если включить отрезок с малым волновым сопротивлением $z_в$ в разрыв линии передачи со значительно большим волновым сопротивлением (эквивалентным режиму холостого хода) $Z_в \gg z_в$, то согласно (4) такой отрезок линии будет эквивалентен четырёхполюснику с ёмкостным элементом, включённым в поперечную ветвь [2].

Задание: сконструировать ФНЧ из отрезков однородной линии передачи с максимально плоской частотной характеристикой (характеристикой Баттерворта), удовлетворяющий следующим требованиям:

– частота среза f_1 = 1 ГГц;

– граничная частота полосы непропускания f_S = 2 ГГц;

– минимально допустимое ослабление в полосе непропускания A_S = 30 дБ;

– фильтр встраивается в линию передачи с волновым сопротивлением 25 Ом;

– фильтр реализуется на отрезках полосковой линии с относительной толщиной полоски $t / b = 0,05$ и относительной диэлектрической проницаемостью заполняющего диэлектрика $\varepsilon_r = 4$.

Расчёт фильтра

1. Выполняем нормирование частотной переменной относительно частоты среза. Определяем порядок фильтра N = 5 и корни характеристического уравнения.

2. Для реализации фильтра на полосковых элементах выбираем лестничную структуру (рисунок 1) с индуктивными элементами в продольных ветвях и ёмкостными элементами – в поперечных. Такая топологическая схема удовлетворяет требованиям к реализации фильтра на полосковых элементах [3].

3.

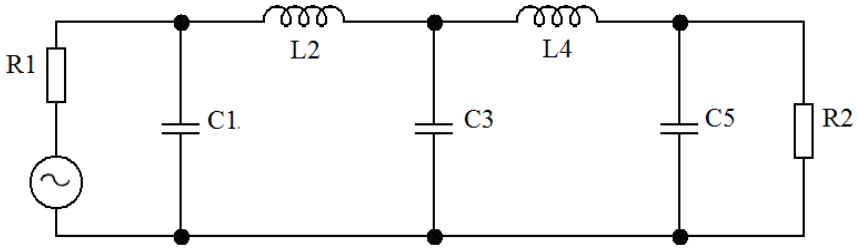


Рис. 1. Топологическая схема

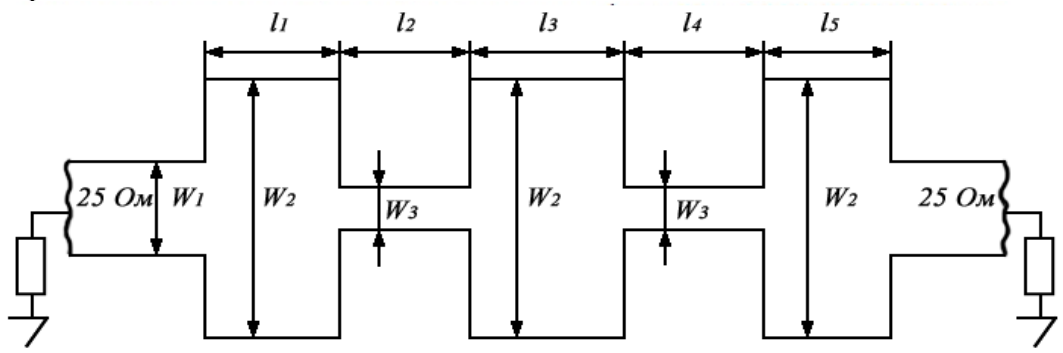
4. По известной методике синтеза фильтров на L-C элементах рассчитываем нормированные параметры элементов ФНЧ-прототипа:

$\hat{r}_1$	$\hat{C}_1$	$\hat{l}_2$	$\hat{C}_3$	$\hat{l}_4$	$\hat{C}_5$	$\hat{r}_2$
1	0,618	1,618	2	1,618	0,618	1

5. Денормированные значения параметров элементов:

R_1	C_1	L_2	C_3	L_4	C_5	R_2
25 Ом	$3,935 \cdot 10^{-12}$ Ф	$6,438 \cdot 10^{-9}$ Гн	$12,73 \cdot 10^{-12}$ Ф	$6,438 \cdot 10^{-9}$ Гн	$3,935 \cdot 10^{-12}$ Ф	25 Ом

6. На рисунке 2 представлена эквивалентная схема фильтра на элементах с распределёнными параметрами.



Тип элемента R_1	C_1	L_2	C_3	L_4	C_5	R_2
Волновое сопротивл.	$z_в$ =12,5Ом	$Z_в$=70 Ом	$z_в$ =12,5Ом	$Z_в$=70 Ом	$z_в$ =12,5Ом	
Ширина: W_1 =5мм	W_2 =150 мм	W_3 =1 мм	W_2 =150 мм	W_3 =1 мм	W_2=150 мм	W_1 =5мм
Длина:	l_1 =2,49см	l_2 =1,25см	l_3 =3,328см	l_4 =1,25см	l_5 =2,49см	

Рис 2. Схема фильтра на элементах с распределёнными параметрами

Результаты вычислений представлены в таблице 2.

Таблица 2

Результаты вычислений

Вычисление параметров элементов ФНЧ-прототипа при $f_1 = 1$ ГГц, $\omega_1 = 2\pi \cdot 10^9$, $R_н = 25$ Ом			
$C_1 = C_3$, пФ	C_2, пФ	$L_1 = L_2$, нГн	$R_1 = R_2$, Ом
3,935	12,73	6,438	25
Ослабление, вносимое фильтром на граничной частоте полосы непропускания $f_2 = 2$ ГГц			
$A(f_2) = 30,087$ дБ			
Вычисление длин отрезков линий, реализующих индуктивности при $L_1 = L_2 = 6{,}438$ нГн, $f_1 = 10^9$ Гц, $Z_в = 70$ Ом			
$l_{инд1} = l_{инд2} = 1,251$ см			
Вычисление длины отрезка линии, реализующего ёмкости при $C_1 = C_5 = 3,935$ пФ, $f_1 = 10^9$ Гц, $z_в = 12,5$ Ом и при $C_3 = 12,73$ пФ			
для $C_1; C_5$		для C_2	
$l_C = 2,499$ см		$l_C = 3,328$ см	

Разработка приложения на языке Visual C++

Для создания программы, позволяющей решить поставленную задачу, был создан новый проект CLR (.NET Framework) с целевой версией платформы NET Framework: v4.7.2. В целях оптимизации процесса разработки была создана библиотека классов среды CLR, содержащая базовые функции, используемые во всем проекте, а также библиотеку символов греческого алфавита соответствующих физическим величинам, используемым в расчётах. Помимо того, по мере разработке программы использовались такие системные заголовочные файлы как:

- "math.h" – содержащий набор математических функций
- <iostream> – содержащий функции и переменные для организации ввода-вывода в языке программирования C++
- <complex> – содержащий объявления функций для комплексной арифметики

Помимо этого, была использована директива #define _USE_MATH_DEFINES позволяющая вызвать предопределённую внутри среды программирования константу пи для расчетов высокой точности.

Среди элементов конструктора были использованы:

- Button – для создания кнопок
- Label – для создания подписей и комментариев в окне приложения
- TextBox – для осуществления ввода исходных данных расчётов в программу
- Chart – для построения графиков

На рисунке 3 представлено окно программы, представляющей ввод исходных требований к фильтру, вводимых пользователем, и вывод параметров фильтра на полосковых элементах.

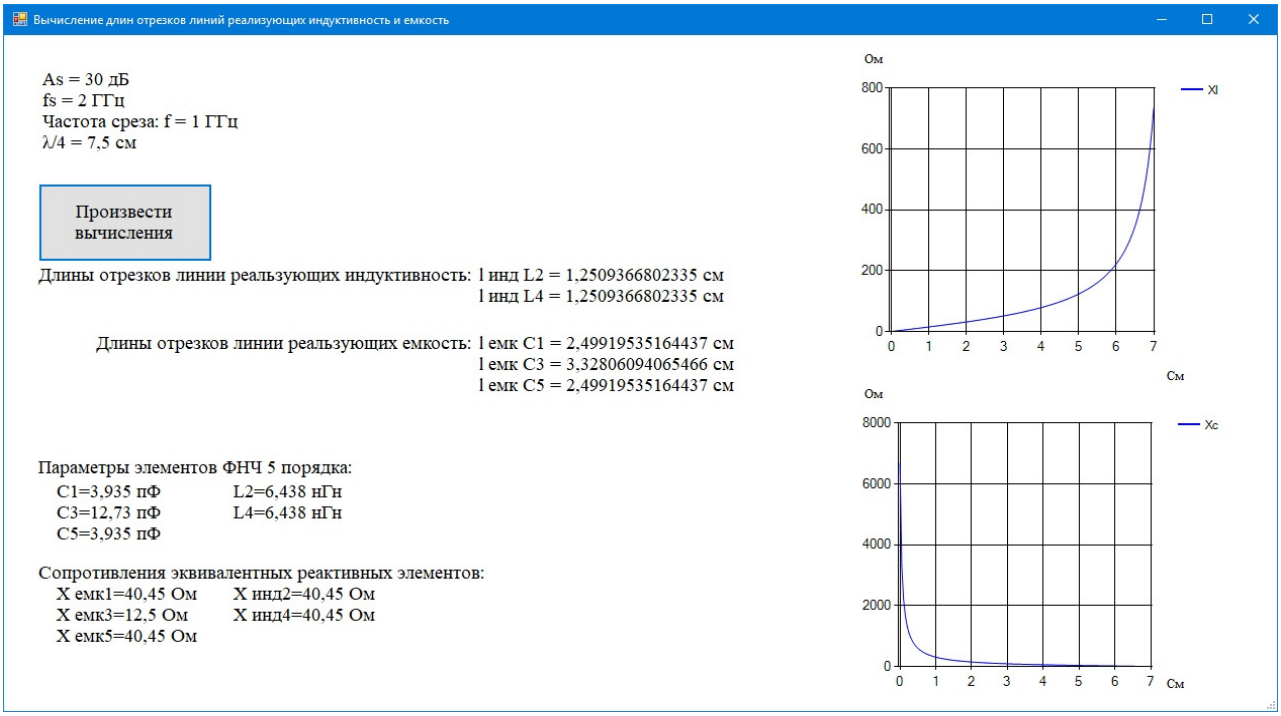


Рис. 3. Окно программы, содержащее функцию расчёта

Важно отметить, что погрешность вычислений задаётся при разработке программы и таким образом, существует возможность определения необходимой точности расчётов в зависимости от поставленной задачи. Помимо гибкой настройки точности вычисления, необходимо обратить внимание на то, что модульная структура языка C++ позволяет использовать многие функции, написанные в ходе разработки данного проекта и при создании новых программ, что позволяет сэкономить время и упростить решение последующих задач.

Заключение

Проведённая работа позволяет сделать вывод о том, что создание и использование в учебном процессе виртуальных лабораторных работ является эффективным методом оптимизации учебного процесса, позволяющим наглядно представить решение тех или иных задач в рамках курса. Кроме того, собственная разработка виртуальных лабораторных работ предоставляет возможность избежать применения проприетарного программного обеспечения.

Литература

1. *Бакалов В.П., Дмитриков В.Ф., Крук Б.И.* Основы теории цепей. М.: Горячая линия-Телеком, 2013. 596 с.
2. *А.Таланов*. Микрополосковые фильтры. «Электронные компоненты», 2019. №5.
3. *В. Фуско*. СВЧ цепи. Анализ и автоматизированное проектирование. Под. ред. В.И. Вольмана. – М.: Радио и связь, 1990. 288 с.

4. *Тихомирова Е.О., Барков А.С., Степанова А.Г.* Фильтры в Matlab // Телекоммуникации и информационные технологии. 2016. Т. 3. № 1. С. 71-74.

5. *Григорьева Е.Д., Семёнова Т.Н., Степанова А.Г.* Информационные технологии в организации самостоятельной работы студентов при изучении дисциплины "Электротехника" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 3. С. 26-28.

6. *Григорьева Е.Д., Семёнова Т.Н., Степанова А.Г.* Методическое обеспечение самостоятельной работы студентов при изучении дисциплины "Электротехника" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2017. Т. 6. № 2. С. 16-19.

7. *Крейнделин В.Б., Григорьева Е.Д.* Модификация метода билинейного преобразования для синтеза цифровых фильтров // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 1. С. 4-9.

8. *Крейнделин В.Б., Григорьева Е.Д.* Реализация банка цифровых фильтров с пониженной вычислительной сложностью // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 7. С. 48-53.

9. *Крейнделин В.Б., Григорьева Е.Д.* Применение системы Matlab в самостоятельной работе студентов при изучении дисциплины "теория электрических цепей" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2018. Т. 7. № 2. С. 25-27.

10. *Григорьева Е.Д., Семёнова Т.Н., Степанова А.Г.* Организация самостоятельной работы студентов с применением электронного учебника при изучении дисциплины "теория электрических цепей" // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2018. Т. 7. № 2. С. 7-9.

USE OF VIRTUAL LABORATORY WORK IN TEACHING THE DISCIPLINE «FUNDAMENTALS OF COMPUTER ANALYSIS OF ELECTRICAL CIRCUITS»

Kazina Elizaveta Vladimirovna,
Student MTUCI, Moscow, Russia,
lizakazinamtuci@gmail.com

Tupikov Ilya Vladislavovich,
Student MTUCI, Moscow, Russia,
worst.angr@gmail.com

Karetina Marina Aleksandrovna,
Student MTUCI, Moscow, Russia,
m-karetina@mail.ru

Shmanev Anton Olegovich,
Student MTUCI, Moscow, Russia,
aoshmanev@gmail.com

Yelena D.Grigoreva,
Associate Professor of the Department of the TEC, PhD., MTUCI, Moscow, Russia,
e.d.grigoreva@mtuci.ru

Abstract

The modern learning process is based on the use of advanced technologies for developing telecommunications devices. Accordingly, there is a question of developing completely new manuals for students, in particular, such manuals are virtual laboratory work that allows you to simplify and speed up the process of learning new material. The main advantages of this approach are the visibility and flexibility in application to research various problems in the field of electrical circuits. A modern specialist should first of all clearly understand and represent the physical basis of the processes occurring in electronic circuits, since due to the existence of specialized software, manual calculation has long lost its relevance. However, the use of specialized software in the process of teaching students is difficult due to the high cost of such proprietary software. In turn, creating a custom application allows you to get rid of manual calculations, and focus on the problem itself and visual representation of its solution in the format of graphs. In addition, developing similar programs or improving existing ones is a simple task, since it is possible to use previously created DLL libraries containing basic universal functions as the basis for solving new problems.

Keywords: *Virtual lab work, stripe transmission lines, programming environment, Visual C++ software, proprietary software*.

ПРИМЕНЕНИЕ МЕТАМАТЕРИАЛОВ В АНТЕННЫХ СИСТЕМАХ

Машкова Маргарита Антоновна,
студент МТУСИ, Москва, Россия,
MargaritaMashckova20@yandex.ru

Саргсян Александра Давитовна,
студент МТУСИ, Москва, Россия,
alexa.sargsyan@bk.ru

Каравашкина Валентина Николаевна,
доцент кафедры «Электроника», к.т.н., МТУСИ, Москва, Россия,
v.n.karavashkina@mtuci.ru

Аннотация

Представлена краткая историческая справка по развитию метаматериалов. Рассмотрена классификация метаматериалов по степени преломления и электродинамическим свойствам. Приведены примеры использования метаматериалов в радиотехнических устройствах. Описаны способы применения метаматериалов и метаструктур в конструкциях электрически малых и рупорных антенн и излучателей.

Ключевые слова: *метаматериалы, метаструктуры, диэлектрическая проницаемость, магнитная проницаемость, электрически малые антенны, рупорные антенны, широкополосность, минитюаризация.*

Ещё в середине прошлого столетия создание материалов со свойствами, на первый взгляд сложно согласующимися с законами физики, позволяющими воплотить самые смелые фантазии о сверхминиатюрной технике, мощных лазерах и даже невидимости, казалось если не антинаучной сказкой, то по крайней мере технологически сложной привилегией будущего. Но уже сейчас невероятная скорость научного прогресса позволяет воплотить в жизнь многие смелые фантазии и оставляет огромный простор для воображения. Да, на данный момент у нас по-прежнему нет невидимых глазу самолетов и плащей-невидимок, и вряд ли в ближайшем будущем мы сможем на них рассчитывать. Но уже сейчас мы можем создавать конструкции, невидимые для излучения инфракрасного, красного и сине-зеленого спектра. Для этих целей современные технологии позволяют создавать совершенно необычные по свойствам материалы, названные «метаматериалами». Данный класс материалов уже широко применяется в радиотехнике, военной технике, медицине, в космической отрасти и других областях. Рассмотрим в данной статье использование метаматериалов в радиотехнических устройствах, в частности в антенных системах.

Говоря о метаматериалах нельзя ограничиться лишь простым определением их искусственно созданной многокомпонентной структуры. Имея поистине потрясающую природу, метаматериалы по праву занимают место среди главных научных достижений современности. Особая периодическая структура этих материалов обеспечивает их различными оптическими, электромагнитными и другими свойствами, практически не встречающимися у материалов природного происхождения. Особого внимания заслуживают отрицательная магнитная и диэлектрическая проницаемости. Как будет показано ниже, именно они и будут определяющими в использовании этих материалов в антенных системах.

Уже само название «метаматериалы» позволяет судить об их необычных свойствах – заимствованная из греческого языка приставка «мета-» означает «вне». Такой выбор названия неслучаен: необычные свойства метаматериалы приобретают не за счет индивидуальных свойств материалов, из которых они состоят, а благодаря микроструктуре композитных материалов [1, 6, 7].

Первым в своих работах о них написал Джагадис Чандра Бозе еще в конце 19 века, упомянув о своем микроволновом эксперименте, в котором он исследовал поляризационные свойства искрив-

ленных структур.

В 1950-х годах американский инженер и исследователь Уинстон Э. Кок сконструировал микроволновые линзы, являющих собой совокупность периодически расположенных металлических полосок, проводящих сфер и дисков. Такая конструкция позволяла получить необычный эффективный показатель преломления, что приближало ее к структуре метаматериала. Таким образом, Уинстон Э. Кок и созданная им среда еще на один шаг приблизили человечество к эре метаматериалов.

Первым из советских ученых о метаматериалах написал Виктор Георгиевич Веселаго в 1967 году. В одной из своих статей он упомянул, что допускает существование так называемых «левосторонних» материалов. И если «обычные», «правосторонние» материалы обладали положительным коэффициентом преломления, то «левосторонние», наоборот, по словам В.Г.Веселаго, обладали коэффициентом преломления, меньшим нуля. Подобное отличие существенно повлияло на разницу оптических свойств этих материалов. Однако гипотеза В.Г.Веселаго на тот момент не нашла подтверждения, так как технический прогресс того времени не предоставлял возможности доказать ее экспериментально, вследствие чего о ней забыли вплоть до конца XX века.

Интерес к метаматериалам был возвращён в начале XXI века, когда в 2000 году Дэвид Смит совместно с группой ученых из Калифорнийского университета объявили, что им удалось создать композитный материал с отрицательным показателем преломления.

Классификация метаматериалов

Несмотря на относительную молодость, метаматериалы имеют весьма обширную классификацию. В данной статье будут приведены лишь два критерия, являющиеся наиболее существенными при использовании данных материалов в радиотехнических устройствах, в частности в конструкциях антенн.

По степени преломления

1. Одномерные метаматериалы состоят из слоёв элементов, которые расположены параллельно и имеют разные степени преломления. В них волна распространяется лишь в одном направлении.
2. Двумерные метаматериалы – это метаповерхности. В них распространение волны может происходить в двух направлениях.
3. Трёхмерные метаповерхности – метаструктуры – представляют из себя объёмную структуру (шар, куб и т.д.), расположенную в трёхмерном пространстве. Степень преломления в них постоянно меняется в трёх направлениях [2].

В зависимости от электродинамических свойств

1. ε-негативные (*ENG*-материалы) ($\varepsilon<0$). Как видно из названия, такие среды обладают отрицательной диэлектрической проницаемостью. Но что примечательно, одним из существенных свойств данных материалов является возможность управления их диэлектрической проницаемостью. Так, изменяя частоту возбуждения, можно сделать данную среду прозрачной или непрозрачной для электромагнитной волны. Соответственно, при $\varepsilon>0$ электромагнитная волна будет проходить через материал, при $\varepsilon<0$, наоборот, ее прохождение через материал будет существенно затруднено. Кроме того, подобные среды можно встретить и в природе – это плазма. К средам с отрицательной ε, созданным человеком, можно отнести систему из тонких металлических параллельных проводов или индуктивных петель, собранных при помощи двух разрезных рамок.
2. μ-негативные (*MNG*-материалы) ($\mu<0$). Важнейшим материалом такого типа является двойной кольцевой резонатор (*split ring resonator*, *SRR*). Ёмкость, возникающая в таком резонаторе между двумя кольцами (что на первый взгляд может показаться существенной проблемой), компенсируется их индуктивностью. Знак магнитной проницаемости таких материалов, так же как и в случае *ENG*-материала, можно изменять. В этом случае роль своеобразного «управляющего» будет выполнять направленность вторичного магнитного поля, которое создаётся изменяющимся во времени магнитным полем.
3. Бинегативные или *DNG*-материалы ($\varepsilon<0$ и $\mu<0$). Одновременная отрицательность ε и μ обеспечивает такой среде отрицательный коэффициент преломления. Это и есть те самые «левосторонние» материалы, о которых в свое время и писал В.Г.Веселаго. На сегодняшний день они представляют особенный интерес для инженеров, занимающихся разработкой и конструированием СВЧ-устройств [3].

Использование метаматериалов в радиотехнических устройствах

Развитие устройств мобильной связи, эволюция систем радиолокации, радиоастрономии, радионавигации требуют новых принципов в построении и функционировании радиотехнических устройств. И одна из важнейших задач, стоящих на сегодняшний день перед учёными и инженерами, – это уменьшение массы и габаритов радиоэлектронных компонентов при одновременном повышении их энергоэффективности, надежности и функциональности.

Революция технологий производства и проектирования в области микроэлектроники позволила добиться компактных размеров радиоэлектронных устройств. Однако на сегодняшний день технология сокращения габаритов микрополосовых антенн достигла своих пределов. Тем самым она утратила свою былую перспективность, уступив место использованию в конструкциях антенн новых материалов и сред с необычными электродинамическими свойствами. Этим объясняется все возрастающий интерес к созданию и применению в радиоэлектронике метаматериалов.

На данный момент применение метаматериалов в антенной технике позволяет:

1. В первую очередь, как было сказано выше, уменьшить размеры антенных элементов при одновременном увеличении их широкополосности;
2. Добиться компенсации паразитных ёмкостей и индуктивностей в электрически малых антеннах. В основном это достигается за счёт использования *MNG*-материалов, о которых говорилось выше;
3. Уменьшить влияние элементов антенных решеток друг на друга;
4. Улучшить способность излучателя концентрировать сигнал в определенном направлении, то есть достичь сужения его пространственной направленности;
5. Усилить свойства рупорных и других видов антенн [4].

Подложки из метаматериалов

Для начала следует дать кратное определение электрически малым антеннам (здесь и далее – ЭМА). ЭМА представляют собой особый класс антенн. По размерам ЭМА значительно меньше половины длины волны колебаний, принимаемых или излучаемых ими.

Изготовление подложек из метаматериалов и дальнейшее применение их в печатных миниатюризированных антеннах позволяет решить одну из главнейших задач современной микроэлектроники – значительно уменьшить габариты излучателей. Следует ожидать, что подобное уменьшение размеров ЭМА приведёт к снижению эффективности их излучения, однако применение метаматериалов позволяет добиться совершенно иного результата. Благодаря увеличению полосы пропускания, применение данной технологии позволяет не только миниатюризировать устройства, но и не потерять, и даже увеличить их эффективность.

При этом данная технология предоставляет достаточно широкий выбор подходящих материалов: можно выбрать как однородную, так и композитную структуру метаматериала. Рассмотрим следующую конструкцию: в качестве подложки для печатной антенны использована композитная *MNG*-структура – вертикальные квадратные рамки с разрезами, которые при желании могут быть заменены другими элементами, будь то элементы U-образной (при этом их необходимо расположить горизонтально) или спиральной формы. Элементы при этом погружают в диэлектрическую подложку. На рисунке 1 приведена иллюстрация подобной конструкции.

Рис. 1. Печатная антенна с *MNG*-подложкой

В качестве альтернативного варианта в данном случае можно создать и использовать бинегативную среду. При этом конструкция будет представлять собой совокупность ячеек, и сочетать в себе как правосторонние, так и левосторонние элементы. Общепринятое наименование таких материалов – праволевосторонние (от английского *Composite Right/Left-Handed* – здесь и далее *CRLH*) [4] – при учёте их свойств весьма очевидно. Рассмотрим пример такого «гибрида». Как было сказано выше, он представляет собой совокупность ячеек, причем ячейки из правостороннего, «обычного» материала чередуются в нём с ячейками из *DNG*-материала. Обладая отрицательным коэффициентом преломления ($n<0$) в области низких частот, этот материал при превышении значения некоторой граничной частоты становится материалом с положительным коэффициентом преломления ($n>0$). Данную частоту можно легко регулировать, лишь изменяя и подбирая оптимальные размеры сегментов. При этом можно также добиться значительной миниатюризации устройств.

Применение метаматериалов в конструкции излучателей

Американская компания *Netgear* является одной из компаний, сделавших первые шаги в использовании метаматериалов в серийном изготовлении печатных антенн. За основу были взяты антенны *MIMO* компании *Rayspan*, в конструкцию которых была внедрена композитная *CRLH*-структура [5]. Очевидным преимуществом такого решения было не только заметное уменьшение габаритов излучателей, но и снижение их влияния друг на друга. Примечательно, что расположение между двумя традиционными печатными антеннами вставки из совокупности металлических спиралей существенно повлияло на величину их полосы пропускания: компании удалось добиться её увеличения на 15% [4].

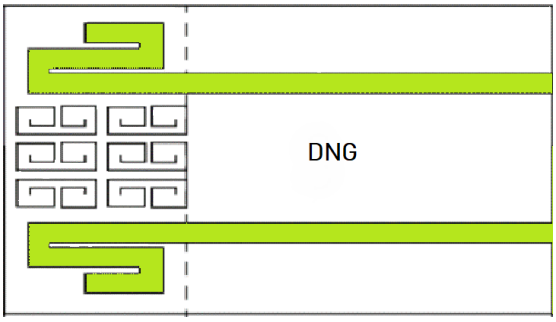


Рис. 2. Использование метаматериала в антенной системе *MIMO*

Метаоболочки, используемые в электрически малых антеннах

При конструировании электрически малых антенн можно использовать *ENG*-материалы, что довольно удобно. Если взять за основу антенны ЭМА-диполь, то придется столкнуться с проблемой его достаточно высокой реактивной ёмкости. Использование *ENG*-оболочки в данном случае будет компенсировать эту ёмкость. При этом можно избежать обычно возникающего в ходе подобной операции затухания электромагнитного поля. Толщина метаоболочки, которая при определённых условиях может составлять меньше сотых долей длины волны, не приводит к заметным ослабеваниям поля.

Теперь рассмотрим конструкцию из *ENG*-оболочки, выполняющей роль своеобразного колпака находящегося внутри него монополя, соединённого с коаксиальным фидером. Наиболее важным является то, что такая конструкция, выполненная из простых метаматериалов, обладает добротностью, большей фундаментального предела Чу. Таким образом, сделан ещё один шаг к созданию сверхминиатюрных антенн. Также стоит отметить, что на резонансной частоте для *ENG*-материала КПД составляет около 98-99% [4].

Соответствующий класс излучателей получил название метаинспирированных (от англ. «вдохновленных метаматериалами») антенн (АИМ) [4].

Рис. 3. Метаоболочки в электрически малых антеннах

Но данные конструкции, преимуществом которых является электрически малый размер, все же обладают достаточно узкой полосой пропускания и, как было рассмотрено выше, максимально эффективны при резонансной частоте. Одним из способов расширения полосы частот таких конструкций является оптимизация вспомогательного элемента, например, использование в качестве него так называемую «пиксельную» конструкцию [4].

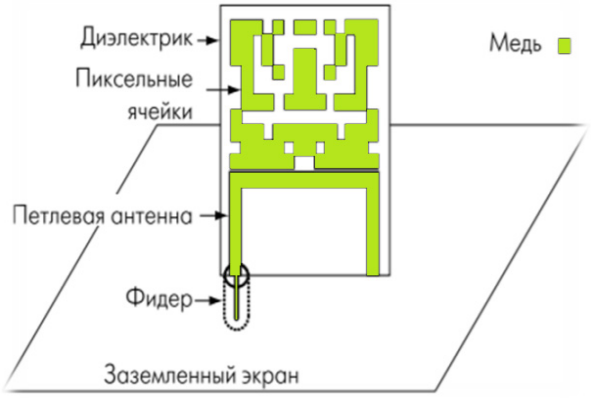


Рис. 4. "Пиксельная" конструкция АИМ

Узкая пространственная направленность

В общих словах, диаграмма направленности дает графическое представление, насколько эффективен приём или излучение электромагнитного сигнала антенной в выбранной пространственной ориентации. При улучшении способности антенны концентрировать основной сигнал в определённом направлении, ее диаграмма направленности будет сужаться. Следственно, сужение пространственной направленности излучения – это ещё одна задача современной антенной техники, решение которой также кроется в использовании метаматеалов.

Явление, при котором диаграмма направленности излучателя существенно сужается, впервые было замечено в конструкциях антенн на основе резонаторов Фабри-Перо. Технически они представляют собой достаточно простую систему, представленную в виде двух экранов. Над первым экраном, обычно представляющем собой металлическую поверхность, располагается излучатель. На расстоянии, равном целому числу полуволн, параллельно первому располагают второй экран. Обычно он полупрозрачен для электромагнитных волн. На данный момент можно добиться существенного разнообразия модельного ряда таких антенн, ведь ничто не запрещает использовать в качестве материалов для экранов не только металлы, но и различные метаматериалы. В частности, в качестве экранизирующей поверхности можно использовать решётки из диэлектрических резонаторов (ДР) [5] – у данной технологии достаточно перспективное будущее.

Использование метаэкранов позволяет также уменьшить габариты антенн (уменьшается их высота). Кроме того, это позволяет управлять их полосой пропускания и резонансной частотой.

Применение метаматериалов в конструкции рупорных антенн

Покрытие метаматериалами внутренней поверхности раструба рупора помогает повысить эффективность его работы. В качестве метаматериала в таком случае можно использовать квадратные решётки, обычно изготавливаемые из меди, вставленные в раструб рупора, как показано на рисунке 5. Кроме того, вместо трёх слоев медных решёток можно использовать многослойные сетки из других проводников. Размещение такой конструкции в качестве линзы в раскрыве рупора позволяет повысить его коэффициент усиления и при этом сократить длину раструба до 56% [4]. Однако необходимо помнить, что подобная операция может привести к сужению полосы пропускания антенны. Есть несколько решений этой проблемы, в общем случае сводящихся к поиску оптимальных для данных условий и задач параметров метавставок. Можно, к примеру, изменить интервал между слоями таких вставок или поработать с конструкцией самих решёток, изменив количество и расстояние между проводниками и т.д.

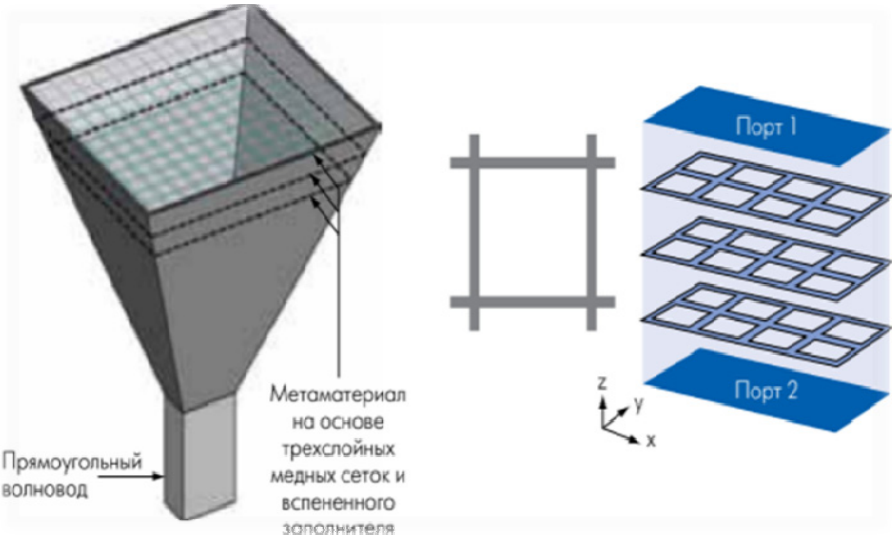


Рис.5. Конструкция рупорной антенны с вставками из метаматериалов

Использование комбинации продольных и поперечных решеток проводников позволяют еще больше сократить длину рупорного раструба.

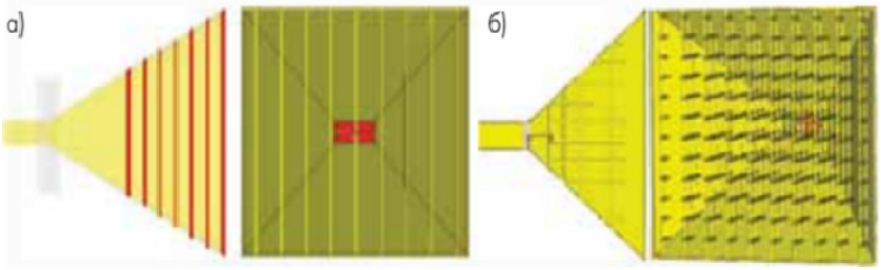


Рис.6. Конструкция рупорной антенны с вставками из метаматериалов:
а) в раструб рупора помещена конструкция из *N*-ого количества проводящих слоев, *N*=7;
б) метавставка представляет собой сетку продольных проводников, совмещённую со слоями проводников в поперечной плоскости

Заключение

Подводя итоги ко всему выше сказанному, остается лишь добавить: уверенное развитие и внедрение метаматериалов в различные отрасли делают их разработку одним из перспективных направлений прикладной физики. Удивительные, почти не встречающиеся в природе свойства метаструктур и конструкций на их основе открывают перед человечеством широкий спектр возможностей от защиты космических аппаратов от радиации и конструирования микроскопической техники до создания конструкций, невидимых при определенных частотах. В частности, появление метаматериалов и применение их в радиотехнических устройствах и по сей день сопровождается открытиями целого ряда эффектов, появлением на рынке новых серийных изделий и технологий. Хотя на данный момент широкое применение метаматериалов ограничивается их высокой себестоимостью и сложностью производства, есть все основания полагать, что это лишь начало новой грандиозной эры - эры, в которой человечество ждет немало впечатляющих открытий.

Литература

1. Новый метаматериал, необычно преломляющий свет, ускорит работу компьютеров [Электронный ресурс] // Импульс/ МФТИ. – 2015. – URL: https://mipt.ru/newsblog/lenta/pro.
2. Метаматериалы. Виды и устройство. Работа и применение [Электронный ресурс]. – URL: https://electrosam.ru/glavnaja/jelektrotehnika/metamaterialy/
3. *Бузов, А.Л, Клюев Д.С., Нещерет А.М., Неганов В.А.* Перспективы использования метаматериалов в антеннах нового поколения [Электронный ресурс] // Физика волновых процессов и радиотехнические системы – 2017. – №3. – С.15-20. – URL: file:///C:/Users/HP/Downloads/7078-16309-2-PB.pdf.
4. *Вендик, И.Б., Вендик, О.Г.* Метаматериалы и их применение в технике сверхвысоких частот: обзор // Журнал технической физики. 2013. №1. С.3.
5. *Слюсар, В.* Метаматериалы в антенной технике: основные принципы и результаты // Последняя миля – 2010. №3-4. С. 44-58.
6. *Елизаров А.А., Шаймарданов Р.В., Пчельников Ю.Н., Каравашкина В.Н.* Исследование замедляющей системы типа "ребристый стержень в азимутально-неоднородном экране" // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 3-12.
7. *Каледина А.В., Чехов А.С., Каравашкина В.Н.* Применение high-k плёнок в современной электронике // Телекоммуникации и информационные технологии. 2016. Т. 3. № 1. С. 75-77.

APPLICATION OF METAMATERIALS IN ANTENNA SYSTEM

Margarita A. Mashkova,
Student MTUCI, Moscow, Russia,
MargaritaMashckova20@yandex.ru

Aleksandra D. Sargsyan,
Student MTUCI, Moscow, Russia,
alexa.sargsyan@bk.ru

Valentina N. Karavashkina,
Associate Professor of Department of the Electronics, PhD, MTUCI, Moscow, Russia,
v.n.karavashkina@mtuci.ru

Abstract

Here is presented the brief historical background on the development of metamaterials. The classification of metamaterials according to the degree of refraction and electrodynamic properties is considered. Examples of the use of metamaterials in radio engineering devices are given. Methods of using metamaterials and metastructures in constructions of electrically small antennas, horn antennas and in emitters are described.

Keywords*: metamaterials, metastructures, dielectric constant, magnetic permeability, electrically small antennas, horn antennas, broadband, miniaturization.*

СИСТЕМЫ ПОДЗЕМНОЙ СВЯЗИ

Фильков Ярослав Дмитриевич,
магистрант МТУСИ, Москва, Россия,
jaroslav2468@mail.ru

Пронина Евгения Дмитриевна,
ассистент кафедры СиСРТ, МТУСИ, Москва, Россия,
e.d.pronina@mtuci.ru

Абстракт

Приводятся данные о системах подземной связи (underground communication systems) и актуальности их использования в настоящий период времени. Рассмотрены типичные проблемы передачи беспроводных сигналов через толщи земной породы и возможные технологические решения передачи данных под землёй. Приводится информация о предоставлении услуг связи операторами в метрополитене и специфичные аспекты применения известных технологий при передаче данных.

***Ключевые слова**: системы подземной связи, метрополитен, мобильные операторы, беспроводная связь, оборудование связи в метро.*

Подземная связь

По всему миру подземная связь требуется во множестве случаев, например, работникам шахт, спасательным службам, предприятиям, расположенным под землёй, военным.

Несколько лет назад ситуация со связью в российских шахтах стала постепенно изменяться в лучшую сторону, и всё больше предприятий добывающей промышленности стали внедрять у себя современные телекоммуникационные решения. Возможность оперативно получать информацию о выполнении работ значительно снижает вероятность возможных производственных ошибок и нарушений технологии производства, а также позволяет оптимизировать координацию спасательных операций. По некоторым оценкам, после внедрения новых систем связи затраты могут быть сокращены на 30–50%.

В большей степени подземная связь используется в метрополитенах. На ноябрь 2020 года в мире насчитывается 201 система метрополитена в 187 городах. Первым метрополитеном стал Лондонский, открытый в 1863 году и электрифицированный в 1890 году [1]. Самым длинным и загруженным является Пекинское метро, а по количеству станций лидирует Нью-Йоркский метрополитен. По примерным подсчётам протяжённость всех линий в мире составляет 17083.28 км. Более 13 тысяч станций в год обслуживают примерно 12,4 млрд пассажиров. При этом, ещё примерно 35 метрополитенов готовятся к открытию в ближайшее время, а на работающих мтрополитенах появляется всё больше новых линий и станций. Примерно 23% от всего километража метрополитенов находится на поверхности, но даже такая протяжённость пассажирской транспортной системы под землёй уже достаточно велика. Этой огромной протяжённости требуется своя система подземной связи, как для обычных пассажиров, так и для работников метрополитена [1].

Подземные системы связи — проводные и беспроводные

В прошлом почти все подземные системы связи были проводные, что накладывало серьёзные ограничения на удовлетворение основных требований надежности подземной системы связи. Сейчас почти везде используются беспроводные системы связи, однако если с ними что-то случается, всегда есть возможность воспользоваться дублирующими проводными линиями. Проводные системы сложно развернуть в труднодоступных местах, преимущественно из-за несимметричной топологии шахты или особенностей земной коры.

Беспроводные системы связи легко развёртываются даже в труднодоступных местах под землей и способны противостоять условиям стихийных бедствий. Они являются наиболее оптималь-

ными, удобными и надёжными.

Однако стандартная наземная беспроводная связь не соответствует требуемым критериям надёжной работы под землёй, так как сотовые сигналы не распространяются через земную породу. Радиоволны подвергаются рассеиванию, поглощению и затуханию из-за свойств минералов (например, угля).

Подземные системы связи отстают в развитии от наземных из-за неблагоприятной и опасной среды и отсутствия интереса к развитию связи в этой области. В настоящее время исследования по совершенствованию подземных коммуникационных технологий и преодолению ограничений проводятся достаточно активно. Требования к подземным системам связи сильно отличаются от наземных, поэтому системы беспроводной связи подземной связи адаптированы для удовлетворения специфических потребностей подземных структур, например, метрополитенов или шахт.

Связь в метрополитене в настоящее время

В наше время трудно представить отсутствие доступного *Wi-Fi* соединения в метрополитене. Сейчас уже почти в каждом метро мира есть доступ в интернет, а некоторые сотовые операторы предоставляют также мобильную связь, но в некоторых случаях, она хуже, чем на поверхности: влияние земли оказывает сильное воздействие [2].

Сложности с покрытием на станциях и в перегонах метрополитена связаны с тем, что для установки оборудования компаниям необходимо проводить согласование с руководством метро, так как это не только важный стратегический объект, но и большая часть старых станций относится к памятникам архитектуры.

При “освоении” метрополитена операторы прибегают к разным технологиям. Если на станциях и переходах просто устанавливаются антенны, обеспечивающие пассажиров доступом к мобильной связи, то с перегонами всё гораздо сложнее.

После отправления поезда от станции сигнал периодически становится слабее. Это связано с тем, что этот сигнал, получаемый от антенны на станции, постепенно затухает из-за изгибов тоннелей. Таким образом обеспечить покрытие линии метрополитена за счёт оборудования только на платформах не возможно [2].

Оборудование для мобильной связи и доступа в интернет монтируется с определёнными сложностями. Временной интервал, когда специалисты могут выполнять монтаж в перегонах, ограничен, так как требуется отключение контактного рельса и использование специального мотовоза. Кроме того, отличается и само оборудование: на станции размещается базовая станция, развёрнутая в перегон. Это позволяет обеспечить абонентам своевременное подключение к сети при подъезде к станции и отъезде от нее. В перегонах же используется фидерный кабель (рисунок 1) который излучает сигнал на всём протяжении перегона. Во многих перегонах такой кабель уже имеется - его использует метрополитен для своих нужд и предоставляет операторам для обеспечения связи [2]. Такое партнерство является взаимовыгодным: перевозчик получает арендную плату за использование своего кабеля, а операторы экономят на капитальных вложениях.

Рис. 1 – Фидерный кабель

Сеть *Wi-Fi* в метро состоит из трёх взаимосвязанных сетей: сеть в тоннелях; радиосеть поезд — тоннель, в которой данные передаются между базовыми станциями в тоннелях и в поездах; сеть внутри поезда [3].

Проектирование сети подземной связи

За пять лет инженеры московского метрополитена обследовали около 400 км тоннелей и 232 станции метро. Разнообразие материалов, геометрии тоннелей и наличие открытых участков пути делают проектирование такой сети сложной задачей. Решением стала разработка уникальной мето-

дики радиопланирования беспроводных сетей связи. Она базируется на симуляции (математическом моделировании) канального и системного уровней транспортной радиосети в тоннелях и на открытых участках [3]. Она позволила определить оптимальные места размещения базовых станций.

Базовая станция — это аппаратный комплекс, который состоит из радиомодуля, антенн, кабельных сборок, шкафов для подвода электрических и оптических кабелей. Базовые станции устанавливаются на специальные металлоконструкции — мачты. Они крепятся к путевой стене тоннеля, не нарушая разрешённые габариты приближения оборудования к пути. Также в данный момент на станциях используются точки доступа Aruba (рисунок 2). Скорость передачи данных, варьируется от 300 до 1733 Мбит/сек. Реализован входной интерфейс 10/100/1000BASE-TX [3]. Предусмотрено полное соответствие точки доступа современным стандартам безопасности. Пользователь получает надёжную беспроводную сеть без возможности несанкционированного доступа к ней.

Рис. 2 – Точка доступа HPE Aruba IAP-315 (RW) Instant 2x/4x 11ac AP [jw811a]

Антенны на базовых станциях в тоннеле через радиоканал позволяют передавать сигнал на базовые станции в поезде [3]. Базовые станции в тоннелях размещаются с интервалами 450–900 м, в зависимости от особенностей путевой инфраструктуры каждой линии метро. Это позволяет поезду двигаться в сплошном радиополе и покрытие сети обеспечивается на всей протяженности линии. В настоящее время в московском метро установлено более тысячи базовых станций. Их установка проводится ночью, когда метро закрыто для пассажиров. На оснащение оборудованием одного перегона между двумя станциями метро требуется около трёх недель [3].

После установки базовых станций в тоннеле протягивают оптический и электрический кабели. Вес одного барабана с кабелем составляет более тонны. Для их перевозки используются мотовозы. Оптический кабель обеспечивает передачу данных с базовых станций к узлам связи и далее к ядру сети [3]. Электрический кабель подводит электропитание от узлов связи к базовым станциям в тоннеле. Сигнал с базовых станций в тоннеле через антенны передаётся по радиоканалу на мобильные базовые станции в поездах. Для обеспечения непрерывной связи и резервирования такими станциями оборудованы первый и последний вагоны каждого поезда.

В зависимости от типа подвижного состава, антенны устанавливаются с внешней или внутренней стороны кабины машиниста. Разные модели подвижного состава имеют свои конструктивные особенности. Для каждой модификации поезда разрабатывалась индивидуальная проектная документация.

При оснащении поездов сетью *Wi-Fi* соблюдаются особые требования: использование комплектующих из негорючих материалов, работа оборудования от бортовой электросети и его проверка на электромагнитную совместимость с техническим оснащением поезда. Работу сети *Wi-Fi* в подвижном составе обеспечивают точки доступа, установленные в каждом вагоне. Точка доступа работает в двух частотных диапазонах – 2,4 и 5 ГГц – поддерживая все современные стандарты *Wi-Fi*. Управление сетью *Wi-Fi* в поезде обеспечивается контроллерами и маршрутизаторами, установленными в головных вагонах. Это позволяет добиться максимального качества покрытия и отказоустойчивости [3].

В каждом промежуточном вагоне поезда нового типа размещается конструктив с установленными на нём коммутатором, точкой доступа и преобразователем напряжения. Всё *Wi-Fi*-оборудование в поезде соединено витой парой. Внутри состава протянуты две независимые кабель-

ные линии пропускной способностью от 1 до 10 Гбит/с. Надёжное сетевое соединение вагонов между собой обеспечивают специальные индустриальные разъёмные перемычки. При смене составности поезда никакой дополнительной настройки оборудования не требуется: сеть перенастраивается автоматически [3].

Питание сети *Wi-Fi* подключено к бортовой электросети вагона и автоматически запускается при включении питания поезда. Таким образом, чтобы обеспечить работу *Wi-Fi* на борту, машинист при приёмке состава по регламенту должен лишь включить автомат бортовой сети. Бесплатный *Wi-Fi* на транспортной инфраструктуре это сервис, который повышает комфорт поездок. Спустя пять лет с момента развёртывания сети *Wi-Fi* в московском метро, пришло время для её модернизации. В ходе улучшения сети на каждой линии метро происходит замена базовых станций, коммутаторов и точек доступа в поездах, а также внедрение нового программного обеспечения. Из пассивного оборудования в поездах меняются кабели, источники питания, антенны [3].

Модернизация *Wi-Fi*-сети прежде всего позволит увеличить пиковые скорости передачи данных в часы наибольшей сетевой нагрузки. Также сократится время задержек при обмене данными, что повысит скорость загрузки информации. После модернизации аппаратный потенциал сети будет существенно выше, чем её фактическая пропускная способность. Внедряемое оборудование в среднем сможет обеспечить полосу около 230 Мбит/с на поезд [3].

Средняя скорость доступа в интернет на подвижном составе составляет 90 Мбит/с. Благодаря сети *MT_FREE*, пассажиры могут смотреть видео в высоком разрешении, слушать музыку, общаться в соцсетях, искать в интернете необходимую информацию. Сервис предоставляется пассажирам бесплатно и без лимита по объёму интернет-трафика, окупаясь за счёт рекламной модели. Часть прибыли компании приносит использование пользователями услуги "Как дома", которая позволяет подключаться к *Wi-Fi* в метро без рекламы и авторизации. Стоит отметить, что проект сети *Wi-Fi* в московском метро был реализован без привлечения бюджетного финансирования. Ежедневно через сеть передается свыше 150 ТБ трафика [3].

Покрытие операторов «большой четверки» обеспечивает стабильную связь в метрополитене. Так, в «МегаФоне» утверждают, что их сетями покрыты все 266 ***станций***, а более 100 перегонов оснащены связью стандарта *4G*. В «МТС» также отчитались о покрытии всех ***станций***. «Билайн» рассказал о покрытии всех ключевых ***станций*** Московского метрополитена. О покрытии всех ***станций*** и переходов метро также отчитался оператор «Tele2».

Инфокоммуникационные технологии стремительно развиваются и на данный момент в метро можно подключиться к интернету, проложить маршрут от станции до станции, посмотреть, сколько времени осталось ждать состав. Для этого создано множество приложений, работающих с инфраструктурой метрополитена, например, Яндекс Метро, МосМетро и другие. Используя подземную связь, можно создать ещё много новых приложений с различным функционалом. Например, приложение, которое будет показывать местонахождение каждого поезда в метро в режиме онлайн, всевозможные технические сбои метрополитена и приблизительное время пути до станции.

Заключение

В настоящее время и в ближайшем будущем подземная связь нуждается в активном развитии и расширении. Работу в метро сегодня трудно представить без различных систем связи, а мобильная связь - прочно вошла в метрополитен в виде мультифункциональных сетей.

Литература

1. Сайт – Википедия метрополитен URL: https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D1%80%D0%BE%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B5%D0%BD.

2. Сайт - www.banki.ru, автор - Антонина САМСОНОВА, Banki.ru- URL: https://www.banki.ru/news/daytheme/?id=10881768.

3. Сайт - nag.ru, автор Антон Рубас, Александр Попов URL:https://nag.ru/articles/article/105009/moskovskiy-podzemnyiy-internet.html.

UNDERGROUND COMMUNICATION SYSTEMS

Yaroslav Dm. Filkov,
Graduate MTUCI, Moscow, Russia,
jaroslav2468@mail.ru

Evgeniya Dm. Pronina,
Assistant of the Department of S&SRT MTUCI, Moscow, Russia,
jane19912007@yandex.ru

Abstract

It tells about underground communication systems, about it relevance in this period of technological progress. Typical problems of transmission of wireless signals through the strata of the earth's rock, possible technological solutions of the problems of data transmission in the underground are investigated. It describes the provision of communication by operators in the subway. It also being discussed of the use of underground communications in the subway, the use of well-known technologies for data transmission and the use of the transmitted data for other developments.

Keywords*: underground communication systems, underground, mobile operators, wireless communication, underground's communication equipment.*

ПЕРЕХВАТ УПРАВЛЕНИЯ МОДЕЛЬЮ КВАДРОКОПТЕРА

Рыбаков Денис Константинович,
магистрант МТУСИ, Москва, Россия,
empio@bk.ru

Суслин Максим Александрович,
магистрант МТУСИ, Москва, Россия,
suslik.ma@mail.ru

Орлов Владимир Георгиевич,
главный специалист отдела ОНИРС, к.т.н., МТУСИ, Москва, Россия
v.g.orlov@mtuci.ru

Аннотация

Рассмотрены принципы системы управления беспилотными летательными аппаратами (дронами). Приведены характеристики и обоснован выбор типа и конструкции модульного приёмопередающего устройства для перехвата управления моделью квадрокоптера. Предложен простой алгоритм реализации перехвата радиоуправления квадрокоптером на основе использования платы семейства Arduino и модифицированного программного кода. Рассмотрена процедура анализа перехваченных пакетных данных и определения протокола радиообмена информационными пакетами между пультом дистанционного управления (ПДУ) и дроном. Приведены результаты экспериментальной реализации перехвата сигналов управления моделью квадрокоптера и блокировки функционирования ПДУ путём синтеза и передачи на дрон переформатированных пакетных данных.

Ключевые слова*: атака на радиоканал,SDR, скетч для прослушивания радиоэфира, библиотека rf24 arduino, беспроводный модуль nrf24l01.*

Введение

В последнее время во всём мире наблюдается значительный рост количества используемых летательных беспилотных устройств – квадрокоптеров. Повсеместное распространение дронов обусловлено их способностью удовлетворять разного рода потребности человека. Дроны позволяют пользователям с высоты птичьего полета активировать и использовать их практически в любом месте и в любое время, при этом во всем мире постоянно растет спрос на их многоцелевые приложения [1]. Реализована возможность управления мини-дронами с помощью смартфонов вместо использования пультов дистанционного управления.

На самом деле использование дронов не ограничивается коммерческими и частными целями. Дроны широко используются правоохранительными и пограничными службами [2]. Однако в последнее время нелегальное воздействие на квадрокоптеры стали активно использовать злоумышленники. Вероятность атак на перехват дрона и его противоправное использования в целях злоумышленника возрастает, что может привести к опасным последствиям.

Уязвимость дронов от различных атак в радиоэфире обусловлена применением беспроводной радиосвязи для их управления. Атаки могут иметь серьезные последствия, включая коммерческие и материальные потери. В этом контексте важно понимание того, как злоумышленники проводят атаки и перехватывают управление дроном для использования его в своих целях. Это позволит повысить эффективность мер защиты по предотвращению перехвата управления злоумышленниками и исключит нанесение ущерба легальным владельцам квадрокоптеров [3].

Состав конструкции и программное обеспечение для устройства перехвата управления дроном

Как известно частоты 2.4 ГГц и 5ГГц используются для передачи в бинарном виде данных по протоколу IEEE 802.11. Эти частоты применяются для управления в различных радиоуправляемых моделях, в частности, существует обширный модельный ряд дронов, использующих частоту 2.4 ГГц и радиопередающую аппаратуру Управление осуществляется по радиоканалу с помощью пульта с встроенным радиопередатчиком, передающим сигналы управления на приемник, вмонтированный в конструкцию дрона. При этом передаваемые незащищенные пакетные данные управления дроном можно перехватить и использовать для нелегальных действий и криминального использования летательного аппарата.

Анализ характеристик некоторых моделей дронов, работающих в диапазоне частот 24 - 1700 МГц показывает, что для перехвата их управления можно использовать устройство RTL SDR V3, относящиеся к категории среднебюджетных устройство со стоимостью от 25 до 35 долл. (1800-2500 руб.). Оно идеально подходит для работы в качестве приёмника радиосигналов, но не имеет возможности их передачи, вследствие чего не может быть применено в радиоуправляемых устройствах различного назначения [4].

В числе устройств высокой ценовой категории, которые могут успешно использоваться для решения задач перехвата управления дронами, модели LimeSDR и LimeSDR Mini. Они способны передавать и принимать радиосигнал в диапазоне частот от 10МГц до 3,8 ГГц. Отличие между ними заключается в цене и функционале. Первое более функционально и, соответственно, более дорогостоящее. Цена этих устройств находится в диапазоне 200-400 долл. (14000-30000 руб.).

Наиболее эффективным и хорошо зарекомендовавшим себя для решения задач перехвата управления дронами является устройство высокой ценовой категории HackRF One. Оно характеризуется весьма обширным функционалом и является оптимальным для использования злоумышленниками, так как принципы его работы и схемо-технические решения находятся в открытом доступе, что даёт возможность их модификации для повышения эффективности решаемых задач. Некоторым недостатком данного устройства является использование в нём устаревших блоков ЦАП-АЦП, не обеспечивающих одновременный приём и передачу радиосигналов, что необходимо для оперативного перехвата управления дроном. Устранение этого недостатка не представляет особой сложности для злоумышленников в виду доступности принципиальных электрических схем устройства и возможности модификации соответствующего блока.

С точки зрения решения задач перехвата управления дроном при ограниченных финансовых возможностях и использования бюджетных решений, оптимальным является конструктивно-технологическое решение, основанное на сборке устройства NRF+Arduino, которое отличается от ранее представленных тем, что может быть смонтировано из отдельных доступных модулей.

Конструкция данного устройство состоит из двух частей: радиомодуля Nrf24l01 и платы Arduino.

В настоящее время доступны три вида радиомодуля:

1. Nrf24l01;
2. Nrf24l01+;
3. Nrf24l01 с усилителем и внешней антенной.

Семейство плат Arduino достаточно обширно и выбор конкретного типа платы определяется характером решаемых задач. Так, для обеспечения одновременного приема и передачи радиосигналов и требований ограничения размеров устройства выбор следует остановить на плате Arduino Nano.

В случае отсутствия существенных ограничений в масса-габаритных характеристиках устройства можно с успехом использовать плату Arduino Mega. При этом стоимость устройства составит всего около 10 долл. (700 руб.) [6].

Рассмотрим последовательность действий и алгоритмы, используемые для перехвата управления квадрокоптером с помощью предложенного для этих целей технического решения – Arduino+NRF.

Для этого необходимо в соответствие с приведённым ниже алгоритмом, последовательно обеспечить решение следующих задач:

1. Осуществить сборку устройства;

2. Написать необходимый программный код (далее скетч), с помощью которого выполняется перехват радиосигнала для модульной платы устройства;
3. Загрузить скетч в плату собранного устройства;
4. Осуществить настройку на необходимый канал радиопередачи дрона;
5. Перехватить последовательность необходимых пакетов данных с дрона;
6. Произвести анализ полученных из радиоэфира пакетов данных;
7. Написать скетч для радиоуправления дроном;
8. Загрузить скетч в плату устройства;
9. Выполнить перехват управления и осуществить блокировку действий легального пользователя дрона.

В процессе реализации алгоритма перехвата управления необходимо использовать программное обеспечение Arduino для создания программного обеспечения самой платы. Ключевой момент при реализации ПО для платы состоит в использовании одной из библиотек Arduino, а именно библиотеки RF24 [5]. Данная библиотека, в основном, используется для взаимодействия модуля платы с персональным компьютером.

Основная часть ПО содержится в файле RF24.cpp данной библиотеки. Необходимо в данном файле найти функцию setAddressWidth(uint8_t a_width) и изменить ее [6].

Рассматриваемая функция должна иметь вид:

```
{
a_width -= 2;
write_register(STEP_AW, a_width%4);
addr_width = (a_width%4) + 2;
}
```

После небольших изменений внутри библиотеки следует приступать к написанию программного обеспечения для выполнения поставленной задачи.

Программное обеспечение платы должно включать следующие функции:

1. Первичная инициализация;
2. Выполнение функции loop, с помощью которой выполняется основная часть программы.

В первичной инициализации необходимо установить:

- Идентификатор адреса в беспорядочном режиме, который будет прослушиваться

Приемником, в данном случае это «0x00AA»;

- Скорость передачи данных;
- Отключение проверки «CRC»;
- Значение длины адреса, длины пакета и прослушиваемого канала.

Также необходимо указать скорость порта, к которому подключена плата. Используемый радиомодуль Nrf24l01 обеспечивает прослушивание до 126 каналов [4].

Функция «loop» является бесконечно-повторяющейся функцией, обеспечивающей выполнение основных действий. В состав этих действия можно включить: смену канала при нажатии на кнопку, прослушивания и вывод принятых радиосигналов и др.

После успешного радиоперехвата соответствующих пакетов необходимо произвести их анализ и ручную обработка с целью определения используемых протоколов передачи данных.

По результатам выявления используемых протоколов и анализа перехваченных пакетов, необходимо написать или переформатировать программное обеспечения, которое теперь должно обеспечивать не прием - а передачу сигналов управления дроном.

Экспериментальная часть

В процессе реализации поставленных задач были использованы плата Arduino и модуль nRF24l01+. Действия выполнялись пошагово, как описано выше.

Перехват пакетов (прослушивание радиоэфира)

После сборки устройства, был написан скетч для прослушивания радиоэфира. В результате радиопрослушивания эфира был определён канал, на котором происходит радиообмен дрона с пультом дистанционного управления (далее ПДУ). В данном эксперименте это 25-й канал. Результат представлен на рисунке 3.

```
24810   ms: 3997864     Ch: 25  Get data: aa880026243c00000000100009002e703db5a6ab65aab2dd2850555a62e1954
24811   ms: 3997901     Ch: 25  Get data: 14908852000000000400009400014048000080005 20a10090422248482500 0
24812   ms: 3997984     Ch: 25  Get data: 40a048a042ae48838a88a95d1696b02a8815145541552b28a54492352a09d259
24813   ms: 3997988     Ch: 25  Get data: 04890844924911fc00101440013121e0000000000800048017381edb5daa6dda
24814   ms: 3998021     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6acfd7be99b5959936a516dd55526aa
24815   ms: 3998054     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6ea52ddcda97ab5c6ddb9b6a12ababf
24816   ms: 3998058     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6a9569b9e977db2555eb9afd57fd4b5
24817   ms: 3998070     Ch: 25  Get data: 6c42489cd078415450ed55bb21932916e95121aaaaad5a5694b4c010404a522a
24818   ms: 3998090     Ch: 25  Get data: aa880026243c00000000100009002e703daa8aeeaaaaaaf3eed7cdad55babb9
24819   ms: 3998118     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6edb6d6ab6948555525a2bff5566efd
24820   ms: 3998120     Ch: 25  Get data: 8959981091592091290 1d528ad5d7f54a5545d4adab2b5ba545d548ea9a97529
24821   ms: 3998162     Ch: 25  Get data: 2e2a5aa9a9f6a52fa95db4b3424295258d5eac5253aae330a95754a941b36ad5
24822   ms: 3998182     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6b7aef675eaa3508c4ae4d28ab5b6ad
24823   ms: 3998188     Ch: 25  Get data: 48a8a36ca6ab7cadb57438851a55630a172594da1b4b952b89a2c8640b655a49
24824   ms: 3998271     Ch: 25  Get data: 9100c0852d9ae5729fd6d5ebddeb3fb7ed6bddffb4777feddd fbebaf576d9f79
24825   ms: 3998338     Ch: 25  Get data: 0812148040414 12a882289080440a52c280022b0082246145852509 6aa4d493a
24826   ms: 3998361     Ch: 25  Get data: 48302810d4156d646abc94acadaa5c64fd5355756ee5d5553aaa6eab6733d547
24827   ms: 3998444     Ch: 25  Get data: aa880026243c00000000100009002e703dba2d6cfadb6b2d9d2adb57efb756f
24828   ms: 3998504     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6d6db692abe6b7ef635bb6ab76a6ede
24829   ms: 3998509     Ch: 25  Get data: aa880026243c00000000100009002e703db5d4a5addc8abee95755b4dbbdbcd
24830   ms: 3998569     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6d6cd73bebdaeeeaa2d574d4f5dedd9
24831   ms: 3998617     Ch: 25  Get data: 042404110204402ed5db74a627637f5eafaf8afafbd649aae5b4dffebdffbaaa
24832   ms: 3998632     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6d9db5b2d752dbb7e74a5d05ed7c975
24833   ms: 3998655     Ch: 25  Get data: aa8d34a2ac29232508a55a9285545655a954d6aa5215a112acaa8925ea92a65a
24834   ms: 3998713     Ch: 25  Get data: 94810894108a85a5a4a4a40aa8b2ad2a4a36aaa82d8aa36694542ad5bf6ed4a8
24835   ms: 3998730     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6dffb56dad77599af6b5d71cb3d796a
24836   ms: 3998766     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6eaa56ad25edf3bf3366dbd79bb6b35
24837   ms: 3998895     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6cff5dd555f5bbfb6f5fd7debed47f6
24838   ms: 3998926     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f692f58c72f4c9a567a5569490a13229
24839   ms: 3998970     Ch: 25  Get data: 951055d4b21a48888b8d62a4b16a9502e534554d2b34cec9145b57526a54a79b
24840   ms: 3999023     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6d6aadd556b74d75b5f5dbb5265d5e6
24841   ms: 3999055     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6edaaed75794b6d763a8edaaed95b54
24842   ms: 3999081     Ch: 25  Get data: aeaab54b321b4a6d555496b5ada92dab6d1bad656d5a9125ab4bc9ead5532a4f
24843   ms: 3999216     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6d7beb5eb7dbd7dfbddfbfb6b777cb5
24844   ms: 3999239     Ch: 25  Get data: 4a0108928b315090a90225134169389654c8444aa4589a2522a4db15bb52b6d4
24845   ms: 3999256     Ch: 25  Get data: a445a01464445948a5aaac4d53d39541643496 32a9887328fefeded7f55575d6
24846   ms: 3999277     Ch: 25  Get data: aa20009890f00000000004000240 0b9c0f6eabbeedd6da6b5d724956365a56ab
24847   ms: 3999304     Ch: 25  Get data: 9b66d76a246faaed57b2aa68cb8d9413b750c269dc102acc48c0da50909554d6
24848   ms: 3999406     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6bb4d45d4a9b56d6b4ad5bb596ead6c
24849   ms: 3999437     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f69b33adddffeefadb32b5adf76b4dea
24850   ms: 3999502     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6f556debaf735a4e54a8fd15e4d576c
24851   ms: 3999506     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6add4dbaf50b225acc450a45a932890
24852   ms: 3999566     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6a0a90404080800165ace93d4e99fcb
24853   ms: 3999570     Ch: 25  Get data: a20009890f00000000004000240 0b9c0f6986df5d434956255a8a8bc57b6c5e3
```

Рис 3. Полученные данные из радиоканала №25

Из полученных данных при условии, что в радиоэфире отсутствуют другие устройства, использующие данный канал, можно обнаружить пакеты, которые начинаются на a20009890f… размером 32 бита. Данные пакеты относятся к нашему перехватываемому устройству. После этого необходимо отфильтровать получаемые данные из радиоэфира. Для этого выставляется адрес передатчика ПДУ (адрес: a20009890f) и длина адреса равная 5-ти байтам в разработанный ранее скетч. Осуществляется повторяемое прослушивание радиоэфира с целью обнаружения пакетов, предназначенных для квадрокоптера. Перехваченные пакеты приведены на Рис. **4**. В процессе перехвата и анализа данных пакетов было выявлено изменение в 10-12 байтах пакета, вследствие чего в скетче было внесено изменение длины пакета с 32 до 10 байтов и включена проверка контрольной суммы (Cyclic redundancy check - CRC) для двух последних байтов. Все байты, которые идут после двенадцатого являются шумом. После внесенных изменений в скетч производится финальное прослушивание радиоэфира. На финальном прослушивании получаем пакеты, показанные на Рис. **5**.

```
Get data: 0000800000400024 00b9c0f6fffff7ffffbfffdf7ffffdfffffffeffffffffff
Get data: 0000000000400024 00b9c0f6ffb7ffefeed11dad6ab5095edaaaac9529526d57
Get data: 0000000000400024 00b9c0f6fffffffeffffffd77fdfffffffbfffffef7dff
Get data: 0000000000400024 00b9c0f6fffffdfffeffffeffff7fffe89cef5a50a2b4
Get data: 0000000000400024 00b9c0f6f57eff7fffffffffffbfdf54b55267428c29848d
Get data: 0000000000410024 00b9d0f6ffffffffffffffffffffffffffffffffffffffff
Get data: 0000000000400024 00b9c0f6fffbffff6fffdfeffffffff7ffffdfffbfdfff7f
Get data: 0000000000400024 00b9c0f6feffffffbfeffffdfffdfffefbfffbefffb7ddf
Get data: 0000000000400024 00b9c0f6bfdfffbfdfffffffffffffeb6556b5692a9aa6b45
```

Рис. 4. Повторное прослушивание радиоэфира

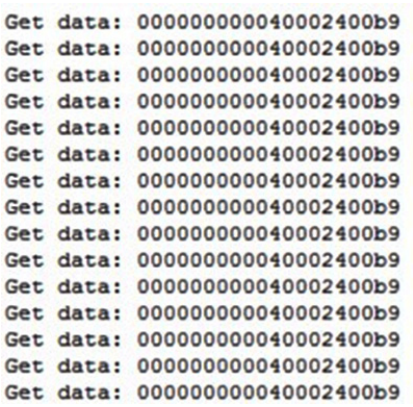


Рис. 5. Итоговые перехваченные пакеты одной повторяющейся команды

Анализ полученных пакетов

После прослушивания радиоэфира и использования различных манипуляций с ПДУ, выявлена логика в процессе отправки команд с ПДУ на квадрокоптер, а именно:

ПДУ генерирует команду согласно следующему принципу:

- Первый байт пакета – означает стик газа, то есть необходимую скорость для работы пропеллеров;
- Второй байт – означает наклон, старший бит выставляется в соответствии выбора оператором направления вперед или назад, остальные семь, значение;
- Третий байт – означает поворот вокруг оси, старший бит выставляется в соответствии выбора оператором направления влево или вправо, остальные семь, значение;
- Четвертый байт – означает наклон, старший бит выставляется в соответствии выбора оператором направления влево или вправо, остальные семь, значение;
- Десятый байт – означает CRC, то есть проверка команды, которая рассчитывается сложением по модулю первых девяти байт и прибавлением значения равного 0x55.

На основе полученных данных можно составить простой пакет для квадракоптера, который заставит крутиться его вокруг своей оси, блокируя управление им с ПДУ со стороны легального пользователя. Данный пакет выглядит следующим образом «92007f000040002400de».

Заключение

Для перехвата управления моделью квадрокоптера можно применить бюджетное устройство, легко собираемое из модулей NRF+Arduino. В процессе реализации алгоритма перехвата для платы собираемого устройства необходимо использовать ПО Arduino и библиотеку RF24 для взаимодействия модуля платы с персональным компьютером. Основная часть ПО заключается в файле RF24.cpp данной библиотеки. Для решения задачи перехвата управления квадрокоптером необходимо в данном файле выделить и изменить функцию setAddressWidth(uint8_t a_width) для обеспечения по результатам радиоперехвата анализа пакетов управления и определения протоколов передачи данных. На основе этого возможен синтез пакетов для перехвата управления и блокировки функционирования дрона.

Литература

1. *Chan K., Nirmal U., Cheaw W.* AIP Conference Proceedings. Vol. 2030. AIP Publishing; 2018. Progress on drone technology and their applications: a comprehensive review. P. 020308.
2. *Campos V.S. Ethics and Civil Drones.* Springer, Cham; 2018. European union policies and civil drones. P. 35-41.
3. *Liu Z., Li Z., Liu B., Fu X., Raptis I., Ren K.* Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing. ACM, 2015. Rise of mini-drones: applications and issues, P. 7-1
4. Security analysis of drones systems: Attacks, limitations, and recommendations. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/
5. nRF24/RF24. URL: https://github.com/nRF24/RF24
6. Optimized high speed nRF24L01+ driver class documentation. URL: https://nrf24.github.io/RF24/

INTERCEPTION OF CONTROL OF THE QUADCOPTER MODEL

Denis K. Rybakov,
Graduate MTUCI, Moscow, Russia,
empio@bk.ru

Maxim A. Suslin,
Graduate MTUCI, Moscow, Russia,
suslik.ma@mail.ru

Vladimir G. Orlov,
Chief Specialist of Department of OoRWoS, PhD., MTUCI, Moscow, Russia,
v.g.orlov@mtuci.ru

Abstract

The principles of the control system for unmanned aerial vehicles (drones) are considered. The characteristics are given and the choice of the type and design of a modular receiving-transmitting device for intercepting control of a quadrocopter model is substantiated. A simple algorithm for the implementation of interception of radio control of a quadcopter based on the use of a board of the Arduino family and modified program code is proposed. The procedure for analyzing intercepted packet data and determining the protocol of radio exchange of information packets between the remote control (RC) and the drone is considered. The results of the experimental implementation of intercepting control signals for a quadcopter model and blocking the operation of the remote control by synthesizing and transmitting reformatted packet data to the drone are presented.

Keywords: *attack on a radio channel, SDR, a sketch for listening to the radio, rf24 arduino library, nrf24l01 wireless module.*

АНАЛИЗ ПРОЦЕДУР ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ ОКС7 И КОРРЕКЦИИ МАРШРУТИЗАЦИИ В ИМИТАТОРЕ СЕТИ ПД СПЕЦНАЗНАЧЕНИЯ

Басараб Михаил Алексеевич,
заведующий кафедрой ИБ МГТУ им. Н.Э.Баумана,
д.ф.-м.н., Москва, Россия,
bmic@mail.ru

Бельфер Рувим Абрамович,
доцент кафедры ИБ МГТУ им. Н.Э.Баумана, к.т.н.,
Москва, Россия,
a.belfer @ yandex.ru

Глинская Елена Васильевна,
ст. преподаватель кафедры ИБ МГТУ им. Н.Э.Баумана,
glinskaya-iu8@rambler.ru

Кравцов Андрей Владимирович
начальник отдела НИИЦ ЦНИИ ВВКО, Москва, Россия
skyak78@gmail.com

Орлов Владимир Георгиевич
главный специалист отдела ОНИРС, к.т.н., МТУСИ, Москва, Россия,
v.g.orlov@mtuci.ru

Абстракт

Исследования зарубежных и отечественных специалистов выявили причину низкой надежности системы общеканальной сигнализации ОКС№7 сети ISDN по результатам более чем двадцатилетнего периода ее эксплуатации. Этот недостаток не удалось устранить, несмотря на проведенные работы в рамках международной организации по стандартизации ITU-T. Показано, что одним из влияющих факторов на этот недостаток в системе общеканальной сигнализации ОКС№7 сети ISDN является сложность алгоритмов резервирования и маршрутизации. В статье рассматриваются и предлагаются менее сложные процедуры для реализации этих алгоритмов на примере их использования в имитаторе сети передачи данных специального назначения.

Ключевые слова*: имитатор сети (network simulator), сеть передачи данных (data transmission network), резервирование (redundancy), надежность (reliability), маршрутизация (routing), коррекция маршрутизации (routing correction), принудительная маршрутизации (forced routing).*

Введение

В резолюции по итогам работы состоявшейся в 2015 г. 4-ой научно-практической конференции «Информационные технологии на службе ОПК России» была особо подчёркнута актуальность задачи создания современной единой системы объединенных коммуникаций в сфере ОПК [1].

Решить эту задачу возможно путём создания сети, включающей для каждого рода войск одну или группу независимых (изолированных) сетей передачи данных (ПД). В отличие от виртуальных частных сетей, ориентированных на предоставление одной из услуг сетей связи общего пользования (ССОП), присвоим этим изолированным сетям наименование частные сети (ЧС). Одной из основных особенностей этих сетей в сравнении с виртуальными частными сетями ССОП является

широкий перечень и конкретный состав характеристик качества обслуживания, а также высокие требования к их нормативным количественным значениям. В частности, в перечень показателей качества обслуживания ЧС данного назначения включены: информационная безопасность, надежность, вероятность доставки сообщения, задержка и др. [1-3].

Из числа типовых ССОП наибольшее внимание отдельным из этих характеристик уделялось немецкой фирмой Дойчен Телеком при разработке и эксплуатации ССОП, используемой в сети ISDN технологии общеканальной сигнализации ОКС7 [2].

В научно-практической зарубежной работе [3] на основании более чем 20-ти летнего опыта создания и запуска в эксплуатацию системы общеканальной сигнализации ОКС№7 сети ISDN отмечается, что для неё характерны низкая надежность и недостаточная информационная безопасность (ИБ). Автор данной работы приходит к заключению, что это обусловлено сложностью большинства используемых алгоритмов, используемых после пуска сети в эксплуатацию.

Разработка и проектирование отечественной объединенной сети ПД частных сетей требует решения задач создания алгоритмически сложного аппаратно-программного комплекса, для реализации которого необходимы высококвалифицированные научно-производственные коллективы и немалые сроки выполнения работы.

Специалисты кафедры «Информационная безопасность» в рамках выполнения совместных исследований с Научно-исследовательским испытательным центром (НИИЦ) ЦНИИ ВКС МО РФ проводят комплексные работы по созданию имитатора объединенной (единой) сети ПД категории специального назначения. В соответствие с классификацией сетей связи, приведённой в ФЗ «О связи», объединённая сеть ПД, кроме сетей ОПК, также включает сети ПД других государственных органов и ведомств. Для подготовки специалистов в области проектирования и эксплуатации национальных сетей ПД данной категории в учебном процессе в МГТУ им. Н.Э. Баумана используется учебный лабораторный стенда (УЛС), служащий в качестве имитатора отечественной действующей сети ПД специального назначения. Первостепенной задачей выполняемых с помощью имитатора сети ПД исследований является поиск и разработка оптимальных алгоритмических и программных решений по реализации функциональных требований и характеристик надёжности объединённой сети ПД.

В представленной работе производится анализ сложности алгоритмов, обеспечивающих показатели надежности и маршрутизации в системе ОКС7 сети связи общего пользования ISDN. Для достижения соответствующих показателей надёжности и реализации требуемых функциональных возможностей единой сети ПД специального назначения в имитаторе были предложены и опробованы менее сложные процедуры и более эффективные алгоритмы.

Процедуры обеспечения надежности в системе ОКС7 и в имитаторе сети ПД

Следует отметить, что ISDN является единственной из числа ССОП, для которой Международный Союз Электросвязи разработал стандарты обеспечения надежности.

Приведем некоторые из числа процедур по обеспечению надежности в системе ОКС7, стандартизированные международной организацией ITU-T.

Как следует из рисунка 1, между пунктами сигнализации операторов разных стран на международном участке сети ПД создается пучок маршрутов, обеспечивающий четыре пути маршрутизации.

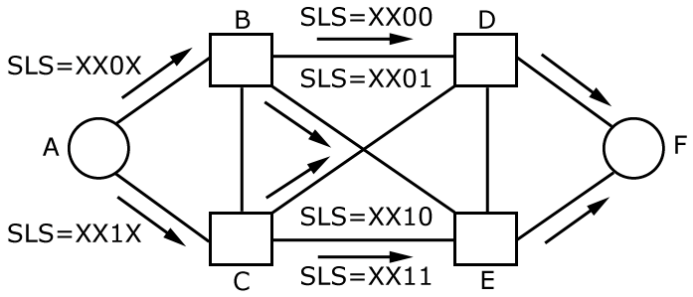


Рис. 1. Пример маршрутизации в пучке из четырех путей маршрутизации

Покажем все четыре направления маршрутизации от узла A к узлу F в условиях отсутствии отказов звеньев сигнализации (ЗС) или пунктов сигнализации, то есть в режиме штатной маршрутизации (рисунок 1). Состояния поля SLS транзитных пунктов сигнализации (B или C) отмечены в скобках по каждому маршруту в сообщениях поступающих в пункт назначения от A в F.

A-B-D-F (SLS=xx00)
A-C-D-F (SLS=xx10)
A-B-E-F (SLS=xx01)
A-C-E-F (SLS=xx11)

По каждому из путей маршрутизации передается разный трафик, т.е. используется резервирование с расщеплением нагрузки. При исправном состоянии всех каналов связи и ЗС, на этом международном участке сети по каналам связи передается трафик только по определенным направлениям маршрутизации в пучке маршрутов. С целью исключения потенциально возможных аварийных ситуаций, обусловленных недоступностью ЗС, в каждом из пунктов сигнализации имеется информация о резервных путях маршрутизации, определяющая для каждого из штатно функционирующих ЗС один или более резервных пучков ЗС.

Для схемы маршрутизации в условиях отказов в таблице 1, составленной для одного из пунктов сигнализации STP B, приведен перечень резервных пучков ЗС. Если отказы отсутствуют, используется разделение нагрузки между основным и резервным (альтернативным) пучками ЗС. Использование резервных пучков приоритета 2 производится только в случае недоступности всех основных и резервных пучков ЗС первого приоритета. При этом:

Приоритет 1 используется, при условии отсутствия неисправностей и нормальной работы основного набора звеньев РС в режиме с разделённой нагрузкой;

Приоритет 2 используется, в условиях недоступности наборов всех звеньев ЗС с приоритетом 1.

В случае отказа основного канала предусмотрено резервирование каналов первого и второго приоритета. При этом резервные каналы (ЗС) приоритета 1 используются только в случае недоступности всех основных каналов первого приоритета, а резервные каналы (ЗС) приоритета 2 - только в случае, когда все основные и резервные каналы первого приоритета становятся недоступными.

Резервные пучки сигнальных звеньев с учетом приоритета в пункте сигнализации STP B.

Таблица 1

Пункт сигнализации	Основной набор звеньев	Альтернативный набор звеньев	Приоритет
STP B	BE	BD	1
STP B		BC	2
STP B	BD	BE	1
STP B		BC	2

Сеть сигнализации системы ОКС7 включает в себя транзитные пункты сигнализации STP (Signaling Transfer Point) и выполняет лишь транспортные функции, то есть не обеспечивает выбор информационного канала, функция которого заключается в изменении пути маршрута при недоступности основного пути маршрутизации.

Процедуры резервирования на немеждународном участке сети B определены в стандарте ITU-T Q.705. При этом используется пучок маршрутов из двух путей с расщеплением нагрузки. В качестве иллюстрации приводится перевод трафика при неисправности между двумя смежными узлами коммутации (пунктами сигнализации SP) на резервный путь маршрутизации через транзитный пункт сигнализации STP.

Для возвращения трафика с резервного ЗС на ставшее вновь доступным исходное ЗС предусмотрена процедура перенаправления трафика на исходный канал (РС) [4]. Другим примером резервирования является перевод трафика между двумя не смежными узлами коммутации (пунктами сигнализации SP) на резервный путь маршрутизации через транзитный пункт сигнализации STP.

Практика эксплуатации системы ОКС7 в сети ISDN, показала, что использование данного алгоритма для выбора путей маршрутизации в условиях отказов является одним из факторов, определяющих низкую надёжность системы вследствие использования сложного алгоритма резервирования [3]. С учётом этого можно сделать вывод, что достижение более высоких требований по харак-

теристикам надежности в сетях связи специального назначения при использовании технологии ОКС7 не представляется возможным.

Существенное повышение показателей надёжности функционирования сети ПД специального назначения можно достигнуть за счёт повышения эффективности процедур резервирования и изменения регламента передачи трафика. Для этого необходимо:

1. Исключить расщепление нагрузки и обеспечить режим одновременной параллельной передачи одного и того же сообщения по всем имеющимся маршрутным путям;

2. Разработать алгоритм резервирования передачи сообщений пучком путей из четырех маршрутов (для волоконно-оптических систем DWDM пучком из трех).

При этом использование параллельной передачи пакетов данных по нескольким каналам связи позволит не только повысить надёжность сетевого обслуживания потребителей, но также обеспечит достижение требуемых в частных сетях объединенной сети ПД специального назначения показателей качества, таких как задержка доставки данных, вероятность потерь пакетов и др.

Коррекция таблиц маршрутизации в ОКС7 и в имитаторе сети ПД

Анализ коррекции таблиц маршрутизации в ОКС7 рассмотрим на примере структуры сегмента международной сети ОКС7, обеспечивающего взаимодействие двух соседних международных сетей связи общего пользования ISDN (рис. 2). На указанном рисунке с изображёнными на нём шестью узлами коммутации A, B, C, D, E, F приведен неисправный один из узлов коммутации (D) при исправном состоянии всех каналов. При исправном состоянии всех узлов коммутации и каналов пучок маршрутов от A к F состоит из четырех путей маршрутизации также как и в имитаторе сети ПД специального назначения, что принципиально важно для корректного анализа процедур маршрутизации рассматриваемых сетей. Пути маршрутизации при исправных каналах в базовой структуре международных сетей имеют следующий вид: A-B-D-F, A-C-D-F, A-B-E-F, A-C-E-F. Пучок маршрутов от F к A включает четыре обратных пути маршрутизации: F-D-B-A, F-D-C-A, F-E-B-A, F-E-C-A, (рис. 2).

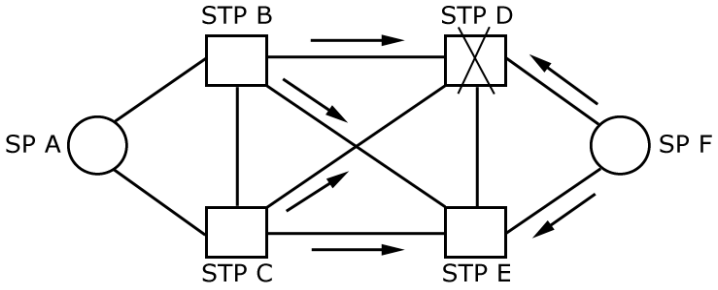


Рис. 2. Упрощённая структура международной сети ПД с ОКС7 и неисправным узлом коммутации D

Приведем последовательность процедур при отказе транзитного узла коммутации D [4]:

- *в штатно функционирующих узлах B, C и F запускается процедура инициализации перехода с блокированных из за отказа каналов BD, CD и FD на соответствующие резервные каналы BE, CE и FE. Одновременно узлы B,C и F осуществляют отправку через пункт E в пункт D сообщения (COO) о переключении соответствующих каналов. Вследствие отказа узла D пункты B,C и F, не получив ответных сообщений COA, по истечении выдержки времени T2=0,2-2 сек. выполняют перезапуск трафика. Одновременно пункт E выполняет передачу сообщения (относительно пункта D) о запрете переноса (TFP) в пункты B, C и F.*

- *после приема сообщения TFP от пункта E относительно недоступности пункта D, в пункте B осуществляется обновление маршрутных таблиц с целью переключения первоначально направляемого к пункту D трафика. Вследствие этого сообщение TFP о недоступности пункта D передается в пункт C, в котором производятся аналогичная процедура по передаче сообщения TFP в пункт B;*

- *после принятия от узла C сообщения TFP, пункт назначения D маркируется узлом B как недоступный, а на узел A отправляется сообщение TFP. Аналогичным образом из пункта C передаёт-*

ся сообщение TFP в пункт A. По результатам приёма из пунктов B и C сообщений TFP узел A фиксирует недосягаемость доставки пакетов данных в узел назначения D. При этом приостанавливается передача трафика в пункт D и, вследствие приема сообщений TFP, производится обновление таблиц маршрутизации в пунктах A,B, и C

➢ *аналогично приведённой выше процедуре производится оповещение узлов A и E об отказе узла D путём последовательной передачи сообщений TFP от канала к каналу. В результате приема в пункте E сообщения TFP производится запуск процедуры обновления таблиц маршрутизации.*

Последовательность процедур восстановления функционирования транзитного пункта D:

✓ *после фиксации восстановления досягаемости узла D узлы B, C и F передают к нему сообщения TRA, инициализирующие перезапуск трафика пакетов данных;*

✓ *сообщения TRA рассылаются всем смежным узлам с помощью транзитного узла D;*

✓ *соответственно в пунктах B, C и F выполняются процедуры переключения с резервных каналов на основные.*

✓ *сообщения разрешения переключения трафика TFA относительно узла назначения D передаются из пункта E в узлы B, C и F, которые после приема сообщений TFA транслируют их в смежные с ними узлам. Таким образом, передача от канала к каналу сообщений TFA обеспечивает оповещение всех узлов о восстановлении доступности узла D;*

✓ *в пунктах B, C и F производится перезапуск трафика, передача которого в штатном режиме производится через транзитный узел D.*

При использовании принятой в ОКС7 маршрутизации неисправность одного канала связи или узла коммутации в пучке маршрутов базовой архитектуры международной сети ПД вызывает необходимость автоматического выполнения процедуры управления сетью и корректировки всех таблицы маршрутизации с передачей специальных сообщений. Восстановление после вывода из эксплуатации этих устройств так же требует автоматического выполнения с использованием специальных сообщений нескольких специальных процедур управления сетью и корректировки таблиц маршрутизации в узлах сети [10,11]. Такой алгоритм выполнения вышеприведённых процедур управления сетью отличается сложностью и не обеспечивает требуемые показатели надёжности.

В созданном имитаторе сети ПД специального назначения предложен алгоритм централизованной принудительной маршрутизации («от источника») в отличие от децентрализованной маршрутизации в ОКС7 сети ISDN. Из числа сетей ССОП такой вид маршрутизации использовался в сети АТМ [5].

Представленный в статье материал направлен на обоснование эффективности использования централизованной принудительной маршрутизации в имитаторе сети ПД специального назначения. В качестве примера приведены процедуры коррекции маршрутизации передачи данных в сети ПД из-за вывода неисправных устройств сети из эксплуатации, и последующего ввода их в штатный режим эксплуатации после восстановительного ремонта.

Для реализации принудительной маршрутизации используется центр эксплуатации сети (ЦЭС), подключенный к узлу коммутации ЦКП 2.1(21) имитатора сети ПД специального назначения, конфигурация которого приведена на рисунке 3. Так же, как и в приведенной выше структуре сегмента ОКС7 международной сети ISDN (рис. 1) устанавливается пучок маршрутов из четырех путей маршрутизации с целью обеспечения надежности соединения между оконечными пунктами сети ПД.

Для примера примем в качестве неисправного узел коммутации ЦКП 2.2 (рис. 3). Тогда при установлении КВК второй путь маршрутизации вместо ЦКП 1.2(12) – ЦКП 2.2 (22) –ЦКП 3.2 (32) будет заменен на ЦКП 1.2 (12) – ЦКП 2.1(21) – ЦКП 3.2 (32), путь 3 вместо 1.1 –2.2 – 3.1 будет заменен на 1.1 – 2.1 3.2. Второй и четвертый путь пучка маршрутов остаются без изменения (соответственно
12-22-32 и 12-21-32).

Приведем краткое описание алгоритмов выполнения функций принудительной маршрутизации в имитатора сети ПД на примере установления соединения коммутируемого виртуального канала (КВК), между оконечными пунктами ОПа – ОПf. В качестве источника установления соединения примем ОПа.

Прежде чем приступить к формированию принудительной маршрутизации следует произвести реализацию выполнения функций имитатора сети ПД (детально описано в [6,7]), а именно на абонентских доступах ОПа – ЦКП 1.1 и ОПа – ЦКП 1.2 произвести установление КВК, включая:

ассоциацию безопасности, взаимную аутентификацию и создание головного ключа, формирование канальных и сквозных ключей, создание логического адреса оконечного пункта источника установления КВК [9-11].

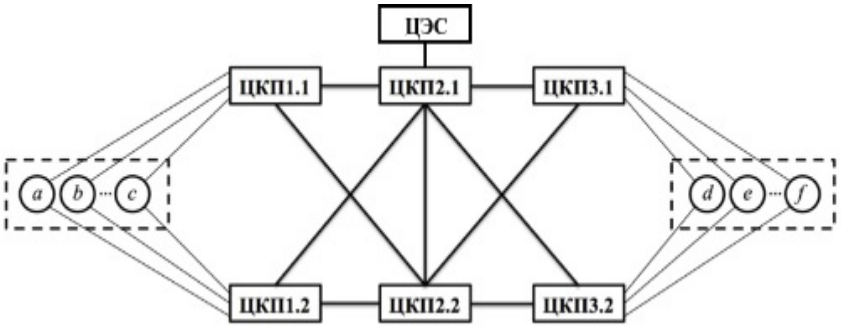


Рис. 3. Обобщённая конфигурация имитатора сети ПД специального назначения

Предложенная в имитаторе сети ПД принудительная маршрутизация не использует таблицы маршрутизации и их автоматическую коррекцию при возникновении неисправностей, выходе из строя отдельных устройств сети с последующим выводом их из эксплуатации. При этом также исключается повторная автоматическая коррекцию маршрутизации после восстановления и ввода в эксплуатацию отремонтированных сетевых устройств. Информация о текущем состоянии устройств сети содержится в центре эксплуатации имитатора сети ПД, что позволяет, централизовано формировать цепочку маршрутов при установлении соединения КВК.

Как показано в работе [8], полностью автоматический обмен сообщениями не позволяет эффективно реализовать алгоритмически сложные процедурные функции необходимые для работы телекоммуникационных сетей. С учётом этого в алгоритме формирования цепочки принудительной маршрутизации некоторые функции ЦЭС по формированию цепочки маршрутизации в сложной архитектуре имитатора бъединенной сети ПД специального назначения целесообразно выполнять в полуавтоматическом режиме. Это позволит создать менее сложные и более надежные алгоритмы маршрутизации и соответствующее программное обеспечение для использования в имитаторе объединенной сети ПД специального назначения с расширяемой иерархической структурой [9].

Выводы

Опыт разработки и последующей эксплуатации на протяжении десятилетий системы общеканальной сигнализации ОКС№7 сети ISDN убедительно показал причины её низкой надежности. Несмотря на проведенные организационно-технические работы в рамках международной организации по стандартизации ITU-T данный недостаток не удалось устранить. Как показано в представленном статье материале ключевым фактором, определяющим данный недостаток, является сложность алгоритмов резервирования и маршрутизации в системе общеканальной сигнализации ОКС№7 сети ISDN. На основе выполнения экспериментальной проверки применения с использованием имитатора сети ПД специального назначения предложены менее сложные процедуры для реализации этих алгоритмов, что позволяет повысить надёжности и улучшить эксплуатационные характеристик сети ПД.

Литература

1. Резолюция конференции «Информационные технологии на службе оборонно-промышленного комплекса России 2015» // Connect. 2015. № 9. С. 78-88.

2. *Росляков А.В.* ОКС№7.: архитектура, протоколы, применение. М.: Эхо-Трендз, 2008. 320 с.

3. *Rufa G.* Developments in Telecommunications. With a Focus on SS7 Network Reliability // Springer, 2009. 277 p.

4. *Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д.* ОКС7: Стек протоколов ОКС7. Подсистема МТР: Справочник. Москва «Радио и связь». 2003. 221 с.

5. *Дикер Палтуш Г.* Сети АТМ корпорации Cisco. М.: Вильямс, 2004. 880 с.

6. *М.А. Басараб, Р.А. Бельфер, Е.В. Глинская, А.В. Кравцов.* Алгоритм ПО установления коммутируемо-

го виртуального канала на абонентском доступе имитатора сети ПД с учетом обеспечения информационной безопасности // Первая миля. 2017. №8. С. 64-69.

7. *Басараб М.А., Бельфер Р.А., Глинская Е.В., Кравцов А.В.* Алгоритм установления защищенного соединения на абонентском доступе имитатора объединенной сети ПД специального назначения // Первая миля. 2019. № 8. С. 46-51.

8. *J. Keeney, Sven van der Meer, Gabriel Hogan A*. Recommender-System for Telecommunications Network Management Actions. IFIP/IEEE International Symposium on Integrated Network Management, 2013. P. 760-763.

9. *Басараб М.А., Бельфер Р.А., Кравцов А.В*. Учебные имитаторы объединенной сети ПД спецназначения и задачи имитатора иерархической структуры // Электросвязь. 2020. №3. С. 62-68.

10. *Басараб М.А., Бельфер Р.А., Кравцов А.В., Е.В. Глинская, В.Г.Орлов*. Сравнение процедур коррекции маршрутизации в имитаторе сети ПД специального назначения и в ОКС7 // REDS: Телекоммуникационные устройства и системы, №4-2020. С. 3-9.

11. *Бельфер Р.А., Глинская Е.В., Кравцов А.В., Орлов В.Г*. Состояние разработки имитатора объединенной сети ПД специального назначения в качестве учебного лабораторного стенда // Телекоммуникации и информационные технологии. 2019. Т. 6. № 1. С. 61-65.

ANALYSIS OF PROCEDURES FOR ENSURING THE RELIABILITY OF ACS 7 AND CORRECTION ROUTING IN THE SIMULATOR OF THE SPECIAL PURPOSE PD NETWORK

Michael A. Basarab,
Head of the Department of IS, Doctor of P&M Sciences,
*MSTU named after N.E. Bauman, Moscow, Russi*a,
bmic@mail.ru

Ruvim A. Belfer,
Associate Professor of the Departmen of IS, PhD,
*MSTU named after N.E. Bauman, Moscow, Russi*a,
a.belfer @ yandex.ru

Elena V. Glinskaya
Senior Lecturer of the Department of IS,
*MSTU named after N.E. Bauman, Moscow, Russi*a

Andrey V. Kravtsov,
Head of the Department of the R&TC of the CRI of ADF,
*Moscow, Russi*a,
skyak78@gmail.com

Vladimir G.Orlov,
Chief specialist of the Department of OoRWoS, PhD.,
MTUCI, Moscow, Russia,
v.g.orlov@mtuci

Abstract

The analysis of foreign experts showed the reason for the low reliability of the general channel signaling system OKS # 7 of the ISDN network during the entire twenty-year period of its operation. This shortcoming could not be eliminated, despite the work carried out within the framework of the international organization for standardization ITU-T. It is shown that one of the influencing factors on this drawback in the system of common channel signaling SS7 of the ISDN network is the complexity of the redundancy and routing algorithms. Less complex procedures for the implementation of these algorithms are proposed in the special purpose data network simulator.

Keywords: *network simulator, data transmission network, peredundancy, reliability, routing, routing correction, forced routing.*

АНАЛИЗ МЕТОДОВ РЕЗРВИРОВАНИЯ В ОПТИЧЕСКИХ СЕТЯХ ДАЛЬНЕГО РАДИУСА ДЕЙСТВИЯ

Кудрявцева Александра Владимировна,
магистрант МТУСИ, Москва, Россия,
motoko@bk.ru

Нетес Виктор Александрович,
профессор кафедры ССиСК, д. т. н., с.н.с, МТУСИ, Москва, Россия,
v.a.netest@mtuci.ru

Аннотация

Представлен обзор типов и методов резервирования каналов LR-PON. Произведен анализ рентабельности и актуальности резервирования, как метода обеспечения надежности сетей в текущих рыночных условиях. Приведены алгоритмы оценки резервирования сетей на основе параметров надежности, учтены издержки в ходе эксплуатации при проведении аварийно-восстановительных работ.

Ключевые слова: *Сети LR-PON, надежность, резервирование, AWG, WDM-PON, MASH, коэффициент готовности, Failure Impact, цена восстановления.*

Пассивные оптические сети дальнего радиуса действия (long-reach PON, LR-PON) – перспективное технологическое решение для предоставления каналов связи. Благодаря своим техническим характеристикам, такие сети позволяют обеспечить доступ для удаленных пользователей с минимальным числом активных компонентов сети. Важную роль в достижении отказоустойчивости и повышении надежности таких сетей играет пассивное и активное резервирование каналов [17-20].

Топология многоступенчатого дерева наиболее характерна для сетей на базе технологии LR-PON, при этом пропускная способность каналов составляет 10 Гбит/с вниз (к абоненту) и 2,5 Гбит/с вверх (от абонента). Протяженность таких сетей составляет до 100 км, при этом на канале может быть задействовано до 17 делителей мощности с разными парами потоков трафика вниз и вверх, разнесенных по длинам волн и обслуживающих до 256 абонентских устройств ONU. В результате на OLT (оптический линейный терминал для доступа по технологии PON) может быть включено до 4352 ONU.

В связи с большим удалением обслуживаемых объектов связи и стремительно возрастающим объемом трафика ужесточаются и требования к отказоустойчивости сети. Для ответственных приложений время общего простоя сервиса в среднем не должно превышать 5,3 минуты в год, что соответствует коэффициенту готовности 0,99999 [1].

В целом задача выбора показателей надежности для сетей доступа была рассмотрена в [2] и [3]. Оценка надежности может быть произведена с точки зрения оператора связи и с точки зрения конечного пользователя. Обосновывается применение коэффициента сохранения эффективности в первом случае и коэффициента готовности во втором.

Причинами деградации сервиса могут служить разнообразные факторы антропогенного и природного происхождения, как следствие, возникает необходимость в прогнозировании возможных негативных воздействий и разработке методов повышения отказоустойчивости и экстренной локализации последствий отказов в сетях и системах связи.

Направления исследований LR-PON с позиций надёжности

Безотказность, ремонтопригодность, долговечность и сохраняемость являются основными свойствами, составляющими надежность. Широко используемыми показателями надежности служат коэффициент готовности, интенсивность отказов, средняя наработка на отказ (Mean operating Time To Failure, MTTF) и др. [4].

Отказоустойчивость компонентов LR-PON обеспечивается за счет разработки и внедрения новых технологических решений на сети передачи трафика, совершенствования технологий производства компонентов, проектирования и внедрения методов резервирования элементов с автоматическим переключением, а также динамического изменения пропускной способности сети. При проектировании отказоустойчивых систем LR-PON используются точные, приближенные и эвристические методы.

Имитационные модели сети наиболее востребованы ввиду наглядности, простоты использования и высокой точности полученных результатов. Программное обеспечение, предназначенное для имитационного моделирования, например AnyLogic [5] и Cisco Packet Tracer [6], позволяет при помощи разработанной имитационной модели изучить и оценить влияние различных методов резервирования на надежность функционирования сетей и систем связи, получить проектную оценку таких параметров, как коэффициенты готовности Кг и неготовности .

С помощью целочисленного программирования (например, MILP – Mixed Integer Linear Programming в [7] и [8]) можно построить модель, учитывающую баланс между издержками и соответствием требованиям к надежности (коэффициенту готовности), направленную на увеличение зоны покрытия, что наиболее полно отвечает задачам проектирования LR-PON.

Приближенные методы используются для построения моделей сети с максимизированными показателями надежности, тем не менее, низкая точность данных методов приводит к необходимости верификации полученных результатов путём их оценки с помощью других методов.

Имеются также эвристические методы (например, LOWLARF [9,10]), систематизирующие и совместно использующие известные решения для достижения желаемых результатов.

Резервирование каналов на основе рекомендации G.983.1

Для обеспечения должного уровня надежности архитектурных решений каналов связи в Рекомендации МСЭ-Т G.983.1 в 1998 году были представлены схемы защиты типа A, B, C, D [9], где частичное или полное дублирование компонентов является основным принципом обеспечения отказоустойчивости на сети [10].

Тип A: Резервирование кабельной линии от CO (здесь и далее Central Office, центральная точка) до клиента: при повреждении кабельной линии происходит переключение на резерв при помощи оптического переключателя (рис. 1).

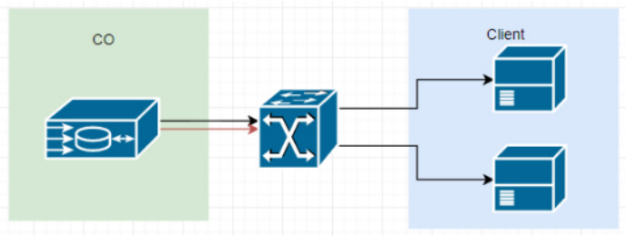


Рис. 1. Тип A

Тип B: Резервируется магистральный кабель и OLT в CO: при данной схеме основной канал активно нагружен, а резерв находится в режиме пассивного ожидания (рис. 2).

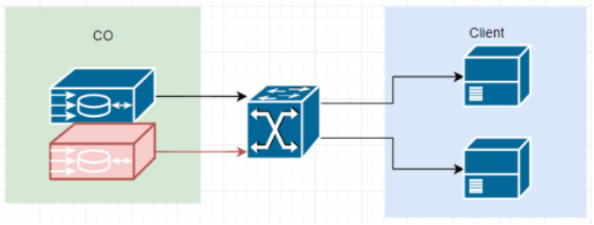


Рис. 2. Тип B

Тип C: Защита с полным дублированием сети, при этом обе OLT активно передают трафик (рис. 3).

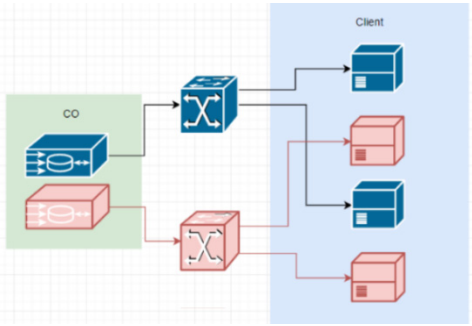


Рис. 3. Тип C

Тип D: Резервирование магистрального и распределительного кабелей с целью минимизации простоя сети в результате повреждения канала на физическом уровне.

Однако резервировать стоит сеть не только на физическом уровне, но и на сетевом, не отдавая предпочтение одному CO, что позволяет избежать (либо минимизировать) проблем с выходом в сеть и получить возможность географического разноса трассы до объекта (рис. 4).

При реализации такого типа проекта резервирования канала требуется опираться на оценку издержек для организации двух параллельных каналов (которые в свою очередь могут быть так же резервированы по вышеописанным схемам A, B, C, D) и соотношения между показателем стоимости эксплуатации канала и потерями, понесенными при деградации сервиса (данное решение широко используется для крупного бизнеса, где простой сервиса не приемлем).

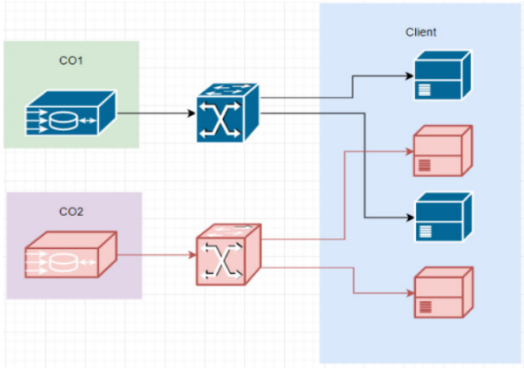


Рис. 4

Также возможно резервирование каналов с использованием оборудования беспроводного широкополосного доступа (БШПД). Такая схема резервирования предусмотрена при высокой стоимости организации двух каналов LR-PON, либо низкой эффективности такого способа резервирования. При таком архитектурном решении возможны централизованная и децентрализованная схемы передачи трафика. В случае централизованной семы передачи трафика мы получаем трафик из одного источника (в случае отказа на CO возникает деградация сервиса), при децентрализованной схеме передачи трафика мы резервируем сам CO, и в случае отказа (полного или частичного) на CO1 сервис продолжает работать без перебоев с минимальным интервалом сходимости через CO2, (рис. 5).

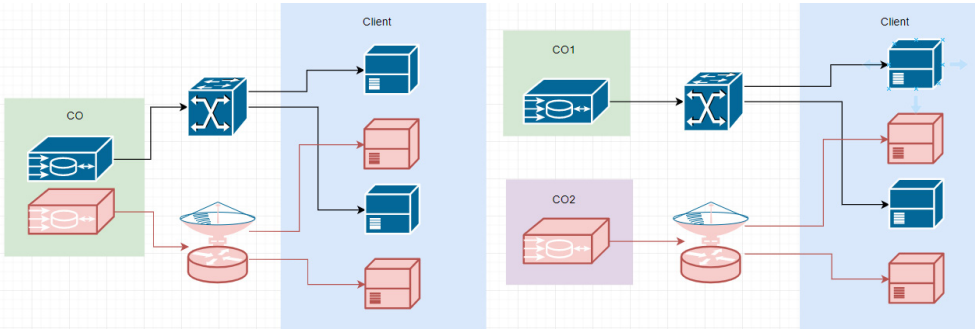


Рис. 5

Активное и пассивное резервирование каналов на основе топологии двойного кольца и MASH

Самым главным преимуществом технологии PON является минимизация оборудования сетевого и канального уровней. Простота инсталляции сети на этапе пуско-наладки и минимальное количество конфигурируемых узлов позволяет избежать отказа сетей в результате проблем с питанием и сбоев конфигурационных файлов, а диагностика и устранение неполадок на таких сетях производится в короткие сроки.

Следуя концепции минимизации активного сетевого оборудования в [11] предложен способ организации канала на основе решетки массива волноводов (Arrayed-waveguide grating, AWG), что позволяет сократить количество промежуточных узлов, повысить скорость и понизить стоимость развертывания связи, минимизировать затраты на обслуживание. В целях обеспечения требуемого значения коэффициента готовности 0,99999 для сети на основе AWG используется топология двойного кольца: создаются два независимых кольца с четырьмя AWG. Это позволяет обеспечить защиту от нескольких одновременных отказов. Принцип работы данной схемы резервирования заключается в использовании чувствительного модуля защиты. Задержка переключения канала в случае возникновения отказа на сети связи для модуля составляет менее 12 мс для всех клиентов. В [12] описан процесс восстановления прямой и обратной связей при отказе на канале.

При большом объеме передаваемого трафика становится актуальным резервирование на основе WDM-PON [13] с функциями защиты и локализации ошибок. В этом случае работа канала связи продолжается даже при отказе нескольких волоконных линий.

При организации кольца используется несколько ONU, связанных между собой двойным кольцом и передающими трафик в обоих направлениях. Такой тип резервирования предпочтителен для операторских сетей, так как является дорогостоящим и чаще всего в такой архитектуре организовывается канал с максимальной пропускной способностью.

В условиях стремительного развития беспроводного широкополосного доступа становится актуальным резервирование с помощью беспроводных технологий, в том числе и MASH, представляющую собой полносвязную беспроводную сеть, основанную на принципе Peer radio. При этом каждый узел такой сети может одновременно принимать на себя функцию коммутатора и маршрутизатора для соседних узлов. Вследствие этого достигается большая дальность передачи сигналов, а дополнительные точки (узлы) играют роль усилителя сигнала и передают трафик на основании данных о сети в целом. В [14,15] предложено доставлять трафик до MASH-портала и далее передавать его по беспроводной сети частично либо в полном объеме.

Расчёт целесообразности использования метода резервирования для сети

Чтобы принять решение в пользу конкретного типа резервирования требуется произвести аналитическую оценку прироста качества сервиса на основании изменения показателей надежности.

Значимым параметром для операторов связи является показатель влияние отказа на имидж оператора (Failure Impact, FI), который рассчитывается по формуле [16]:

$$\mathrm{FI} = \mathrm{N}\overline{\mathrm{K_г}},$$

где $\overline{\mathrm{K_г}}$-коэффициент неготовности, N – количество ONU.

В ходе оценки рентабельности резервирования рассчитывается стоимость восстановления после отказа $Ц_в$ [12]:

$$Ц_в = \frac{T_c}{\mathrm{MTBF}}(Ц_з + \mathrm{MTTR}\ Ц_б)$$

где $Ц_з$ – стоимость заменяемых элементов, $Ц_б$ – оплата услуг ремонтной бригады, T_c/MTBF – среднее число отказов за срок эксплуатации сети T_c, MTTR – среднее время, затраченное на ремонт.

Также учитываются затраты на электроэнергию $Ц_э$, на оплату штрафных санкций $Ц_ш$ за время неготовности в соответствии с SLA и на аренду СО. Полученные затраты сопоставляют с выручкой от реализации услуги и принимают решение об экономической целесообразности использования конкретного метода резервирования на сети.

Еще одним способом анализа целесообразности резервирования элементов сети является анализ отношений показателей надежности для резервированного и нерезервированного канала:

$$K_1 = \frac{Q(t)}{Q_m(t)}, K_2 = \frac{T_m}{T},$$

где $Q_m(t)$ – вероятность отказа резервированного устройства, $Q(t)$ – вероятность отказа нерезервированного устройства, T_m – среднее время безотказной работы резервированного устройства, T – среднее время безотказной работы нерезервированного устройства.

Из результата данной оценки следует, что наиболее экономически эффективным является поэлементное резервирование канальных составляющих, а оптимизация резервирования компонентов канала может быть сведена к задачам линейного и динамического программирования.

Заключение

Обеспечение рационального резервирования канала связи является важной задачей планирования сети и дает возможность достичь требуемого значения коэффициента готовности сети и предоставить качественный сервис конечному пользователю.

При выборе между одним и несколькими СО, выборе архитектурного решения и аппаратных компонентов требуется учитывать все издержки, возникающие в ходе эксплуатации канала. Тип используемой технологии резервирования также зависит от заявленных в SLA требований к каналу и возможности технической реализации того или иного технического решения.

На текущий момент получили широкое распространение методы резервирования с помощью схемы защиты типа A, B, C, D, где резервирование производится для части элементов либо для всей цепи включения канала, включая СО. Востребован тип резервирования на основе WDM-PON для сетей с повышенным требованием к коэффициенту готовности. Также перспективными являются методы резервирование на основе беспроводных сетей MASH и на основе решетки массива волноводов AWG и чувствительного модуля защиты.

Литература

1. *Егунов М.М., Шувалов В.П.* Анализ структурной надежности транспортной сети // Вестник СибГУТИ. 2012. № 1. С. 54-59.
2. *Нетес В.А.* Выбор показателей надежности сетей доступа // Первая миля. 2019. № 8. С. 52-55.
3. *Netes V.* Dependability measures for access networks and their evaluation // Proc. of the 26th Conf. of Open Innovations Association FRUCT, Yaroslavl, Russia, 23-25 April 2020. P. 352-358.
4. *Нетес В.А.* Основы теории надежности. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2019. 102 с.
5. https://www.anylogic.ru.
6. https://www.netacad.com/ru/courses/packet-tracer.
7. *Kantarci B., Mouftah H.T.* Availability and Cost-Constrained Long-Reach Passive Optical Network Planning // IEEE Transactions on Reliability. Vol. 61. No. 1, March 2012. P. 113-124.
8. *Kantarci B. and Mouftah H.T.* Availability and Cost Constrained Fast Planning of Passive Optical Networks under Various Survivability Policies // 35th Annual IEEE Conference on Local Computer Networks LCN. Denver, Colorado, 2010. P. 113-124.
9. ITU-Y Rec. G983.1. Broadband Optical Access Systems Based on Optical Network (PON). 1998.
10. *Kantor M., Chen J., Wosinska L., Wajda K.* Technoeconomic analysis of PON protection schemes Proc. // IEEE Broadband Europe, Antwerp, Belgium. 2007.
11. *Simmons J.M.* Survivable Passive Optical Networks Based on Arrayed-Waveguide-Grating Architectures // Journal Of Lightwave Technology. Vol. 25. No. 12, December 2007. P. 3658-3668.
12. *Wong E., Lee K.-L.* Automatic protection, restoration, and survivability of long-reach passive optical networks // IEEE ICC 2011. P. 305-310.
13. *Cheng X., Wen Y.J., Xu Z., Wang Y, Yeo Y.-K.* Survivable WDM-PON with self-protection and in-service fault localization capabilities // Optics Communications. Vol. 281. No. 18, June 2008. P. 4606-4611.
14. *Вишневский В., Лаконцев Д., Сафонов А., Шпилев С.* Mesh-сети стандарта IEEE 802.11s – технологии и реализация // Первая миля. 2008. № 2-3. С. 26-31.
15. *Ray S., Miedard M., Zheng L.* Fiber Aided Wireless Network Architecture // IEEE Journal on selected areas in Communications. Vol. 29. No. 6, June 2011. P. 1284-1294.

16. *Dixit A., Mahloo M., Lannoo B., Clien J., Wosinska L., Colle D., Pickavet M.* Protection strategies for Next Generation. Passive Optical Networks -2 // International Conference on Optical Network Design Modeling, 2014. P. 13-18.

17. *Сулейманов А.А., Нетес В.А.* Анализ времени подключения к облачной услуге "виртуальный рабочий стол" // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 7. С. 41-46.

18. *Нетес В.А.* Двусторонние оценки для показателей качества обслуживания с учетом надежности обслуживающих приборов // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 8. С. 75-77.

19. *Нетес В.А.* Преподавание теории надежности студентам инфокоммуникационных направлений // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2018. Т. 7. № 2. С. 36-39.

20. *Нетес В.А.* Соглашения об уровне обслуживания при предоставлении сигналов синхронизации // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 2. С. 137-140.

LR-LONG (LONG-REACH PASSIVE OPTICAL NETWORK) REDUNDANCY METHODS ANALYSIS

Alexandra V. Kudryavtseva,
Graduate MTUCI, Moscow, Russia,
motoko@bk.ru

Victor A. Netes,
Professor of the Department of CN&TS, Doctor of Technical Sciences,
Senior Scientist, MTUCI,Moscow, Russia,
v.a.netes@mtuci.ru

Abstract

The paper provides an overview of the types and methods of reserving LR-PON channels, analyzes the profitability and relevance of redundancy as a method of ensuring network reliability in modern market conditions, examines the algorithms for evaluating network redundancy based on reliability parameters and takes into account the costs of emergency recovery operations.

Keywords: *LR-PON redundancy, reliability, AWG, WDM-PON, MASH, availability, Failure Impact, recovery costs.*

СРЕДСТВА СОЗДАНИЯ ХРАНИЛИЩ ДАННЫХ

Некрасов Антон Анатольевич,
магистрант МТУСИ, Москва, Россия,
aa.nekrasov.w@gmail.com

Гаврилов Сергей Олегович,
магистрант МТУСИ, Москва, Россия,
gavrilov.s1999@gmail.com

Беленькая Марина Наумовна,
старший преподаватель кафедры СИТИС, МТУСИ, Москва, Россия,
mn.belenkaya@mail.ru

Аннотация

Описана роль хранилищ данных в корпоративной информационной системе. Рассмотрены основные сложности, возникающие при разработке и сопровождении хранилищ данных. Описаны схемы данных. Представлены методологии построения хранилищ данных иархитектура хранилищ данных. Дано описание основных модулей хранилища данных. Рассмотрено ПО, используемое при создании и администрировании хранилищ данных.

Ключевые слова: *хранилища данных, витрины данных, ETL, проблемы разработки и сопровождения хранилищ данных, архитектуры схем БД, методологии хранилищ данных, выбор СУБД для хранилищ данных, средства управления и администрирования.*

Задача хранилища данных (Data Warehouse – DW) – это создание единого интегрированного источника подготовленных данных для анализа из множества источников данных компании. DW отделяют рабочую нагрузку анализа от рабочей нагрузки транзакций. Витрины данных (Data mart – DM) – это часть DW, ориентированная на конкретную бизнес-линию. Data Mart содержат агрегированные данные, собранные для анализа в определённом разделе или отделе организации [9, 10]. Преимуществом использования DW является то, что гарантируется чистота данных в хранилище. При этой технологии предполагается работа в режиме OLAP (Аналитическая обработка), а не OLTP (Транзакционная обработка).

Сложность разработки и сопровождения хранилищ данных заключается в том, что хранилище данных хранит информацию за большой временной период для временного анализа. Средства ETL (Extract, Transform, Load – извлечение, преобразование, загрузка), постоянно загружают новые данные в DW. Большая часть затрат на проектирование и разработку хранилища тратятся на разработку ETL процессов. Эти процессы являются основой хранилища данных, когда оно запущено в эксплуатацию. Во время сопровождения большинство изменений происходит в ETL процедурах и они связаны с изменениями источников данных. Также большая часть ошибок во время эксплуатации являются ошибками в исходных данных, которые отслеживаются во время выполнения ETL процедур.

Архитектура

Архитектура хранилища данных зависит, прежде всего, от потребности организации и диктуется бизнес-линиями и средствами, для которых в качестве источника будет выступать хранилище данных. В зависимости от выбора архитектуры схемы БД, методологии проектирования и архитектуры хранилища данных будут меняться также и трудовые затраты необходимые для построения.

Принципы построения схем хранилищ данных [1, 7]:

- «Звезда» - самый простой и наиболее широко используемый стиль схемы. Состоит из одной или нескольких таблиц фактов, ссылающихся на любое количество таблиц справочников. Эффек-

тивна для обработки простых запросов. Схема Звезда, имеющая много измерений, иногда называется схемой «многоножки». Данные таблицы денормализованные, это означает, что смягчены требования, предъявляемые к транзакционным реляционным базам данных во время проектирования и реализации звездообразной схемы. Преимуществом подхода является повышение производительности запросов для чтения по сравнению с нормализованными схемами и быстрое агрегирование за счет простых запросов. Звездообразные схемы могут использоваться системами OLAP для эффективного построения кубов OLAP, так как основные OLAP-системы предоставляют режим работы ROLAP, который может использовать звездообразную систему непосредственно в качестве источника без создания новой структуры куба. Пример звездообразной схемы представлен на рисунке 1;

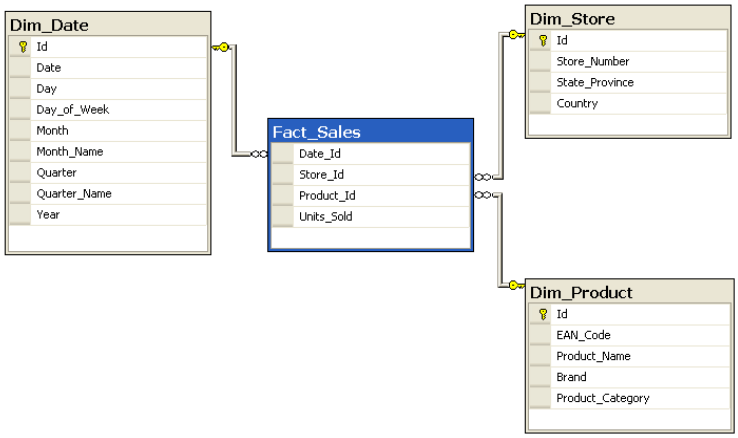


Рис. 1. Пример звездообразной схемы хранилища данных

- «Снежинка» – логическое расположение таблиц в многомерной БД. Представляет собой централизованные таблицы фактов связанных с несколькими измерениями. Приводя измерения звездообразной схемы к 3NF, получаем схему «Снежинка». Преимуществами данной схемы является нормализация, что приводит к экономии места, но вносит дополнительные сложности в запросы за счет добавления соединений. За счет нормализации появляются гарантии целостности данных. Загрузка данных должна строго контролироваться, чтобы избежать аномалий обновления и вставки данных, нарушающих историчность хранилища данных.

Пример звездообразной схемы представлен на рисунке 2.

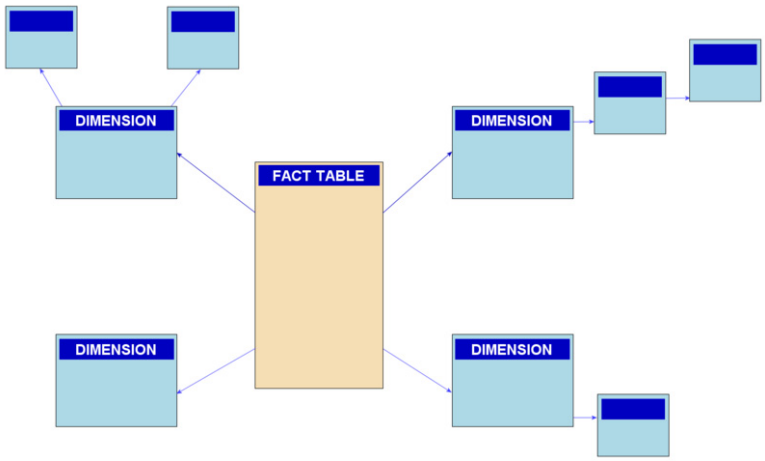


Рис. 2. Пример схемы хранилища данных «Снежинка»

С точки зрения места хранения, таблицы измерений обычно несоизмеримо малы по сравнению с таблицами фактов. Это приводит к уменьшению потенциального преимущества схемы «Снежинка» перед схемой «Звезда». Часто встречаются гибридные схемы, которые представляют собой объединение схем «Звезда» и «Снежинка». За счет гибридных схем удается использовать преимущества обеих схем в зависимости от потребностей в определенной части схемы хранилища данных.

Различают 5 различных методологий проектирования хранилищ данных:

- Inmon - автором данной методологии является Билл Инмон. Модель является нисходящей. При проектировании необходимо иметь целостное представление о структуре хранилища и моделировать ее в соответствии с 3NF [2]. При разработке на основе данной модели требуется высокая квалификация разработчиков для разработки модели данных и интеграции в нее предметных областей. Для запуска модели в эксплуатацию требуется больше времени, но поддерживать ее работоспособность гораздо легче, чем другие.

Поток данных в модели Inmon:

1. Загрузка данных из источников в Staging area;
2. Загрузка данных из Staging Area в Data Warehouse;
3. Заполнение Data marts, созданных поверх Data Warehouse.

- Kimball – автором данной методологии является Ральф Кимбалл. Модель является восходящей. Данный подход был разработан для ответов на конкретные вопросы в предметной области [3]. Подход не имеет гибкости по сравнению с остальными моделями, но позволяет быстро создать и внедрить хранилище данных.

Поток данных в модели Kimball:

1. Загрузка данных из источников в Staging area;
2. Загрузка данных из Staging Area в Data Warehouse;
3. Заполнение Data marts созданных непосредственно в хранилище данных Data Warehouse.

- Data Vault - подход разработанный Дэном Линстедом представляет собой гибридный подход, объединяющий лучшие стороны 3NF и схемы «Звезда» [4]. Данная методология гибкая, масштабируемая, последовательная и адаптируемая к потребностям пользователя. Методология специально разработана для удовлетворения потребностей современных корпоративных хранилищ данных. Существенным недостатком является большое количество join операций. Требуется обязательное наличие Data Mart, так как данная методология плохо подходит для прямых запросов.

Компоненты Data Vault:

- Hub - таблицы предназначенные для описания бизнес сущностей. В совокупности содержит бизнес-ключи, например ИНН организации;
- Link - таблицы, реализующие между хабами связи многие-ко-многим;
- Satellite - таблицы содержащие описательные атрибуты Hub или Link. Содержит только один внешний ключ.

Поток данных в модели Data Vault:

1. Загрузка данных в Hub-ы;
2. Загрузка Link и Satellite (возможна параллельная загрузка, если нет связей Link-to-Link);
3. Расчет Data Marts.

- Data Lake + Data Warehouse – подход, предлагаемый вендором Snowflake. Позволяет объединить и получить преимущества хранилищ данных и больших данных [5]. Data Lake подразумевает хранение всех структурированных, полуструктурированных и неструктурированных данных. Оно является дополнительным слоем перед DW. Предполагается построение на его основе DW. Data Lake требует учета и управления, иначе может перестать быть эффективным. Данный подход выделяет гибкость и доступность данных. Он обладает способностью предоставлять пользователю или приложению данные без схемы и в “естественном формате” независимо от происхождения. Данный подход гораздо дороже по сравнению с другими, но он обладает большим числом преимуществ по сравнению с классическими хранилищами данных.

Поток данных в модели Data Lake + Data Warehouse:

1. Загрузка данных в облачное хранилище, HDFS или другой репозиторий;
2. Построение метаданных о загруженных данных.

- Lakehouse – термин, введенный в начале 2020 года компанией Databricks [6]. Методология подразумевает работу непосредственно на исходных данных, (большинство ML/AI инструментов предназначены на работу с неструктурированными данными и предварительная обработка, а также очистка данных лишь увеличивают время работы). Сообщество специалистов посчитало данную методологию не готовой к выходу на рынок, так как большое количество необработанных и не очищенных данных могут привести к ложным выводам и предположениям, что отталкивает нас от главной концепции хранилищ данных - быть одним источником правды компании.

Поток данных в Lakehouse подразумевает только загрузку данных в хранилище.

Хранилища данных и их архитектура различаются в зависимости от специфики ситуации в организации.

Далее будет рассмотрена архитектура хранилища данных предлагаемая компанией Oracle, в которой выделяются три основных модуля [1]:

- Staging area – место хранения “сырых” данных, загруженных из источников и подготовленных к обработке и загрузке в DW;
- Data Warehouse - консолидированное хранилище необработанных данных, являющееся центром архитектуры хранилища данных;
- Data Marts - встроенное хранилище данных, предназначенное для определенного направления бизнеса, например продаж, маркетинга или финансов. В зависимой витрине данных данные могут быть получены только из DW. В независимой витрине данных можно собирать данные из DW и SA (Staging area- область временного хранения данных). Они могут быть созданы физически или реализованы чисто логически с помощью представлений. Кроме того, витрины данных могут быть размещены вместе с корпоративным хранилищем данных или построены как отдельные системы.

Классическая схема хранилища данных представлена на рисунке 3.

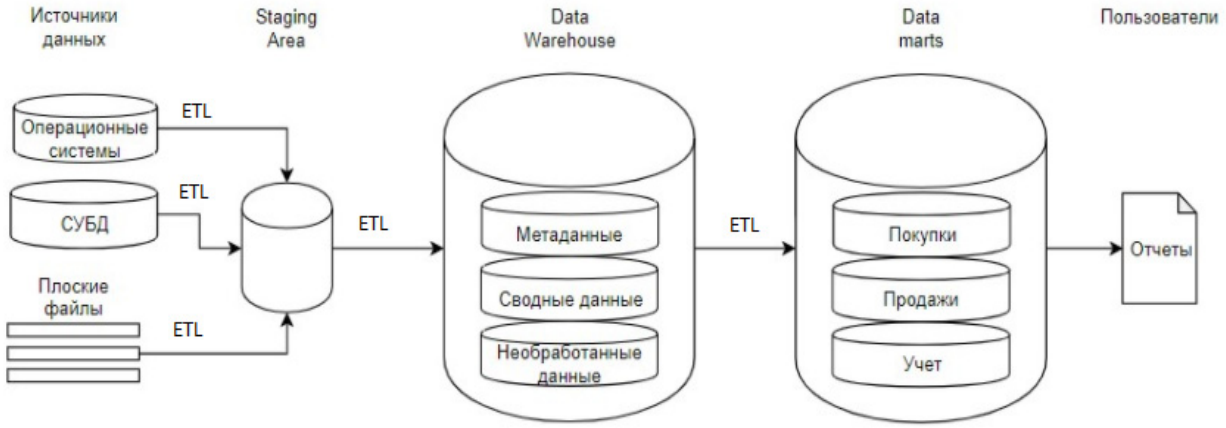


Рис 3. Архитектура хранилища данных, с промежуточной областью и витринами данных, предлагаемая компанией Oracle [1]

- Источники данных: базы данных, приложения, репозитории или файлы, которые передают данные в хранилище данных.
- Метаданные: данные, описывающие данные и другие структуры, такие как объекты, бизнес-правила и процессы.
- Сводные данные: механизм для предварительного вычисления распространенных дорогостоящих, длительных операций для быстрого извлечения данных.
- Необработанные данные: данные загруженные в исходном виде.

Список работ необходимых для разработки и сопровождения хранилищ данных описанных компании Oracle [1, 7, 8]:

- Настройка базы данных для использования её в качестве хранилища данных;
- Проектирование хранилища данных;
- Обновление программного обеспечения и версии хранилища данных;
- Управление схемой и объектами базы данных;
- Управление пользователями;
- Управление безопасностью;
- Разработка ETL;
- Генерация отчетов на основе данных в хранилище;
- Резервное копирование и восстановление в случае необходимости;
- Наблюдение за производительностью хранилища данных и корректировка при необходимости.

Инструменты

Для создания DW необходимо 3 основных вида средств [1]:

1. ETL;
2. СУБД;
3. Средства разработки и администрирования СУБД.

В качестве ETL инструментов используется такие инструменты, как Pentaho Data Integrator, Loginom, Oracle Data Integrator, Apach Airflow, Informatica или ViExtract. Из вышеперечисленных средств Oracle Data Integrator и Informatica являются дорогостоящими и сложными в реализации продуктами, Apach Airflow распространяется под свободной лицензией, но также сложен в реализации. ViExtract свободно распространяемое ПО, но отсутствует визуальный интерфейс, и все процессы пишутся на языке Python3.

В результате вышеперечисленных факторов, на проектах по построению корпоративных хранилищ данных зачастую используются Pentaho Data Integrator или Loginom. Также возможно выполнить задачу ETL не используя специализированного ПО, например, с помощью библиотеки Petl языка Python3, но необходим отдельный планировщик и оркестратор.

В коммерческих проектах используются такие СУБД, как Oracle, Postgres Pro или Microsoft SQL Server. В государственных организациях необходимо использовать ПО из Единого реестра российских программ для электронных вычислительных машин и баз данных. В связи с этим из вышеперечисленных СУБД используется только Postgres Pro.

Инструменты администрирования выбираются в зависимости от выбранной СУБД. Для Oracle достаточно среды разработки и администрирования СУБД Oracle SQL Developer, а для Postgresql данным средством будет являться PgAdmin4.

Заключение

Таким образом, при использование корпоративного хранилища данных у компании появляется единый источник консолидированных достоверных данных, которые будут использоваться всеми отделами предприятия. Основные проблемы, возникающие при проектировании и сопровождении хранилища данных, связаны с источниками данных и ETL процедурами. Существуют различные типы схем и методологий проектирования, выбор которых основывается на требованиях, предъявляемых к хранилищу, информации о бизнес модели, которая имеется на стадии проектирования, или выделяемых средств на разработку. Для разработки и сопровождения хранилища данных необходимо три основных вида ПО, выбор которого основывается на бюджете, заложенном на приобретение ПО, или требованиях, которые выдвигает заказчик.

Литература

1. Padmaja Potineni, Oracle Database Data Warehousing Guide, 21c [Электронный ресурс]: Data Warehousing Guide URL: https://docs.oracle.com/en/database/oracle/oracle-database/21/dwhsg/index.html (дата обращения: 31.03.2021).
2. *L. Yessad and A. Labiod,* "Comparative study of data warehouses modeling approaches: Inmon, Kimball and Data Vault," 2016 International Conference on System Reliability and Science (ICSRS), Paris, France, 2016, с. 95-99, doi: 10.1109/ICSRS.2016.7815845.
3. The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling, 3rd Edition:Ralph Kimball, 2013. -603 с.
4. *Dan Linstedt.* Data Vault Standards. [Электронный ресурс]: Стандарты Data Vault v1.2. URL: https://danlinstedt.com/allposts/datavaultcat/standards/data-vault-loading-specification-v1-2/ (дата обращения: 21.03.2021).
5. *Nikolay Komissarenko. Data Lake.* [Электронный ресурс]: Data Lake. URL: https://www.bigdataschool.ru/wiki/data-lake (дата обращения: 21.03.2021).
6. *M. Armbrust, A. Ghodsi, R. Xin and M. Zaharia. Lakehouse:* A New Generation of Open Platforms that Unify Data Warehousing and Advanced Analytics. 2021,-8 с.
7. *Thomas Connolly,* University of Paisley. Database Systems: A Practical Approach to Design, Implementation, and Management.:Carolyn Begg, Paisley University, 2015. 1440 с.
8. *Беленькая М.Н., Малиновский С.Т., Яковенко Н.В.* Администрирование в информационных системах. М.: Горячая линия – Телеком, 2019. 408 с.

9. *Краснов К.А., Корионов И.П., Хороший А.А., Беленькая М.Н.* Анализ атак типа "отказ в обслуживании" при использовании протоколов ICMP, UPD, TCP // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2018. № 2. С. 116-118.

10. *Беленькая М.Н., Зайцев Е.С., Акопян В.А., Кошепаров Д.Я.* Обзор методов анализа сетевого трафика средствами DPI // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2018. № 1. С. 15-20.

OVERVIEW OF DATA WAREHOUSE DEVELOPMENT TOOLS

Anton A. Nekrasov,
Graduate MTUCI, Moscow, Russia,
aa.nekrasov.w@gmail.com

Sergey O. Gavrilov,
Graduate MTUCI, Moscow, Russia,
gavrilov.s1999@gmail.com

Marina N. Belenkaya,
Senior Lecturer of the Department of NITES, MTUCI, Moscow, Russia,
mn.belenkaya@mail.ru

Abstract

The role of data warehouses in the corporate information system is considered. The main difficulties in the development and maintenance of a data warehouse are considered. These schemes are described. Methodologies for constructing data warehouses are presented. The architecture of data warehouses is presented. The main modules of the data warehouse are described. The software used in the creation and administration of the data warehouse is considered.

Keywords*: data warehouses, data marts, ETL, problems of development and maintenance of data warehouses, database schema architectures, data warehouse methodologies, the choice of a DBMS for the data warehouse, management and administration tools.*

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ СЕГМЕНТАЦИИ ВИДЕОПОТОКА В КВАЗИРЕАЛЬНОМ ВРЕМЕНИ

Власов Глеб Геннадьевич,
студент МТУСИ, Москва, Россия,
gleb2605@bk.ru

Городничев Михаил Геннадьевич,
доцент кафедры МКиИТ, к.т.н., МТУСИ, Москва, Россия,
m.g.gorodnichev@mtuci.ru

Аннотация
В статье рассматривается механизм реализации интеллектуальной системы сегментации видеопотока в квазиреальном времени. Описываются процесс первичной обработки собранного набора данных (датасета) и его дальнейший анализ, а также структура свёрточной нейронной сети, используемая для решения данной проблемы.

Ключевые слова: *искусственный интеллект, нейронные сети, компьютерное зрение, сегментация видеопотока.*

1. Выбор данных для обучения

Для реализации данного проекта использовалась база данных Udacity Self-Driving car Nanodegree Program, которая содержит 16 048 RGB изображений с разрешением 64 × 64 пикселей.

Рис. 1. Пример негативных изображений

Рис. 2. Пример позитивных изображений

В изображениях класса «транспортные средства» содержится 8048 фотографий различных автомобилей с разных ракурсов. Эти изображения содержат множество шумов, таких как тени, световые блики, присутствуют просто размытые изображения. Во втором классе изображений «части дорожного полотна» находятся фотографии различных объектов дорожного полотна (рис. 1 и 2). Для задачи классификации несбалансированная выборка как положительных, так и отрицательных обучающих примеров оказывает огромное влияние на производительность сети [2].

2. Расширение данных (аугментация)

Свободно распространяемые, обучающие базы изображений отлично подходят для учебных работ, но почти всегда их нельзя применять в реальных задачах. Приём расширения данных позволяет создавать дополнительные обучающие данные из уже доступных путём изменения изображений

различными случайными преобразованиями. В идеале модель на этапе обучения не должна видеть одно и то же изображение дважды. Существует несколько способов подготовки выборки изображений для создания систем распознавания.

Обучающие наборы данных из естественных изображений, которые создаются на основе реальных данных. Создание таких датасетов состоит из следующих этапов:

1. Сбор данных (например, снятие видеопотока с видеорегистратора машины);
2. Фильтрация – проверка изображений на ряд необходимых требований;
3. Написание разметчика датасета или настройка готового.
4. Разметка (выделение интересуемых объектов);
5. Присвоение меток.

Этот алгоритм требует значительных временных затрат, но с другой стороны, по результатам обучения системы на таких данных можно узнать об её эффективности в реальных условиях.

Обучающие наборы данных состоят из искусственных изображений. Достаточно взять несколько реальных изображений и с помощью разных манипуляций сгенерировать необходимое число примеров для обучения. Существуют следующие виды изменений [3]:

1. Изменение яркости/цвета;
2. Замена фона (или других частей изображения);
3. Геометрические (аффинные, проективные и др.);
4. Уникальные преобразования, применяемые для определённой задачи (световые блики, размытия, шумы, добавление капель дождя, снега), рисунки 3 и 4.

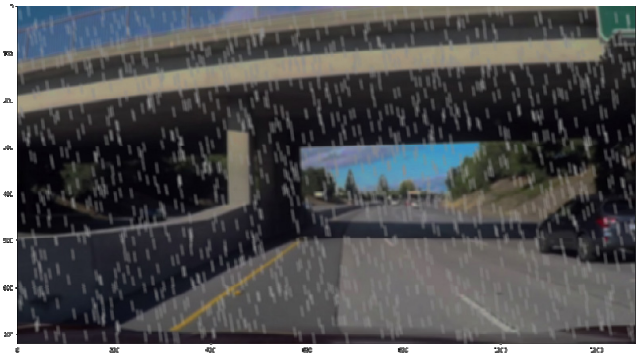


Рис. 3. Добавление эффекта искусственного дождя

Рис.4. Добавление эффекта искусственного снега

Этот подход помогает значительно экономить время, но достаточно сложно предсказать эффективность данного метода в реальных условиях.

3. Описание нейронной сети

Свёрточный слой.

Главной составляющей свёрточной нейронной сети является свёртка. Эти слои содержат фильтры для каждого канала изображения и ядро свёртки, которое является матрицей N x N.

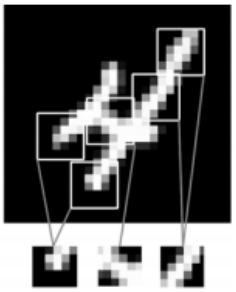


Рис. 5. Примеры локальных шаблонов

Свёрточные нейронные сети обладают несколькими важными свойствами:

1) Инвариантностью излучаемых свёрточных ядер в отношении переноса. После изучения какого-либо ядра в центре изображения свёрточная нейронная сеть сможет найти его в любом другом месте. Эта способность повышает эффективность свёрточных сетей в задачах компьютерного зрения, так как видимый мир, по сути является инвариантным в плане переноса. Этим сетям требуется намного меньше обучающих образцов для получения результата.

2) Способностью изучать пространственные иерархии ядер. Первый свёрточный слой будет изучать небольшие локальные признаки, второй - более крупные (рисунок 6), состоящие из признаков, возвращаемых первым слоем, и т.д. [1].

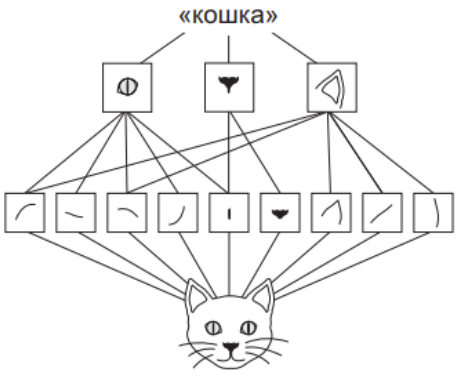


Рис. 6. Пример второго свойства

Свёртка двигает окно размером 3 x 3 или 5 трёхмерной входной карте признаков, останавливается в каждой возможной позиции и извлекает трёхмерный шаблон окружающих признаков. Затем каждый из полученных шаблонов преобразуется в одномерный вектор. Затем все эти векторы формируют трёхмерную выходную карту признаков.

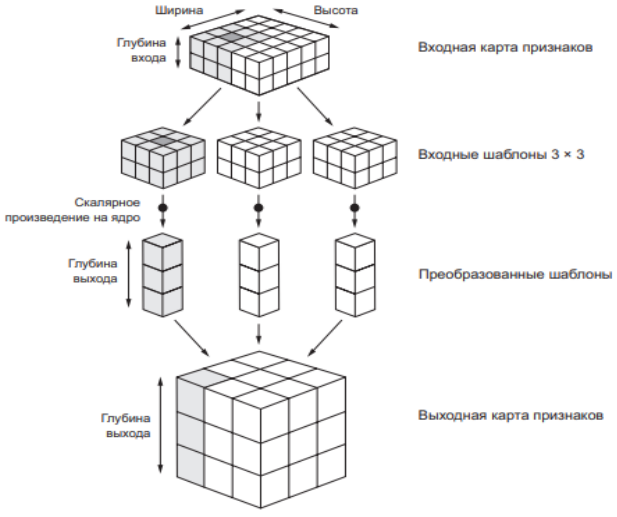


Рис. 7. Принцип работы свёрточного слоя

Операция пулинга является нелинейным уплотнением карты признаков (рис. 8). Из входной карты признаков извлекается ядро, и из него выбирается максимальное значение для каждого канала. Уменьшение разрешения используется для уменьшения количества коэффициентов в карте признаков для обработки. Пулинг даёт возможность сделать инвариантным представление относительно малых переносов входа, выделяя основные признаки. Инвариантность переноса говорит о том, что при сдвиге входа на некоторую величину, значение большинства задействованных пулингом выходов не изменится [3]. Обычно слой пулинга размещают после слоя свёртки, но перед новой свёрткой.

Слой пулинга

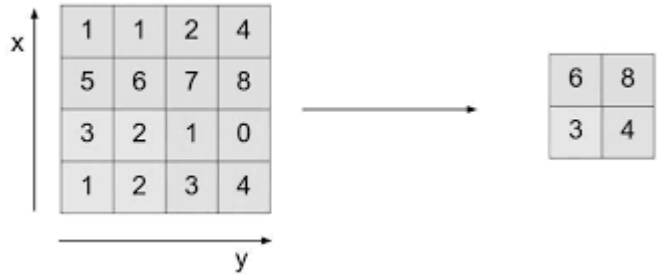


Рис. 8. Пример пулинга

Сеть с прямым распространением

После свёрточной нейронной сети идёт полносвязная сеть, которая выполняет роль связи для абстрактных признаков. Как правило, такая сеть представляет собой многослойный персептрон [1-3]. Каждый нейрон предыдущего слоя этой сети связан со всеми нейронами следующего слоя (рис. 9).

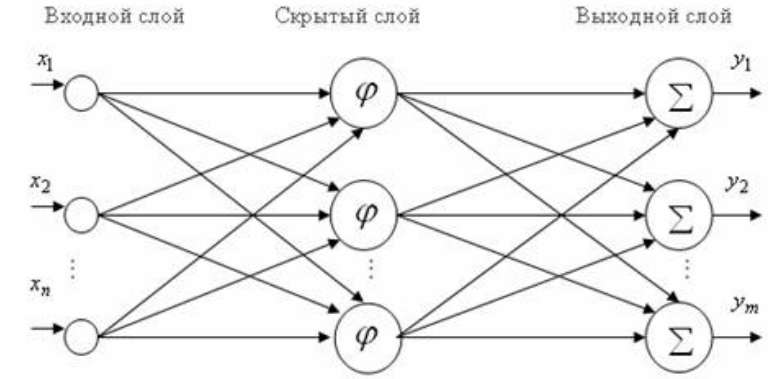


Рис. 9 . Нейронная сеть прямого распространения

Функция активации

Огромную роль в свёрточных нейронных сетях играет функция активации. В данном проекте используется функция активации ReLU. Она возвращает значение x, если x положительно, и 0 в других случаях (рис. 10).

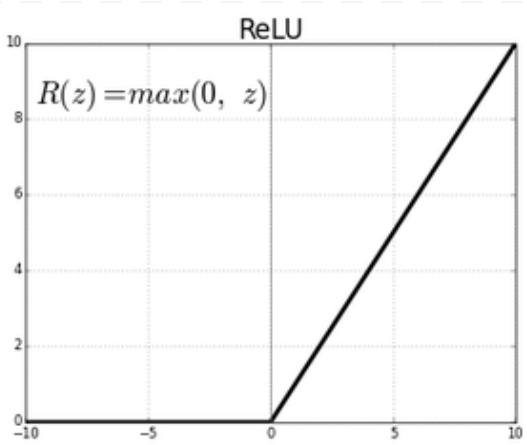


Рис. 10. Рисунок функции активации ReLu

Преимущества ReLU:

1) Для вычисления гиперболического тангенса или сигмоиды требуются ресурсоёмкие операции, такие как возведение в степень, а ReLu можно реализовать с помощью простого порогового преобразования матрицы.

2) ReLu значительно повышает скорость сходимости стохастического градиентного спуска, (этот вид градиентного спуска часто используется в задачах компьютерного зрения).

Одним из недостатков функции ретификации является то, что она может привести к такому обновлению весов, что данный нейрон никогда больше не активируется. В таком случае, градиент, проходящий через этот нейрон, всегда будет равен нулю. Обычно эта проблема решается настройкой скорости обучения.

Существует несколько разных блоков линейно ретификации:

Leaky ReLU (с «утечкой») - является одной из попыток решить указанный выше недостаток выхода из строя обычных ReLu. Функция LReLu имеет вид f(x) = ax при x<0 и f(x) = x при x >= 0;

Parametric ReLU - авторы утверждают, что использование этой функции позволило превысить уровень способности человека при распознавании изображений базы данных ImageNet;

Randomize ReLU - позволяет уменьшить переобучение благодаря характерному элементу случайности;

Способы регуляризации

Регуляризация — это методы контроля ёмкости нейронной сети, которые позволяют предотвратить переобучение, математическая операция, ограничивающая запоминание, которая способствует обобщённому обучению [4].

В данном проекте использован простой, но очень эффективный метод Dropout. Его суть заключается в том, что во время обучения некоторые узлы, попадающие в полносвязный слой случайным образом, отбрасываются. Удаление узла означает, что значение его веса устанавливается на 0. Такие узлы выбираются случайно на каждом этапе градиентного спуска (рисунок 11).

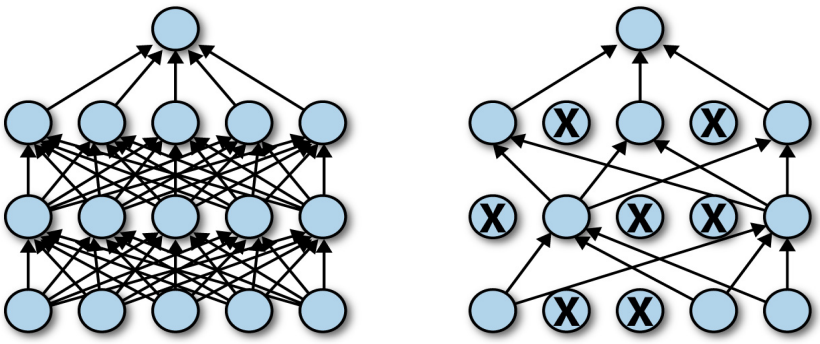


Рис. 11. Отображение принципа работы Dropout

Заключение

В результате работы реализована программа по сегментированию видеопотока, детектированию транспортных средств и определению дорожной полосы. Исследованы методы первичной обработки датасета и расширения данных. Построена структура эффективной свёрточной нейронной сети для решения поставленной задачи.

Литература

1. Deep Learning with Python François Chollet - by Manning Publications .
2. Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification - Kaiming He Xiangyu Zhang Shaoqing Ren Jian Sun.
3. A Simplified Computer Vision System for Road Surface Inspection and Maintenance Marcos Quintana, Juan Torres, and José Manuel Menéndez.
4. *K. Chatfield, K. Simonyan, A. Vedaldi, and A. Zisserman.* Return of the devil in the details: Delving deep into convolutional nets. In BMVC, 2014.

DEVELOPMENT OF AN INTELLIGENT SYSTEM FOR SEGMENTING A VIDEO FLOW IN QUASI-REAL TIME

Gleb G. Vlasov,
Student MTUCI, Moscow, Russia,
gleb2605@bk.ru

Mikhail G. Gorodnichev,
Associate Professor of Department of MC&IT, PhD., MTUCI, Moscow, Russia,
m.g.gorodnichev@mtuci.ru

Abstract

The article discusses the mechanism of realization of intelligent system of segmentation of video stream in quasi-real time. It describes the process of initial processing of the collected dataset and its further analysis, the structure of the convoluted neural network used to solve this problem.

Keywords*: artificial intelligence, neural networks, computer vision, video-flow segmentation.*

ПРИМЕНЕНИЕ СИСТЕМ РАСПОЗНАВАНИЯ ЕДИНИЦ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ

Бауэр Елисей Владимирович,
аналитик Центра перспективных разработок и исследований
ФГУП НПП «Гамма», Москва, Россия,
severjanen@rambler.ru

Воронова Лилия Ивановна,
заведующий кафедрой ИСУиА, д.ф.-м.н., профессор, МТУСИ, Москва, Россия,
voronova.lilia@yandex.ru

Аннотация

Бурное развитие в ведущих странах мира информационных технологий неизбежно привело к переосмыслению концепций применения систем распознавания, путей дальнейшего их развития и придания им многоцелевого характера. Системы распознавания на базе БПЛА занимают достойное место в производственных программах систем воздушной разведки военного назначения. Использование БПЛА в военных целях стало одним из важных направлений развития современной авиации и позволяет автоматизировать управление войсками, сократить потерю личного состава в бою за счет оперативной разведывательной информации о текущей обстановке. В этой связи актуальна задача создания мобильных, простых в эксплуатации и дешевых средств ведения воздушной разведки. Основой для распознавания объектов в реальном масштабе времени может быть алгоритм YOLO, предложенный Джозефом Редмоном (Joseph Redmon) и представляющий собой единую нейронную сеть, применяемую сразу ко всему изображению.

Ключевые слова: *БПЛА, YOLO, машинное обучение, искусственный интеллект, система распознавания, бронетехника, анализ данных, алгоритм, модель, авиация, автоматизированное управление войсками.*

Введение

На сегодняшний день искусственный интеллект (ИИ) является настоящим технологическим трендом. Растет число стартапов с применением технологий ИИ, крупнейшие гиганты IT-индустрии такие как, Microsoft, IBM, Yandex и Google борются за доминирование в области искусственного интеллекта. Правительства таких стран как США, Россия, Китай уделяют значительное внимание и привлекают ученых, программистов и математиков для разработки эффективных систем технического зрения на основе искусственного интеллекта в военной промышленности [1].

Системы технического зрения (СТЗ) предназначены для восприятия визуальной информации об окружающей среде, обработки и анализа изображений рабочих сцен с целью решения задачи распознавания образов. Под распознаванием образов понимается процесс, при котором на основании многочисленных характеристик (признаков) некоторого объекта определяется одна или несколько наиболее существенных, но недоступных для непосредственного определения его характеристик, в частности его принадлежность к определенному классу объектов. Данное определение является «кибернетическим» и используется в задачах искусственного интеллекта при анализе любых сложных изображений, когда отсутствует ограничение по времени обработки данных [2].

Ключевым движущим фактором развития СТЗ является компьютерное зрение. Проще говоря, компьютерное зрение-это дисциплина в рамках широкой области искусственного интеллекта, которая учит машины видеть. Его цель состоит в том, чтобы извлечь «смысл» из пикселей. [3]

Компьютерное зрение – это область искусственного интеллекта, которая позволяет компьютерам понимать и анализировать реальный мир. Используя модели глубокого обучения, машины могут точно идентифицировать и классифицировать объекты из цифровых изображений, а затем реагировать на то, что они «видят». Растущая потребность в автоматизации, спрос на робототехнику с визуальным контролем в отраслевых системах приводят к массовому использованию приложений

компьютерного зрения. Ожидается, что этот рынок вырастет с 10,9 млрд.$ до 17,4 млрд.$ к 2024 году, что означает среднегодовой темп роста 7,8%. [4]

На сегодняшний день, компьютерные системы могут выйти за рамки обычного распознавания объектов и научиться выявлять детали визуального мира. Нейронные сети можно обучить видеть триллионы изображений и видео, полученных из интернета.

Чтобы «компьютерный мозг» осваивал самые большие наборы данных классификации изображений «ImageNet», которые содержат 15 миллионов изображений в 22 тысячах классов объектов, была создана хорошо известная технология “Глубокого обучения”, продемонстрировавшая подавляющее превосходство в сравнении с традиционными компьютерными алгоритмами.

Глубокое обучение – это особый класс алгоритмов машинного обучения, который упрощает процесс извлечения и описания признаков с помощью многослойной сверточной нейронной сети (CNN multi-layer convolutional neural network). CNN стремится преобразовать входное изображение высокой размерности в низкоразмерное, но при этом получить высокоабстрагированный семантический выход. На основе массива данных от ImageNet и использования современных центральных и графических процессоров (CPU, GPU), методы, основанные на использовании глубокой нейронной сети (DNN), обеспечивают высокую производительность и беспрецедентное развитие компьютерного зрения, как в алгоритмических, так и в аппаратных реализациях. Однако высокая точность достигается ценой больших вычислительных затрат. С учётом этого для оптимизации рабочих нагрузок на основе DNN, исследуются выделенные аппаратные платформы, от универсальных графических процессоров, до специализированных процессоров приложений [5].

В статье рассмотрен созданный авторами набор данных трех классов танков для формирования системы распознавания целей на базе алгоритма глубокого обучения «YOLO» и «OpenCV».

Набор данных бронетехники и алгоритм YOLO

В работе используется новый подход для системы распознавания вооружений и военной техники, основанный на глубоком обучении и использовании алгоритме «YOLO». Ранее применение систем распознавания с БПЛА в ВПК основывалось только на методах K-средних, случайного леса и метода опорных векторов.

Предложенный Джозефом Редмоном (Joseph Redmon) алгоритм YOLO представляет собой единую нейронную сеть, которая применяется сразу ко всему изображению. Она одновременно выделяет и предсказывает зону обрамляющего прямоугольника (bounding boxes) и вероятности нахождения в них объектов различных классов.

При использовании этой системы нужно всего один раз пропустить изображение через нейронную сеть, чтобы предсказать объекты и их расположение.

YOLO предполагает обнаружение объектов как единую задачу регрессии, которая начинается с разрешения входного изображения (пикселей), а завершается вычислением координат обрамляющих прямоугольников и вероятностей принадлежности классам. При прогнозировании, YOLO рассматривает изображение глобально. В отличие от методов скользящего окна и методов областных предложений, алгоритм YOLO обрабатывает всё изображение целиком во время обучения и тестирования. Поэтому он неявно кодирует контекстную информацию о классах, а также их внешний вид, благодаря чему в этой модели ошибочное срабатывание детектора на фоне изображения менее вероятно, по сравнению с Fast R–CNN. При обучении на естественных изображениях и тестировании на художественных работах, YOLO также превосходит DPM и R–CNN, с большим отрывом. Поскольку YOLO использует сильное обобщение, вероятность его ошибки при применении к новым входным данным мала [6].

Набор данных для обработки нейронной сети состоит из 3 классов изображений современных образцов военной техники ведущих стран мира формата PGN, количество изображений приведено в таблице 1.

Таблица 1

Набор данных для обработки нейронной сети

№ п/п	Наименование и государство – изготовитель	Образец	Количество изображений
1	Танк Т-14 «Армата» - Российская Федерация		3508
2	Танк Т-90М - Российская Федерация		4304
3	Танк M1A2SEP «ABRAMS» - США		4535

YOLOv1.

Архитектура YOLO основана на модели распознавания GoogleNet. YOLOv1 имеет 24 сверточных слоя, за которыми следуют 2 полносвязанных слоя FC (рисунок1). Вместо входных слоев, используемых в GoogleNet, YOLOv1 использует редукционные слои 1x1, уменьшая глубину карт признаков, за которыми следуют слои 3x3. В качестве активационной функции в YOLOv1 применяется Leaky rectified linear unit (неплотный выпрямленный линейный блок – LReLu) (1):

$$\begin{cases} f(x) = ax \text{ при } x < 0, \\ f(x) = x \text{ при } x \geq 0; \end{cases} \quad (1)$$

где a – малая константа (~0,01).

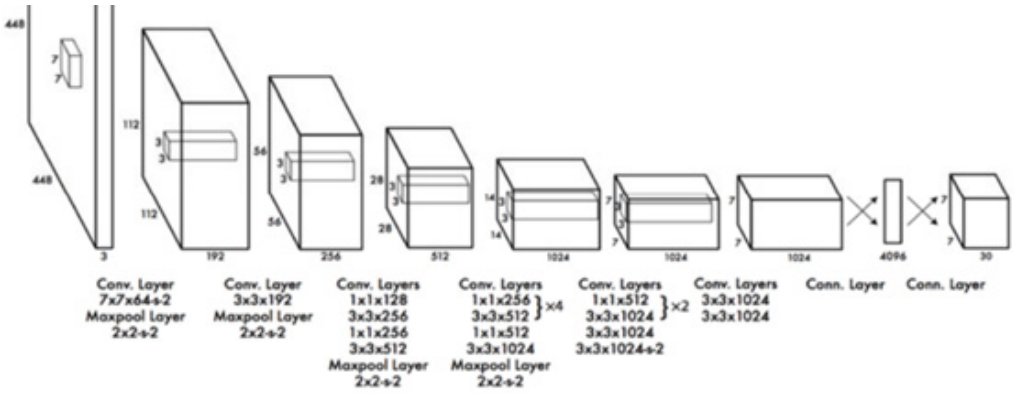


Рис. 1. Архитектура YOLOv1

На вход сверточной нейронной сети подаётся трёхканальное изображение размером 448x448. После прохождения 20 сверточных слоёв исходный тензор, содержащий полученные карты признаков, имеет размерность 14x14x1024. К нему применяется ряд слоев с LRelu, после чего размерность тензора становится7x7x30, и к нему применяется процедура детектирования [1].

Фактически, на исходное изображение наносится сетка размером 7x7 (рис. 2).

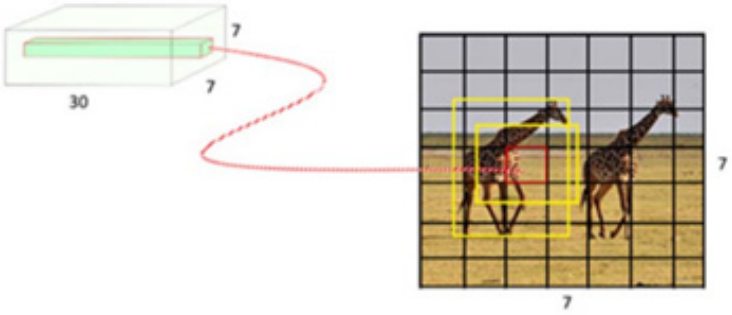


Рис. 2. Вектор из тензора 7x7x30, соответствующий выделенной ячейке

YOLO v3.

YOLOv3 выполняет обнаружение в трех разных масштабах, которые задаются путем понижающей дискретизации размеров входного изображения на 32, 16 и 8 соответственно. В YOLO v3 обнаружение производится путем применения 1x1 ядер обнаружения на картах признаков трех разных размеров в трех разных уровнях сети.

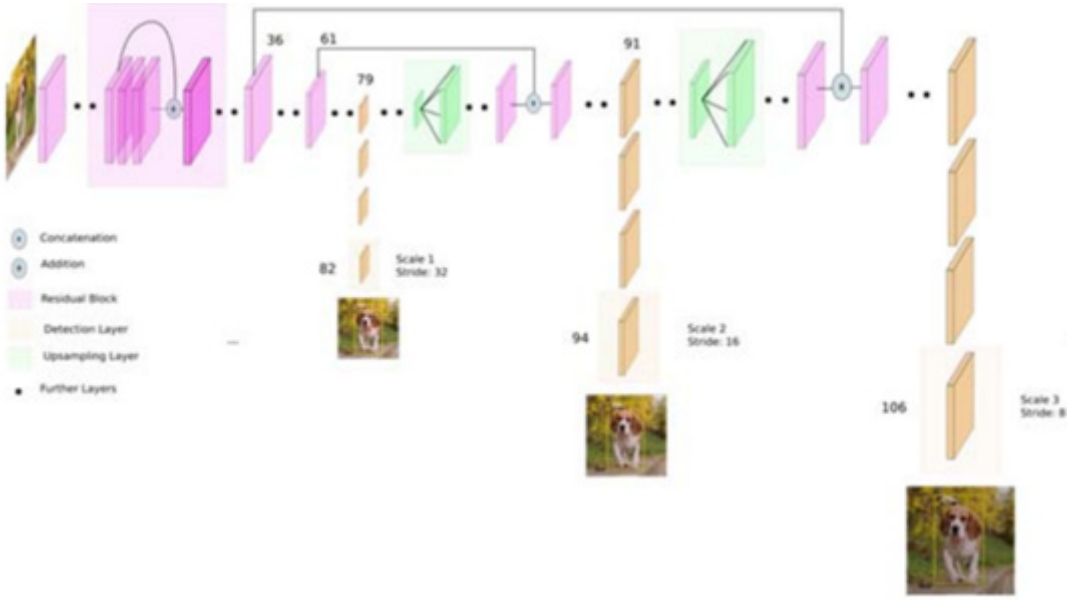


Рис. 3. Архитектура YOLOv3

Размер ядра/фильтра обнаружения равен 1x1x(B x (5 + C)). Здесь B-количество «bounding box», которое может предсказать ячейка, число 5 включает в себя 4 – атрибута «bounding box» и вероятность правильного определения объекта, а C – количество классов [8]. Например, в YOLO v3, обученной на базе данных «coco», B = 3 и C = 80, и поэтому размер ядра равен 1 x 1 x 255.

Для первых 81 слоев разрешение изображения уменьшается сетью, так что 81–й уровень имеет шаг 32. Под шагом сети понимается коэффициент, который показывает, во сколько раз выходное изображение слоя меньше входного изображения в сеть. Поэтому для исходного изображения с разрешением 416x416, результирующая карта признаков будет иметь размер 13x13. Первое обнаружение производится на 82-м слое с использованием фильтра 1x1, что дает тензор 13x13x255.

На следующем этапе сеть вновь обращается к карте признаков из 79-го слоя, пропуская ее через несколько сверточных слоев и повышая дискретизацию в два раза, так что размер карты становится 26x26. Для того, чтобы учесть признаки более раннего слоя, полученная карта объединяется с картой признаков из слоя 61 и результат объединения вновь подвергается нескольким сверточным слоям 1x1, после чего на 94–м слое выполняется второе обнаружение, которое выдает тензор 26 x 26 x 255.

Аналогичная процедура повторяется для 91-го слоя, объединение которого уже совершается с картой признаков из слоя 36. На 106–м слое происходит финальное детектирование с результирующим тензором размером 52 x 52 x 255.

Каждая ячейка может прогнозировать 3 «bounding box», используя 3 «anchor box». Поскольку имеется три масштаба, количество «anchor box» составляет 10647 :13x13x3+26x26x3+52x52x3 = 10647.

Результаты исследования и их обсуждение

В данной исследовательской работе использован алгоритм YOLO для обнаружения и детектирования объектов в изображениях с помощью глубокого обучения, а также OpenCV и Python. Применяя данные алгоритмы, можно определить, не только то. что находится на изображении, но и где находится данный объект. В структуру проекта входят катаог изображений и 1 скрипт Python. Папка изображений содержит три статических изображения, на которых выполня-

ется обнаружение объектов для целей тестирования и оценки.

Далее произведен анализ четырех аргументов командной строки. Аргументы командной строки обрабатываются во время выполнения и позволяют нам изменять входные данные для нашего сценария из терминала.

Аргументы командной строки включают в себя:

- Изображения (путь к входному изображению);
- YOLO (базовый путь к каталогу YOLO);
- Точность (минимальная вероятность фильтрации слабых обнаружений, значение по умолчанию 50%);
- Порог (порог подавления без максимумов со значением по умолчанию: 0.3).

Точность при обучении отдельных классов изображений составила от 70% до 95%.

YOLO способен правильно обнаружить каждый класс танка на изображении. На рисунке 4 представлен инерфейс терминала и процесс обработки файла. Результат обработки показан на рисунке 5. Необходимо отметить, что на рисунке 5 все три танка обнаруживаются, несмотря на то, что в некоторых местах область изображения сильно затемнена. На рисунке 5 приведен результат распознавания трех танков T-90M.

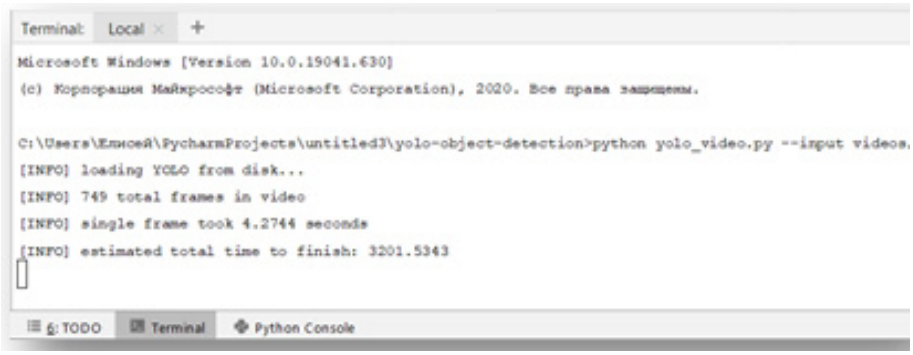


Рис. 4. Обнаружение детектором YOLO танка «Abrams»

Следующий пример изображения демонстрирует ограничения и недостатки детектора объектов YOLO: на рисунке 6 представлен пример обнаружения не всех танков на изображении. Не все машины, расположенные на изображении близко друг от друга идентифицируются, однако распознавание произошло с точностью в 84% (рис. 4).

Рис. 5. Обнаружение детектором YOLO танка «T-90M»

В ходе исследования обнаружены следующие ограничения и недостатки детектора объектов YOLO:

- не всегда хорошо справляется с мелкими предметами;
- не обрабатывает объекты, сгруппированные близко друг к другу.

Причина такого ограничения кроется в самом алгоритме YOLO:

- детектор объектов YOLO разделяет входное изображение на сетку SxS, где каждая ячейка в

сетке предсказывает только один объект;

- если в одной ячейке существует несколько небольших объектов, то YOLO не сможет их обнаружить, что в конечном итоге приведет к фиксации пропущенных объектов.

Рис. 6. Обнаружение детектором YOLO танка «Abrams»

В целом точность обнаружения моделей танков при тестировании различных типов составила от 64% до 92%.

Выводы

По результатам шести проведённых экспериментов по изменению архитектуры сети. установлено, что если обучающий набор данных состоит из многих небольших объектов, сгруппированных близко друг к другу, то не эффективно использовать детектор объектов YOLO. С точки зрения идентификации небольших объектов, R-CNN, как правило, работает лучше аналогов, однако, он отличается малым быстродействием. В оперативной обстановке можно применять алгоритм распознавания только с БПЛА, поскольку объекты, распознаваемые с высоты не будут наслаиваться друг на друга. Компьютерные эксперименты, проведенные с обучающими наборами данных, позволили доказать эффективность алгоритма YOLO и добиться достаточно высоких результатов в распознавании типовых образцов вооружения и военной техники.

Литература

1. *М.А. Абумуталлапулы, Л.Б. Алтынбекова,* «Искусственные нейронные сети в военной сфере». 2020 URL: https://moluch.ru/archive/309/69627/

2. *Воротников С. А.* - Информационные технологии в робототехние. 2014. 319 с.

3. *R. Singh,* “Computer Vision — An Introduction”, Towardsdatascience. 2019. URL: https://towardsdatascience.com/computer-vision-an-introduction-bbc81743a2f7.

4. A. Mort, How “Computer Vision Applications are Changing the World”. 2019 URL: https://techsee.me/blog/computer-vision-applications/

5. *A.Donovan*, “What Is Deep Learning and Why Is It More Relevant Than Ever?”, Interestingengineering. 2019. URL: https://interestingengineering.com/what-is-deep-learning-and-why-is-it-more-relevant-than-ever.

6. *Redmon J.*, «YOLO: Real–Time Object Detection». 2018. URL: http://pjreddie.com/darknet/yolo/

USE OF RECOGNITION SYSTEMS FOR WEAPONS AND MILITARY EQUIPMENT

Elisey V. Bauer,
Graduate MTUCI, Moscow, Russia,
Lilia I. Voronova,

Head of the Department of IC&AS, Doctor of physical and mathematical Sciences, Professor, MTUCI, Moscow, Russia,
voronova.lilia@yandex.ru

Abstract
The rapid development of information technologies in the leading countries of the world has inevitably led to a re-thinking of the concepts of using recognition systems, ways to further develop them, improve the payload and give them a multi-purpose character. Recognition systems based on UAVs occupy a worthy place in the production programs of military air reconnaissance systems. The use of UAVs for military purposes has become one of the important areas of development of modern aviation and allows you to automate the management of troops, reduce the loss of personnel in combat due to operational intelligence about the current situation. In this regard, the task of creating mobile, easy-to-use and cheap means of conducting aerial reconnaissance is urgent. The basis for real-time object recognition is the YOLO algorithm proposed by Joseph Redmon, which is a single neural network applied to the entire image at once.

Keywords: *UAVs, YOLO, machine learning, artificial intelligence, recognition system, armored vehicles, data analysis, algorithm, model, aviation automated command and control.*

АНАЛИЗ СИСТЕМ МОНИТОРИНГА АВТОТРАНСПОРТА

Арсеньева Диана Горановна,
магистрант МТУСИ, Москва, Россия,
ars.dian@yandex.ru

Маликова Елена Егоровна,
доцент кафедры ССиСК, к.т.н., МТУСИ, Москва, Россия,
emalikova@gmail.com

Аннотация

В настоящее время для мониторинга автотранспорта, а также для повышения безопасности дорожного движения, используются интеллектуальные системы мониторинга. В работе приводится описание различных систем мониторинга автотранспорта, отмечены особенности аппаратных и программных частей этих систем. Рассмотрен метод анализа иерархий, позволяющий пользователям определить критерии, которыми должна обладать система мониторинга. Приведены результаты сравнительного анализа, с использованием метода анализа иерархий, основанном на функциях системы мониторинга автотранспорта, позволившие определить приоритетные системы мониторинга для компаний городской курьерской доставки.

Ключевые слова: *система мониторинга автотранспорта, метод анализа иерархий, бортовой терминал, датчики, трекер, сети подвижной сотовой связи.*

Введение

В последние годы услуга мониторинга автотранспортных средств обрела большую популярность, что, в свою очередь, привело к увеличению количества операторов связи. Цель данной работы заключается в изучении рынка услуг мониторинга автотранспорта и выявлении базовых функций, которыми должна обладать система мониторинга автотранспорта, а также в анализе систем мониторинга на основе приоритетов потребителей услуг.

Описание системы мониторинг автотранспорта

Система мониторинга транспорта – это комплекс аппаратных и программных средств, позволяющий в режиме реального времени осуществлять дистанционное наблюдение за маршрутами передвижения и техническим состояние автотранспорта и подвижных объектов [1,2,6,7].

Аппаратная часть системы мониторинга состоит из бортового терминала и датчиков различного назначения. Бортовой терминал или трекер, является основным элементом системы. С его помощью осуществляется прием и обработка сигналов со спутников ГЛОНАСС/GPS, определение географических координат местоположения, построение маршрута передвижений, определение скорости движения и т.п. Наличия бортового терминала, как аппаратного средства, необходимо для создания простейшей системы мониторинга автотранспорта. Для того чтобы получать дополнительную информацию о техническом состоянии объекта, или осуществлять контроль над водителями транспортного средства, можно оборудовать систему дополнительными датчиками. Датчики подключаются к аналоговым и цифровым входам бортового терминала, информация с них сохраняется терминалом и передается совместно с информацией, собранной самим трекером. Существуют датчики общего назначения, например, для контроля расхода топлива, давления масла, количества открываний дверей и т.п., а также датчики, специфичного характера, например - для отслеживания количества оборотов емкости автобетоносмесителя.

Вся информация, собранная бортовым терминалом, по каналам сотовой связи GSM и других стандартов сетей подвижной связи передается на сервер системы мониторинга (рис. 1).

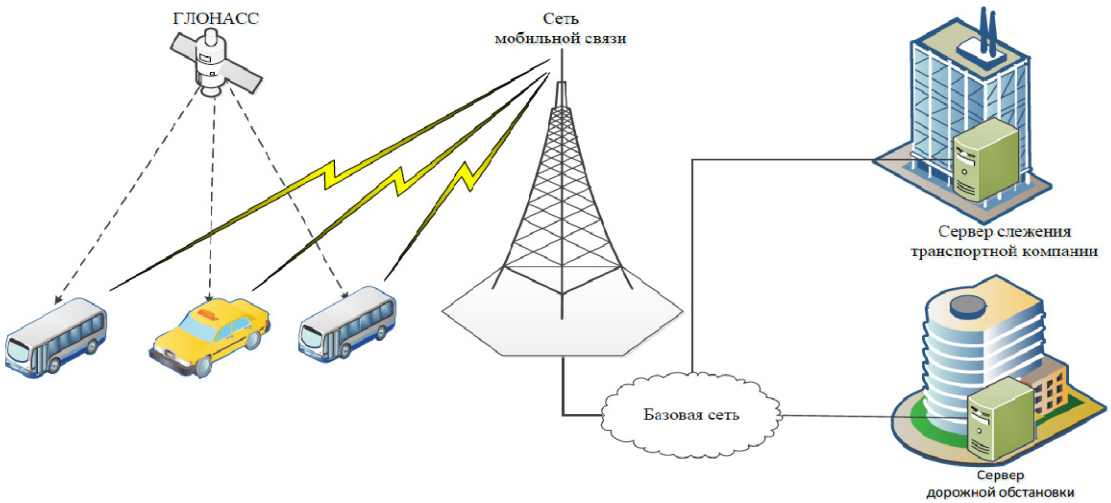


Рис. 1. Система мониторинга автотранспортных средств

На сервере установлено программное обеспечение, предназначенное для сбора, обработки и хранения данных с трекера. Обработанная и наглядная информация с сервера передается на автоматизированные рабочие места (АРМ) диспетчеров, или на устройства пользователей со специальным установленным приложением, в зависимости от того, как организована доставка оператором информации до пользователя услуги связи [3].

Описание метода анализа иерархий

Системы мониторинга транспорта разных операторов имеют одинаковый принцип работы, но могут отличаться, в зависимости от количества установленных датчиков, получаемой информацией от потребителей услуг монитортнга. Использование дополнительных датчиков увеличивает затраты потребителей услуг связи на организацию системы. В случае, когда необходимо оснастить большое количество объектов, например, каждый автомобиль таксопарка, потребитель понесет значительные расходы, так как дополнительные датчики увеличат стоимость системы. Если сумма расходов ограничена, то потребителю необходимо определиться, какая информация об объекте будет для него наиболее важной. Для этого может быть использован метод анализа иерархий [4].

Метод анализа иерархий заключается в разделении объемной задачи на подзадачи с дальнейшей оценкой их приоритетности и проведением попарного сравнительного анализа для поиска оптимального варианта решения. Метод используется при условии определенности цели задачи и наличия большого количества критериев.

Алгоритм метода состоит из следующих шагов:

Шаг 1: Формирование иерархии;

Шаг 2: Экспертная оценка приоритетов;

Шаг 3: Расчет локальных векторов приоритета;

Шаг 4: Проверка экспертной оценки (вычисление индекса согласованности);

Шаг 5: Расчет значения глобального приоритета на основе синтеза локальных приоритетов.

Основные принципы метода анализа иерархий:

Принцип декомпозиции – структурирование задачи в виде иерархии. Необходимо, чтобы каждый элемент уровня был связан со всеми элементами последующего уровня. Пример иерархии задачи в общем виде приведен на рисунке 2.

Рис. 2. Иерархия задачи

Принцип сравнительных суждений – альтернативы и критерии сравниваются попарно с позиции их воздействия на общую характеристику. Для этого строится обратно симметричная матрица сравнений $A = \|a_{ij}\|$, где $a_{ii} = w_i / w_j$, w_i – вес i-го элемента иерархии. Для каждой матрицы определяются векторы локальных приоритетов и вычисляются индексы согласованности.

Принцип синтеза приоритетов – формирование набора локальных приоритетов, выражающего влияние множества элементов иерархии на элемент верхнего уровня. Принцип применим, когда построена матрица сравнений для критериев и матрицы сравнения альтернатив для каждого из критериев, а также рассчитаны векторы локальных приоритетов.

Синтез приоритетов происходит путем умножения значения локального приоритета альтернативы на значения локального приоритета соответствующих ему ,критериев и суммирования по каждому из элементов.

Итоговой оценкой, или глобальным приоритетом альтернативы, является вычисленное значение свертки весовых коэффициентов локальных критериев всех уровней иерархии.

Сравнительный анализ систем мониторинга автотранспорта

Для проведения сравнительного анализа систем мониторинга автотранспорта были выбраны 10 операторов, предоставляющих данную услугу, и выделены 16 функций систем, на которых будет основан анализ. Данные функции были описаны на официальных сайтах операторов услуг связи. Стоит заметить, что все системы мониторинга автотранспорта соответствуют требованиям приказа Минтранса РФ от 31.07.2012 №285 [5].

Список выбранных систем мониторинга автотранспорта приведен ниже. Для удобства присвоим им следующие номера:

1. ANTOR;
2. Position Report;
3. СКАУТ-Платформа;
4. AutoSCAN;
5. 1С: Центр спутникового мониторинга;
6. Автолокатор;
7. ST matix;
8. Wialon Hosring;
9. Omnicomm;
10. Monitor-3S.

В табл. 1 приведены наименования функций и отмечено, у каких систем мониторинга они присутствуют. Также по таблице можно определить количество функций у каждой системы и какие функции встречаются наиболее часто.

Таблица 1

Функции мониторинга автотранспорта

Номер системы мониторинга / Функции систем мониторинга	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	**Итого**
1. Отображение транспорта в реальном масштабе времени	+	+	+	+	+	+	+	+	+	+	**10**
2. Автоматический мониторинг транспортных средств	+		+	+	+	+	+	+	+	+	**9**
3. Маршрутизация транспорта	+	+	+		+		+	+	+	+	**8**
4. Интерактивный топливный график	+	+	+	+	+		+	+	+	+	**9**
5. Возможность построения мнемосхем управления										+	**1**
6. План-фактный анализ	+	+	+	+	+	+	+	+	+	+	**10**
7. Отчет по движению	+	+	+	+	+	+	+	+	+	+	**10**
8. Отчеты расхода топлива	+	+	+	+	+	+	+	+	+	+	**10**
9. Статистика по водителю				+							**1**
10. Противоугонный сервис				+		+				+	**3**
11. Реализация технического процесса отложенной передачи мониторинговой информации в условиях полного отсутствия сотовой связи						+			+		**2**
12. Интеграция с программой 1С	+	+	+	+	+	+	+	+	+	+	**10**
13. Интеграция с тахографами			+	+			+				**3**
14. Контроль соблюдения фактических норм работы автотранспорта									+	+	**2**
15. Возможность использование спутниковых каналов связи										+	**1**
16. Возможность использования резервного SMS-канала										+	**1**
Итого	**8**	**7**	**9**	**10**	**8**	**8**	**9**	**9**	**10**	**13**	

Основываясь на данных содержащихся в табл. 1, используем метод анализа иерархий. Определим, какая из десяти выбранных нами систем мониторинга автотранспорта наилучшим образом подойдет под требования компании, занимающейся курьерской доставкой малогабаритных товаров по Москве в пределах МКАД. Для доставки используется легковые автомобили. Системы мониторинга имеют незначительные различия в цене, поэтому этот критерий мы не учитываем. Также будем считать, что качество услуг служб поддержки всех операторов находится на одном уровне.

Диспетчеры компании должны знать местонахождение автомобилей в текущий момент времени. Водители должны обладать информацией о всех адресах доставки. Желательно, чтобы на карте навигатора были отмечены удобные маршруты. Компания является пользователем системы «1С: Предприятие», в которой ведется вся документация. Чтобы рассчитывать будущие затраты на ресурсы перевозки, желательно, чтобы велся учет расхода топлива. В компании должны работать только высококвалифицированные специалисты, поэтому необходимо иметь информацию о рабочей деятельности водителей.

Структурируем задачу в виде иерархии. Выше сформулирована цель задачи. У нас заданы 16 функций систем и выбрано 10 систем мониторинга автотранспорта. Номера функций и систем в иерархии, соответствующие их порядковым номерам, приведены в таблице 1. Иерархия задачи сравнительного анализа представлена на рисунке 2.

Рис. 2. Иерархия задачи сравнительного анализа

Далее попробуем провести экспертную оценку приоритетов и рассчитать значения локальных приоритетов функций, используя парное сравнение. Для этого построим обратно симметричную матрицу $A = \|a_{ij}\|$, где $a_{ii} = 1$, $a_{ji} = 1/a_{ij}$. Элементом матрицы a_{ij} является интенсивность проявления элемента иерархии i относительно элемента иерархии j. То есть мы, построчно сравниваем функции друг с другом, оцениваемая их приоритеты по шкале относительной важности от 1 до 9, где оценки имеют следующий смысл:

- равная важность – 1;
- умеренное превосходство – 3;
- значительное превосходство – 5;
- сильное превосходство – 7;
- очень сильное превосходство – 9;
- в промежуточных случаях ставятся четные оценки: 2, 4, 6, 8 (например, 4 – между умеренным и значительным превосходством).

При проведении сравнения двух функций мы ставим перед собой вопрос: какая из функций для нас предпочтительнее?

Матрица приведена в таблице 2. Так же мы рассчитаем нормализованный вектор приоритетов (НВП) – вес функции. Для этого нам нужно будет найти сумму каждого столбца матрицы по формуле (1), рассчитать среднее геометрически строк, включая строку сумм столбцов по формуле (2), а затем поочередно разделить среднее геометрической строк на среднее геометрическое значение суммы - формула (3).

$$S_j = \sum_{i=1}^{n} a_{ij} = a_{1j} + a_{2j} \ldots + a_{nj} \quad (1)$$

$$\bar{X}_{геом\ i} = \sqrt[n]{a_{i1} \cdot a_{i2} \cdot \ldots \cdot a_{in}} \quad (2)$$

$$НВП = \frac{\bar{X}_{геом\ i}}{\bar{X}_{геом\ S}} \quad (3)$$

Далее проверим согласованность локальных приоритетов матрицы, рассчитав максимальное собственное значение матрицы λ_{max} по формуле (4), индекс согласования (ИС), используя формулу (5), и отношение согласованности (ОС) по формуле (6). Показатель случайной согласованности (ПСС) – теоретической значение, зависящее от размера матрицы (представлено в табл 3). Отношение согласования не должно превышать 0.1, иначе матрица не является согласованной, то есть в этом случае наша оценка приоритетов будет неверной.

$$\lambda_{\max} = \sum_{i=1}^{n} \sum_{j=1}^{n} S_j \cdot НПВ_i + S_{j+1} \cdot НПВ_{i+1} + \ldots + S_n \cdot НПВ_n \quad (4)$$

$$ИС = \frac{|\lambda_{\max} - n|}{n-1} \quad (5)$$

$$ОС = \frac{ИС}{ПСС} \leq 0,1 \qquad (6)$$

Матрица оценки важности функций

Таблица 2

	$Ф_1$	$Ф_2$	$Ф_3$	$Ф_4$	$Ф_5$	$Ф_6$	$Ф_7$	$Ф_8$	$Ф_9$	$Ф_{10}$	$Ф_{11}$	$Ф_{12}$	$Ф_{13}$	$Ф_{14}$	$Ф_{15}$	$Ф_{16}$	**Ср.геом**	**НВП**
$Ф_1$	1	1	2	3	7	2	3	3	3	5	5	1	5	5	5	7	3,03	**0,132**
$Ф_2$	1	1	2	3	7	2	3	3	3	5	5	1	5	5	5	7	3,03	**0,132**
$Ф_3$	0,5	0,5	1	2	7	1	2	2	2	5	5	0,5	5	5	5	7	2,20	**0,096**
$Ф_4$	0,33	0,33	0,5	1	7	1	1	1	2	5	5	0,33	5	5	5	7	1,71	**0,074**
$Ф_5$	0,143	0,143	0,143	0,143	1	0,2	0,2	0,2	0,3	0,5	0,5	0,143	1	0,5	0,5	1	0,31	**0,014**
$Ф_6$	0,5	0,5	1	1	5	1	1	1	1	3	3	0,5	5	5	5	7	1,70	**0,074**
$Ф_7$	0,33	0,33	0,5	1	5	1	1	1	1	3	3	0,3	5	5	5	7	1,50	**0,065**
$Ф_8$	0,33	0,33	0,5	1	5	1	1	1	1	3	3	0,3	5	5	5	5	1,47	**0,064**
$Ф_9$	0,33	0,33	0,5	0,5	3	1	1	1	1	3	3	0,3	5	5	5	5	1,36	**0,059**
$Ф_{10}$	0,2	0,2	0,2	0,2	2	0,3	0,3	0,3	0,3	1	2	0,2	5	5	5	5	0,73	**0,032**
$Ф_{11}$	0,2	0,2	0,2	0,2	2	0,3	0,3	0,3	0,3	0,5	1	0,2	2	1	1	3	0,50	**0,022**
$Ф_{12}$	1	1	2	3	7	2	3	3	3	5	5	1	5	5	5	7	3,03	**0,132**
$Ф_{13}$	0,2	0,2	0,2	0,2	1	0,2	0,2	0,2	0,2	0,5	0,5	0,2	1	0,5	0,5	3	0,34	**0,015**
$Ф_{14}$	0,2	0,2	0,2	0,2	2	0,2	0,2	0,2	0,2	0,2	1	0,2	2	1	2	3	0,45	**0,019**
$Ф_{15}$	0,2	0,2	0,2	0,2	2	0,2	0,2	0,2	0,2	0,2	1	0,2	2	0,5	1	2	0,40	**0,017**
$Ф_{16}$	0,143	0,143	0,143	0,143	1	0,143	0,143	0,2	0,2	0,3	0,3	0,143	0,3	0,3	0,2	1	0,23	**0,010**
Сумма	6,606	6,606	11,286	16,786	64	13,543	17,543	17,6	18,7	39,8	43,3	6,516	58,3	53,8	55,2	77	**23,01**	**1,000**

Далее проведем экспертную оценку, и рассчитает приоритетность функций в рамках систем.

При проведении сравнения двух систем мы ставим перед собой вопрос: какая из систем с этой функцией для нас предпочтительнее? У нас нет иных данных, кроме как наличие или отсутствие функции в системах. Поэтому, при сравнении системы будут иметь равный приоритет важности относительно друг друга, то есть оценка – 1. Метод анализа иерархий не подразумевает оценку 0 при проведении сравнения приоритетов, поэтому система, у которой функция отсутствует, не может сравниваться с той, у которой она есть и оценка не может быть произведена. В этом случае, локальный приоритет системы не будет учитываться в дальнейшем расчёте.

В таблице 4 приведена матрица оценки важности систем в общем виде. В ходе вычислений были получены значения средних геометрических, суммы каждой системы, рассчитан нормализованный вектор приоритетов (НВП) – вес системы при наличии функции. Также была проведена проверка согласованности локальных приоритетов матрицы. Из табл. 4 видно, что все системы обладают одинаковым значением НВП равном 0,1.

После того, как все значение получены, приступим к расчетам глобальных приоритетов (ГП). Для этого построим матрицу с полученными значениям весов функций и весов систем. Соотнесем функции и системы, обратившись к табл. 1. Если у системы отсутствует критерий, то ставим "–". Рассчитаем ГП для каждой системы, умножая каждое значение веса системы на соответствующее значение веса функции, и суммируя их по каждому элементу строки. Наиболее высоким рейтингом будет обладать система с наибольшим значением глобального приоритета. Расчеты приведены в таблице 5.

$$\lambda_{\max} = 16,029 \quad ИС = 0,02 \quad ОС = 0,001216$$

Значения случайной согласованности

Таблица 3

Размер матрицы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Случайная согласованность	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,53	1,56	1,57	1,59	1,6

Матрица оценки важности систем в общем виде

Таблица 4

Фп	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	**Среднее геометрич.**	**НВП**
C_1	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_2	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_3	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_4	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_5	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_6	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_7	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_8	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_9	1	1	1	1	1	1	1	1	1	1	1	**0,1**
C_{10}	1	1	1	1	1	1	1	1	1	1	1	**0,1**
Сумма	10	10	10	10	10	10	10	10	10	10	**10**	**1**

$$\lambda_{\max} = 10 \quad ИС = 0 \quad ОС = 0$$

Расчет глобальных приоритетов

Таблица 5

	$Ф_1$	$Ф_2$	$Ф_3$	$Ф_4$	$Ф_5$	$Ф_6$	$Ф_7$	$Ф_8$	$Ф_9$	$Ф_{10}$	$Ф_{11}$	$Ф_{12}$	$Ф_{13}$	$Ф_{14}$	$Ф_{15}$	$Ф_{16}$	**ГП**
	0,132	0,132	0,096	0,074	0,014	0,074	0,065	0,064	0,059	0,032	0,022	0,132	0,015	0,019	0,017	0,01	
C_1	0,1	0,1	0,1	0,1	–	0,1	0,1	0,1	–	–	–	0,1	–	–	–	–	0,077
C_2	0,1	–	0,1	0,1	–	0,1	0,1	0,1	–	–	–	0,1	–	–	–	–	0,064
C_3	0,1	0,1	0,1	0,1	–	0,1	0,1	0,1	–	–	–	0,1	0,1	–	–	–	0,078
C_4	0,1	0,1	–	–	–	0,1	0,1	0,1	0,1	0,1	–	0,1	0,1	–	–	–	0,071
C_5	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	–	–	–	0,1	–	–	–	–	0,078
C_6	0,1	0,1	0,1	0,1	–	0,1	0,1	0,1	–	0,1	–	0,1	–	–	–	–	**0,080**
C_7	0,1	0,1	–	0,1	–	0,1	0,1	0,1	–	–	0,1	0,1	0,1	–	–	–	0,071
C_8	0,1	0,1	0,1	0,1	–	0,1	0,1	0,1	–	–	–	0,1	–	–	–	–	0,077
C_9	0,1	0,1	0,1	0,1	–	0,1	0,1	0,1	–	–	0,1	0,1	–	0,1	–	–	**0,081**
C_{10}	0,1	0,1	0,1	0,1	–	0,1	0,1	0,1	–	0,1	–	0,1	–	0,1	0,1	0,1	**0,085**

Выводы

Проведя сравнительный анализ и используя метод анализа иерархий, удалось выяснить, что под требования компании, занимающейся курьерской доставкой малогабаритных товаров по Москве в пределах МКАД, подойдут следующие системы мониторинга автотранспорта: C_{10} – Omnicomm, C_9 – Monitor-3S, C_6 – Автолокатор,

Наличие большего числа функций не всегда делает систему мониторинга более приоритетной для пользователя услуги. Система C_4 – AutoSCAN обладает десятью функциями, но имеет один из самых низких приоритетов, так как эти функции не являются важными для описанного пользователя услуг. Система C_6 – Автолокатор обладает всего восемью функциями, но по их приоритетности опережает многие системы, или не уступает тем, кто лидирует по числу функций.

Стоит отметить, что в приведенном расчете по методу анализа иерархий не были взяты в расчет такие важные критерии как, например, стоимость системы мониторинга автотранспорта или аппаратного комплекса. Нельзя с уверенностью утверждать, что выбранные нами системы будут наилучшим вариантом для всех пользователей, подходящих под наше описание. Для них нужно будет сделать дополнительный расчет с учетом и других факторов.

В дальнейшем планируется провести дополнительный детальный анализ трех отмеченных систем мониторинга автотранспорта.

Литература

1. *Тихвинский В.О., Коваль В.А., Бочечка Г.С., Бабин А.И.,* Сети IoT/M2M: технологии, архитектура и приложения. М.: Медиа Паблишер. 2017. 319 с.
2. *Гольдштейн Б.Г.* Инфокоммуникационные сети и системы, СПб.: БХВ-Петербург, 2019. 208 с.
3. M2M системы удаленного управления и мониторинга. Законченные решения на базе резервируемых GSM / GPRS терминалов. [Электронный ресурс]. Источник: https://wireless-e.ru/gsm/m2m-analitik-ts/.
4. *Саати Т.* Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. 278 с.
5. Приказ Минтранса РФ от 31 июля 2012 г. N 285 "Об утверждении требований к средствам навигации, функционирующим с использованием навигационных сигналов системы ГЛОНАСС или ГЛОНАСС/GPS и предназначенным для обязательного оснащения транспортных средств категории M, используемых для коммерческих перевозок пассажиров, и категории N, используемых для перевозки опасных грузов".
6. *Степанов С.Н., Степанов М.С., Маликова Е.Е., Цогбадрах А., Ндайикунда Ж.* Построение и анализ обобщенной модели разделения ресурса для LTE технологий с функциональностью NB-IOT // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 12. С. 71-77.
7. *Антонова В.М., Маликова Е.Е.* Исследование эффективности совместной передачи разнородного трафика в соте сети LTE // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 22-25.

ANALYSIS OF TRANSPORT MONITORING SYSTEMS

Diana G. Arsenyeva,
Graduate MTUCI, Moscow, Russia,
ars.dian@yandex.ru

Elena E. Malikova,
Associate Professor of Department of NC&SC, PhD., MTUCI, Moscow, Russia,
emalikova@gmail.com

Abstract

Currently, intelligent monitoring systems are used to monitor vehicles, as well as to improve road safety. The paper describes various systems for monitoring vehicles, notes the features of the hardware and software parts of these systems. A method for analyzing hierarchies is considered, which allows users to determine the criteria that a monitoring system should have. The results of a comparative analysis using the hierarchy analysis method based on the functions of the vehicle monitoring system, during which the priority monitoring systems for urban courier delivery companies were identified.

Keywords: *transport monitoring system, vehicle monitoring system, hierarchy analysis method, on-board terminal, sensors, tracker, mobile cellular network.*

ИСПОЛЬЗОВАНИЕ МЕТОДА CRAMM ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ

Волкова Любовь Васильевна,
магистрант МТУСИ, Москва, Россия,
lvv.14@mail.ru

Макарова Дарья Викторовна,
магистрант МТУСИ, Москва, Россия,
d4riya.makarova@yandex.ru

Докучаев Владимир Анатольевич,
профессор, заведующий кафедрой СИТиС, д.т.н., МТУСИ, Москва, Россия,
v.a.dokuchaev@mtuci.ru

Аннотация

В статье рассматривается возможность применения метода CRAMM для управления информационными рисками в организациях. Актуальность данной проблемы вызвана всё увеличивающимися случаями утечки конфиденциальной информации в организациях различных видов собственности. В материале приведены основные этапы по оценке рисков при использовании метода CRAMM, показаны сложности формализации результатов анализа, в частности при оценке потенциальных рисков при создании и эксплуатации программно-конфигурируемых сетей центров обработки данных.

В материале приводятся особенности метода CRAMM, рассматриваются его преимущества и недостатки. Показано, что данный метод может быть использован при анализе различных бизнес и (или) технологических процессов, требующих оценки рисков и выбора контрмер. Процесс управления информационными рисками позволяет значительно повысить эффективность и рациональность всех бизнес и (или) технологических процессов в организации, и незаменим при выработке политики информационной безопасности и обеспечении непрерывности ведения бизнеса.

Ключевые слова: *риск, управление рисками, защита информации, информационная безопасность, CRAMM, информационные системы, уязвимости, методы управления рисками.*

Введение

В настоящее время информация является одним из наиболее ценных активов во всех сферах экономической, политической и социальной деятельности человека, и с каждым годом её ценность только возрастает. Одновременно информационные системы и технологии становятся неотъемлемой частью практически любой стороны нашей жизни. Зависимость от информационных систем и технологий означает, что организации становятся более уязвимыми по отношению к разного рода угрозам и, следовательно, информация, подобно любым другим активам организации, нуждается в защите [1, 10-13].

Защита информационных активов обретает всю большую актуальность, так как с каждым годом увеличиваются угрозы. На рисунке 1 приведена статистика одной из наиболее часто встречающихся проблем информационной безопасности – утечка информации. По результатам исследования аналитического центра компании InfoWatch [2], в России к концу 2019 года было зарегистрировано 370 случаев утечки конфиденциальных данных из компаний различных сфер деятельности, как государственного, так и частного типа, что на 45%больше, чем в предыдущем году.

Приведенная статистика отображает лишь зарегистрированные случаи утечки информации. Если бы удавалось обнаруживать и отслеживать все случаи, то число зарегистрированных утечек информации возросло бы в два или даже три раза. Также следует учитывать, что кроме утечки информации существуют и другие виды угроз информационной безопасности: несанкционированный доступ, потеря данных, кибератака, мошенничество и т.п.

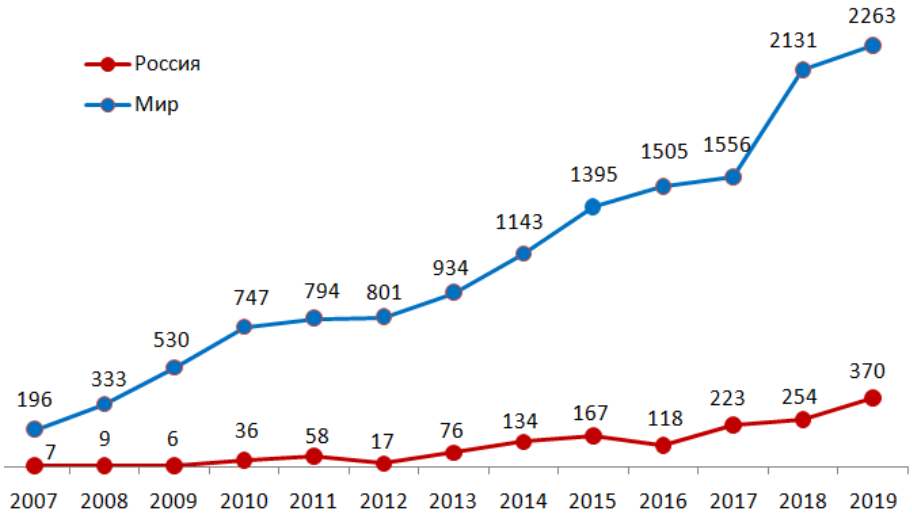


Рис. 1. Число зафиксированных утечек информации за 2007-2019 гг.

С каждым годом увеличивается использование информационных технологий для автоматизации многих бизнес и технологических процессов: огромное количество информации и данных хранится в электронном виде, а также обрабатывается и передаётся с помощью информационных систем и информационно-телекоммуникационных сетей. От отказоустойчивости и защищенности этих систем напрямую зависит надежность и целостность данных. Таким образом, с развитием информационных систем и технологий также развиваются и увеличиваются информационные угрозы и риски и, следовательно, требуется уделять особое внимание созданию и применению в организациях систем обеспечения информационной безопасности и защиты информации [3]. При этом, особое внимание следует уделять умению определять, оценивать и управлять рисками, возникающими в информационных системах и информационно-телекоммуникационных сетях, обеспечивающих их взаимодействие (в частности, в программно-конфигурируемых сетях центров обработки данных, и устанавливаемым в них, информационным системам по работе с персональными данными) [4-7].

Управление информационными рисками в организациях

Управление рисками – это совокупность действий, направленных на уменьшение и устранение неблагоприятных последствий, связанных с уязвимостями системы или организации в целом [8].От выбора методов расчета рисков и подхода организации к защите информации зависит эффективность применяемой в организации политики информационной безопасности. Управление рисками в информационных системах в первую очередь предполагает выявление рисков, а затем определение мер для предотвращения или минимизации ущербов.

ИТ-риски можно условно разделить на две группы: риски, связанные с отказоустойчивостью системы, т.е. технические сбои работы программно-аппаратного обеспечения, каналов передачи, которые приводят к потере (повреждению) данных или к убыткам; риски, вызванные утечкой информации и использованием её конкурентами или сотрудниками в целях причинения вреда компании.

Принимая во внимание бизнес-среду организации и доступные ресурсы, лица, принимающие решения, могут реализовать одну или несколько из следующих стратегий управления рисками[9]:

- снижение рисков (снижение рисков с применением выбранных контрмер);
- принятие риска (принятие остаточного риска или даже начального уровня, если контрмеры более дорогостоящие, чем стоимость активов);
- передача риска (передача риска другой организации, например, путем страхования или аутсорсинга).

Величину значения риска можно выразить через такие составляющие как активы, угрозы и уязвимости:

РИСК = АКТИВ x УГРОЗА x УЯЗВИМОСТЬ.

Применение контрмер позволяет ограничивать величину риска. Любая информационная система имеет начальный уровень риска до того, как будут применены какие-либо контрмеры. Контрмеры, полагая, что их значения определяются теми же параметрами, которые используются для оценки угроз, уязвимостей и активов, могут снизить риск. Таким образом, за счет уменьшения угроз (например, запертых дверей, брандмауэров), уменьшения уязвимости (например, осведомленности, исправлений и т.п.) или снижения стоимости активов (например, шифрование), уменьшается значение стоимости риска. После расчета результатов каждой комбинации угрозы, уязвимости, актива и меры противодействия определяется остаточный риск.

Особенности метода CRAMM

В настоящее время существует большое число методов, которые упрощают работы по управлению рисками. Одним из таких методов является метод CRAMM (CCTA Risk Analysisand Management Method) — это метод анализа рисков, разработанный британской правительственной организацией CCTA (Central Communication and Telecommunication Agency) и в настоящее время переименованной в Office of Government Commerce (OGC). В методе предполагается выполнение трех этапов анализа рисков: идентификация, анализ и оценка рисков [8].

В основе метода CRAMMлежит комплексный подход оценки рисков, включающий количественные и качественные методы анализа [4].Основные элементы сбора данных, анализа и вывода результатов, которые должны присутствовать в автоматизированном инструменте анализа рисков, охватываются тремя этапами CRAMM:

- идентификация и оценка активов;
- выявление угроз и уязвимостей, расчет рисков;
- выявление и приоритезация контрмер.

Первый этап предполагает анализ всех ресурсов системы, включающий определение и оценка активов, которые будут исследоваться в дальнейшем. Методология CRAMM использует встречи, интервью и структурированные анкеты для сбора данных. На начальном этапе анализа важна первоначальная встреча с рецензентами (лицами, проводящими обзоры CRAMM, которые должны быть обучены и иметь опыт использования инструмента) и руководством организации для определения целей, объема и границ обзора, сроков реализации проекта, необходимой справочной информации, структуры проекта, графика, а также определение респондентов. Результаты должны быть задокументированы в «Документе об инициировании проекта».

Таким образом, в конце первого этапа оценки рисков методом CRAMM должен быть получен отчёт, в котором указываются цели, ресурсы (оборудование, данные) и границы анализируемой системы. На основе полученной информации делаются выводы о состоянии существующей информационной безопасности системы и определяется требуется ли полный анализ и доработка или достаточно имеющейся политики безопасности.

Второй этап ориентирован на выявление уязвимостей и оценку рисков. На данном этапе также производится группировка активов организации для дальнейшей оценки. Ценность активов для организации играет центральную роль в определении рисков и необходимого уровня защищённости информации. Идентифицируются три типа активов, составляющих информацию: данные, прикладное программное обеспечение и физические активы (например, оборудование, здания, персонал). С помощью метода CRAMM все взаимосвязанные активы, включая услуги конечных пользователей для дифференциации обработки данных (например, электронная почта, интерактивный сеанс, просмотр веб-страниц), могут быть определены в моделях активов, которые могут отражать бизнес и технологические процессы. Моделирование - одна из наиболее важных проблем при использовании инструмента, поскольку слишком мелкая детализация может излишне затянуть процесс проверки, а слишком грубая может упустить важные активы, что приведет к неверным результатам.

Оценка информационных активов зависит от того, кто (например, конфиденциальная информация в руках конкурента) и когда (например, пароли с истекшим сроком действия) владеет ими. При использовании метода CRAMM рецензент проводит интервью с «владельцами данных» (например, менеджерами бизнес и (или) технологических подразделений) для оценки активов данных, что повышает уровень принятия решений. Эта часть оценки является наиболее сложной, поскольку иногда бывает трудно идентифицировать владельцев данных (или бизнес и (или) технологических процессов), или респондентам могут потребоваться некоторые рекомендации для оценок, которые так-

же можно рассматривать как процесс осведомленности.

Аналогично вышеизложенному производится оценка и в автоматизированной системе CRAMM:

1. Производится группировка ресурсов с точки зрения угроз и уязвимостей. Например, инженерные системы ЦОДов можно декомпозировать на такие составляющие как электроснабжение, кондиционирование, безопасность хранения данных, системы передачи данных (в частности, программно-конфигурируемую сеть передачи данных между подсистемами ЦОД), система резервирования данных. Также следует уделить внимание диспетчеризации системы ЦОД, так как стабильный и качественный мониторинг позволит избежать многих проблем [10]. Кроме того, необходимо рассматривать ресурсы по их местоположению в случае угрозы пожара или кражи (серверный зал, комната средств связи, диспетчерская и т.п.);
2. Выполняется оценка вероятности угроз и уязвимостей. Для оценки угроз, в основном, используются косвенные факторы, к примеру, в информационных системах, в частности в программно-конфигурируемых системах ЦОДов, особое внимание уделяется политическим факторам обеспечения безопасности, а именно существующим стандартам обеспечения защиты данных и безопасности систем: Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ», ГОСТ
3. Р ИСО/МЭК 27018-2020 «Информационные технологии. Методы и средства обеспечения безопасности»; Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки» и т.п. Для каждой группы ресурсов, определённых на начальном этапе, программным обеспечением CRAMM генерируется список вопросов, которые предполагают однозначный ответ. В последующем, эти вопросы будут использоваться для оценки рисков;
4. После определения вероятностей возникновения угроз и уязвимостей проводится анализ рисков качественным и количественным методами [4]. В зависимости от ответов на сгенерированные вопросы для каждой определённой угрозы выявляется её уровень: очень высокий, высокий, средний, низкий, очень низкий. На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7 [9];
5. Вывод полученных результатов – система выдаёт отчёты по полученным данным оценки рисков.

Прикладное программное обеспечение и физические активы с точки зрения затрат на их замену или реконструкцию легче оценить, опросив «вспомогательный персонал» (например, ИТ-менеджеров, сотрудников служб технической поддержки и т.п.). Результаты опроса переводятся в значения шкалы от 1 до 10. Если программное обеспечение имеет свои собственные внутренние требования к конфиденциальности или целостности (например, исходный код программного обеспечения, созданного на заказ), оно оценивается так же, как и актив данных [8].

Помимо стоимости активов, двумя другими ключевыми компонентами анализа риска по методу CRAMM являются уровни (вероятность возникновения) угрозы и уязвимости. Угрозы и уязвимости исследуются в отношении выбранных групп активов, которые собираются вместе, чтобы оставаться в разумных временных рамках. В CRAMM есть предварительно определенные таблицы для комбинаций угроз/активов и угроз/воздействий. Исчерпывающая оценка каждой угрозы для каждой группы активов не имеет смысла и неосуществима. Поэтому проверяющий выбирает все возможные подходящие угрозы и активы в соответствии с потребностями клиента. Следует отметить, что относительно уязвимостей метод CRAMM ориентирован на оценку рисков на уровне управления, поэтому подробные технические уязвимости системы, которые могут быть идентифицированы сканерами уязвимостей, не устраняются.

Отметим, что есть два способа оценки угроз и уязвимостей: «полная» и «быстрая» оценки рисков. При полной оценке рисков, что рекомендуется в большинстве случаев, угрозы и уязвимости идентифицируются путем задания вопросов из структурированных анкет обслуживающему персоналу (например, системным или сетевым администраторам, специалистам по информационной безопасности и т.п.) и ввода ответов в инструмент.

Хорошо подготовленный и опытный специалист может использовать быструю оценку риска. При такой оценке уровни угрозы и уязвимости вводятся непосредственно в систему с рейтингом (например, «очень низкая» угроза для инцидента, «ожидаемая в среднем не более один раз в 10 лет», или «средняя» уязвимость для инцидента, «происходящего с вероятностью реализации наихудшего сценария от 33 до 66%»).

Третий этап предполагает предложение различных вариантов защиты. Когда проверка CRAMM завершена, программное обеспечение CRAMM содержит полную базу данных проверяемой системы или сети, которую можно использовать для управления конфигурацией и аудита. На этой стадии CRAMM генерирует большое число вариантов контрмер [8]. Предложенные рекомендации и меры защиты требуют еще более тщательного изучения и отбора, в чем, наверное, заключается самая сложная часть работы с результатами вывода данных программного обеспечения. Отчет об управлении рисками (например, отчет об анализе) также можно экспортировать в текстовый редактор Microsoft Word, что позволяет редактировать и форматировать результаты в зависимости от размера организации. Отметим, что при этом отсутствует возможность встраивать собственные шаблоны в автоматизированный инструмент. В программно-конфигурируемых сетях (ПКС) необходимо единожды определить политики, применяемые к оборудованию и интерфейсу, а впоследствии заниматься только их применением и поддержкой. В этом случае метод CRAMM удобно использовать при начальном внедрении, так как метод поможет определить «слабые» места в исследуемой системе и основные принципы построения политики информационной безопасности. Кроме того, концепция программно-конфигурируемых сетей не является еще широко распространенной и поэтому в базе данных CRAMM на данный момент времени не существует параметров, связанных конкретно с программно-конфигурируемыми сетями, а возможности вносить правки специалистом не предусмотрено. В связи с этим требуется высокая квалификация специалиста как для работы с системой анализа рисков, так и понимающего принципы работы и поддержки ПКС. От специалиста требуется четкое понимание различий традиционных сетей от ПКС, а также умение оценивать уровень наносимого ущерба при реализации риска. В таблице 1 представлены основные достоинства и недостатки применения метода CRAMM применительно к анализу потенциальных рисков, возникающих в программно-конфигурируемых сетях ЦОДов.

Таблиц 1

Достоинства и недостатки метода

Достоинства	**Недостатки**
Обширная база данных для оценки рисков программно-конфигурируемых сетей центров обработки данных	Требуется высокая квалификация специалиста
Структурированный подход к анализу и управлению рисками, основанный на хорошо отработанных методах	Нет возможности создания шаблонов
Регулярное обновление базы данных контрмер и оценки рисков	Большой объем отчетов
Возможность применения на начальном этапе настройки программно-конфигурируемых сетей	Высокая трудоемкость
Не требует много ресурсов, кроме ПК под управлением Windows и лицензионного ключа для ПО	ПО недоступно для свободного скачивания

Система может сообщать о результатах, которые должны быть представлены руководству для согласования и утверждения, чтобы перейти к этапу управления рисками. На этом этапе обзорное совещание с руководством должно быть сосредоточено на основных выводах, таких как области с высокой степенью угрозы/уязвимости, которые следует предварительно проанализировать на предмет несоответствий, например, с помощью средства «обратного отслеживания» инструмента на основе ошибок оценки или ввода, что также способствует их осознанию.

Заключение

Для выполнения надлежащей оценки защищённости информации в информационных системах (подсистемах), в последние годы были разработаны различные методы, методологии и инструменты, одним из которых является метод CRAMM. Данный метод основан на стандартах управления информационной безопасностью и описывает корреляцию между уязвимыми ИТ-активами и угрозами, которые могут повлиять на ИТ-активы организации через эти уязвимости.

Управление ИТ-рисками должно происходить в соответствии со спецификой предприятия, в частности при создании и эксплуатации программно-конфигурируемой сети ЦОД. Основным достоинством рассмотренного метода CRAMM в данном случае является то, что метод можно применять при начальной конфигурации ПКС и с его помощью определить изначальные параметры для

системы защиты информации, что значительно упрощает работу по минимизации потенциальных рисков. Следует отметить, что программное обеспечение, реализованное на основе метода CRAMM, является универсальным и может быть использовано для анализа информационных рисков в организациях различных видов собственности и различных размеров. Однако, оценка рисков в более крупных компаниях выполняется значительно дольше (даже с помощью программного обеспечения) в связи с тем, что требуется анализировать большее число активов компании. Это является существенным недостатком метода, так как информационные технологии развиваются с экспоненциальной скоростью, так же, как и возникающие новые угрозы и уязвимости, и, следовательно, необходимо регулярно обновлять и корректировать исходные данные для определения информационных рисков системы.

Литература

1. *V. A. Dokuchaev,* "Digital Transformation: New Drivers and New Risks," 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/EMCTECH49634.2020.9261544.Отчёт компании InfoWatch.[Электронный ресурс]. - Режим доступа: https://www.infowatch.ru/analytics/reports, свободный – (07.12.2020).
2. *Докучаев В.А., Шведов А.В.* Классификация показателей надёжности корпоративных цифровых платформ. В сборнике: Актуальные проблемы и перспективы развития экономики, труды XIX Всероссийской с международным участием научно-практической конференции. Симферополь, 2020. С. 28-29.
3. *V. A. Dokuchaev, V. V. Maklachkova, D. V. Makarova and L. V. Volkova,* "Analysis of Data Risk Management Methods for Personal Data Information Systems," 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2020, pp. 1-5, doi: 10.1109/IEEECONF48371.2020.9078547.
4. *V. A. Dokuchaev, V. V. Maklachkova, V. Yu. Statyev,* "Risks identification in the exploitation of a geographically distributed cloud infrastructure for storing personal data," 2020 International conference «Engineering management of communication and technology» (EMCTECH) IEEE Conference Record #49634, Vienna, Austria (Springer Schloessl).
5. *Dokuchaev V.A., Maklachkova V.V., Statev V.Yu*. Classification of personal data security threats in information systems // T-Comm. 2020. Т. 14. № 1. С. 56-60.
6. *Маклачкова В.В., Мытенков С.С., Сидорова О.А.* Классификация угроз информации по уровням типовой корпоративной инфокоммуникационной системы. В сборнике: Технологии информационного общества, Материалы XIII Международной отраслевой научно-технической конференции. 2019. С. 433-435.
7. ISO 31000:2018. Riskmanagement – Guidelines [Электронныйресурс]. - Режимдоступа: https://www.iso.org/standard/65694.html, свободный – (16.03.2019).
8. *Баранова С.Ю.* Методики анализа и оценки рисков информационной безопасности, Вестник Московского университета им. С.Ю. Витте. Серия 3. Образовательные ресурсы и технологии, 2015. № 1(9). С. 73-79.
9. *Докучаев В.А., Кальфа А.А., Маклачкова В.В.* Архитектура центров обработки данных / Под ред. профессора В. А. Докучаева. М.: Горячая линия – Телеком, 2020. 240 с. ISBN 978-5-9912-0849-9.
10. *Pavlov S.V., Dokuchaev V.A., Maklachkova V.V., Mytenkov S.S.* Features of supporting decision making in modern enterprise infocommunication systems // T-Comm. 2019. Т. 13. № 3. С. 71-74.
11. *Pavlov S.V., Dokuchaev V.A., Mytenkov S.S.* Model of a fuzzy dynamic decision support system // T-Comm. 2020. Т. 14. № 9. С. 43-47.
12. *Докучаев В.А., Маклачкова В.В., Статьев В.Ю.* Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 6. С. 27-32.
13. *Макарова Д.В., Докучаев В.А.* Основные методы сбора и защиты биометрических персональных данных // REDS: Телекоммуникационные устройства и системы. 2019. Т. 9. № 1. С. 7-12.

THE CRAMM METHOD USING TO ASSESS INFORMATION RISKS

Liubov V. Volkova
Graduate MTUCI, Moscow, Russia,
lvv.14@mail.ru

Darya V. Makarova
Graduate MTUCI, Moscow, Russia,
d4riya.makarova@yandex.ru

Vladimir A. Dokuchaev
Head of Department NIT&S, DSc Tech., Professor, MTUCI, Moscow, Russia,
v.a.dokuchaev@mtuci.ru

Abstract

The article discusses the possibility of using the CRAMM method for information risk management in organizations. The urgency of this problem is caused by the ever-increasing cases of leakage of confidential information in organizations of various types of property. The material presents the main stages of risk assessment when using the CRAMM method, shows the complexity of formalizing the analysis results, in particular, when assessing potential risks in the creation and operation of software-defined networks of data centers. The material describes the features of the CRAMM method, considers its advantages and disadvantages. It is shown that this method can be used in the analysis of various business and (or) technological processes requiring risk assessment and selection of countermeasures. The information risk management process can significantly increase the efficiency and rationality of all business and (or) technological processes in an organization and is indispensable in developing an information security policy and ensuring business continuity.

Keywords*: information security, risk, risk management, risk management methods, CRAMM.*

РАЗРАБОТКА МАКЕТА УМНОЙ ТЕПЛИЦЫ

Савин Вадим Евгеньевич,
студент МТУСИ, Москва, Россия,
vadsavin@mail.ru

Покутняя Людмила Святославовна,
студент МТУСИ, Москва, Россия,
poctnyaya@yandex.ru

Харламова Ирина Сергеевна,
студент МТУСИ, Москва, Россия,
kharlam905@mail.ru

Вовик Андрей Геннадьевич,
ассистент каф. ИСУиА, МТУСИ, Москва, Россия,
andreyvovik@gmail.com

Аннотация

В статье описывается процесс проектирования и реализация умной теплицы с возможностью дистанционного мониторинга и управления на базе микроконтроллера Arduino. Показания с датчиков умной теплицы отправляются на MQTT сервер по технологии беспроводной связи на основе стандарта IEEE 802.11. Разработаны алгоритмы для обмена данными между сервером, Arduino и другими устройствами в сети Интернет, а также алгоритм автоматического полива растений с возможностью удалённого контроля влажности почвы и других параметров. Разработан протокол для управления подписками ESP на MQTT сервере по последовательному соединению.

Ключевые слова*: IoT, ESP8266, Arduino, умная теплица, автоматический полив, удаленный контроль.*

«Умный город – это созданная человеком система умных вещей, связанных технологиями IoT – Интернета вещей. Каждая вещь, так или иначе, должна иметь выход в общую сеть для сбора данных и гибкого управления. Это позволит эффективно использовать городские ресурсы и сделать жизнь его жителей более комфортной [1].

Однако «умными» становятся не только города, но и сельское хозяйство. Современные тенденции таковы, что людям приходится эффективно использовать имеющиеся у них ресурсы, в том числе землю. Для этого важно получать максимум результатов, вкладывая минимум средств. Именно эту задачу позволяет решить «умное сельское хозяйство», используя датчики, которые собирают и отправляют на сервер информацию о влажности, температуре и, возможно даже о химическом составе почвы. Благодаря этой информации можно оптимизировать полив и обработку посевов. Автоматизированные комбайны могут работать круглосуточно и строить наиболее эффективные маршруты движения, чтобы минимизировать затраты. Но кроме промышленного сельского хозяйства есть еще и простые теплицы, которые так же можно автоматизировать. В «умной теплице» можно упростить или вовсе полностью автоматизирован полив, а также автоматически контролировать микроклимат, освещение и собирать статистику параметров для анализа её эффективности [2].

Существующие готовые проекты «умной теплицы» являются дорогостоящими из-за относительно высокой стоимости комплектующих. Также готовые решения могут быть не совместимы с имеющимся типовым оборудованием автоматики. Например, актуаторы или сервоприводы могут не подходить к конкретной теплице, капельный полив может обеспечивать недостаточный проток жидкости и т.д.

Разработанный макет должен соответствовать следующим функциональным требованиям: производить настройку и отладку других, построенных на его принципеах автоматических систем; быть гибким и масштабируемым и обеспечивать возможность подключения к сети Интернет по WiFi. В соответствие с функциональными требованиями к «умной теплице» необходимо подобрать совместимые друг с другом устройства, протоколы, сервисы. Также крайне необходимо реализовать программную часть, чтобы при смене устройств система продолжала устойчиво работать с минимальными изменениями в коде программы [1,2].

Выбранные устройства:

1. ESP8266.

Контроллеры серии ESP выделяются на фоне своих аналогов. Любой из них имеет как минимум два ядра, оно из которых всегда задействовано для WiFi соединения. Целое выделенное ядро позволяет ему быстро отвечать на запросы, обслуживать сразу несколько клиентов и поддерживать несколько протоколов. Данный модуль может работать в режиме CLAP (Client – Access Point), что обеспечивает возможность одновременно организовать WiFi- сеть, полностью управляя ее трафиком, и быть подключенным к другой сети. Благодаря этому режиму работы появляется возможность оперативного создания WIFI MESH сети [3].

2. Arduino UNO.

Это одна из самых распространённых платформ для создания различных макетов, стендов, реализации проектов и т.д. На платах этой серии используются контроллеры Atmega, которые отличаются своей дешевизной, универсальностью и простотой в использовании.

3. Датчики влажности почвы и температуры воздуха

Так как к этим элементам не предъявлялись какие-то особенные требования, было решено взять типовые доступные устройства: электролитический гигрометр и датчики влажности и температуры воздуха DH11. Недостатки гигрометра заключаются в том, что он со временем портится, так как он измеряет сопротивление почвы, пропуская через нее ток и его контакты окисляются. В надёжных системах его нужно заменить на ёмкостной датчик, который измеряет не сопротивление почвы, а ее емкость. Но основе значений емкости также можно сделать выводы о наличии влаги в почве. Модуль DH11 является цифровым датчиком, который взаимодействует с контроллером по протоколу OneWire, позволяя измерить температуру и влажность воздуха.

Принцип работы макета заключается в следующем: Arduino собирает данные со всех датчиков и отправляет их в особом формате по последовательному соединению в контроллер ESP8266, который, будучи подключенным к сети Wi-Fi и к MQTT серверу, декодирует полученную информацию от Arduino, преобразует её в другой формат и отправляет пакеты в соответствующий топик на MQTT сервере. Эти сообщения становятся доступными всем пользователям, которые подключены к серверу. Также и другие пользователи имеют возможность отправлять информационные пакеты в любые топики, если их ESP подписан на эти топики, и в дальнейшем, прочитав эти сообщения, - перенаправить их в особом формате в Arduino [3].

Протокол MQTT (Message Queue Telemetry Transport) – это протокол для общения сервера-брокера с клиентами. Он работает поверх протокола TCP/IP и ориентирован на работу с малыми сообщениями и небольшой нагрузки на сеть в условиях нестабильного соединения. Клиенты могут подписываться на определенные топики на сервере с возможностью читать и присылать туда сообщения. Простота и надежность этого протокола обеспечила ему широкое распространение в среде IoT. Один из способов реализации этого протокола предполагает подтверждение получения сообщения, что определяет его надёжность. Фактически это означает, что сообщения не просто посылаются отправителю, а еще и требуется подтверждения от сервера их получения и также отправки сообщения о том, что отправитель получил данное подтверждение. На рисунке 1 показан принцип работы MQTT сервисов [3, 4].

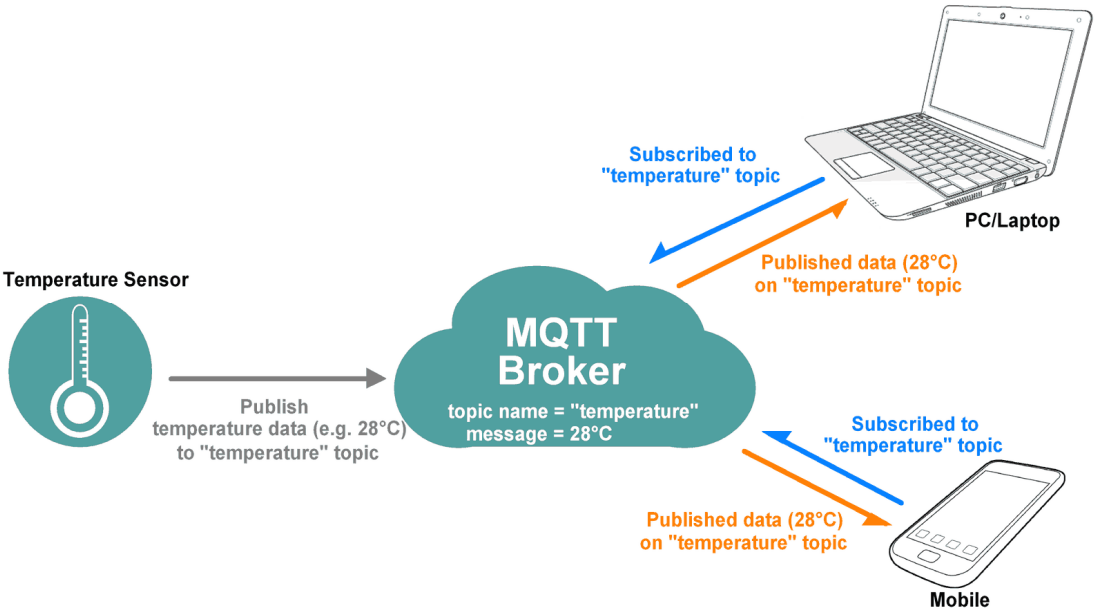


Рис. 1. Обобщённая схема работы MQTT сервисов

В схеме в качестве сервера-брокера был выбран уже готовый облачный сервис CloudMQTT. Он предоставляет бесплатный план со значительными ограничениями. Однако, не смотря на это, его возможностей, хватает с запасом для исключения каких либо проблем для пользователей. Просмотр данных возможен с помощью любого приложения, в название которого, так или иначе, фигурирует название MQTT, так как независимо от платформы, они все взаимодействуют с MQTT серверами.

При подключении к сети WiFi контроллер ESP8266 пытается авторизоваться на сервере CloudMQTT для того, чтобы сервер имел данные о клиенте и мог корректно обрабатывать сообщения, получаемые и адресованные ему. По определенной команде, полученной по последовательному соединению, ESP может подписаться на топик, указанный в команде. Далее, если в этот топик придет сообщение, то ESP получит его и продублирует в последовательное соединение названия топика и в сообщение из него. Таим образом, ESP выступает лишь посредником между сервером и контроллером. Основные функции контроллера возложены на плату Arduino, именно она «заведует» умной теплицей. Сначала она производит сбор данных с датчиков, нормализует их и приводит к необходимому формату данных. Далее, используя специальный протокол, отправляет их по последовательному соединению в ESP, с указанием топиков, в которые необходимо переслать соответствующие сообщения. Также плата Arduino, на основе информации с датчиков принимает решение о необходимости полива растений в теплице. Если влажность почвы недостаточная, на один из пинов подаётся сигнал высокого уровня.

Схема макета является весьма гибкой, так как позволяет проверять разные системы по отдельности: сеть, последовательное соединение контроллеров, работу с датчиками и исполняющимися устройствами и т.п. Все эти элементы связаны между собой только программой-скетчем, на которую можно влиять избирательно, изменяя параметры системы и схемы взаимодействия ее компонентов. Это обеспечивает возможности для быстрого масштабирования, удобной отладки и легкой замены компонентов макета.

На рисунке 2 представлена функциональная схема системы. Особенность такого строения системы заключается в том, что несколько устройств могут взаимодействовать друг с другом через независимый сервер. Например, можно связать несколько теплиц вместе, управляя поливом во всех них нажиманием одной кнопку в телефоне, при этом находясь где-нибудь в метро. При этом, что MQTT сервер может управляться любыми подключёнными к нему устройствами: стационарным компьютером, смартфоном, контроллером, или даже с другого сервера. Особенность работы протокола MQTT заключается в том, что он использует веб-сокет, благодаря чему обеспечивается высокая скорость доставки сообщений, что позволяет для решения более сложных задач использовать ESP отдельно с другими контроллерами. При этом модели ESP8266 - ESP32, обладающее гораздо более впечатляющими характеристиками в серии ESP, обеспечивают даже анализ потокового видео. На рисунке 3 приведена монтажная схема системы «умная теплица».

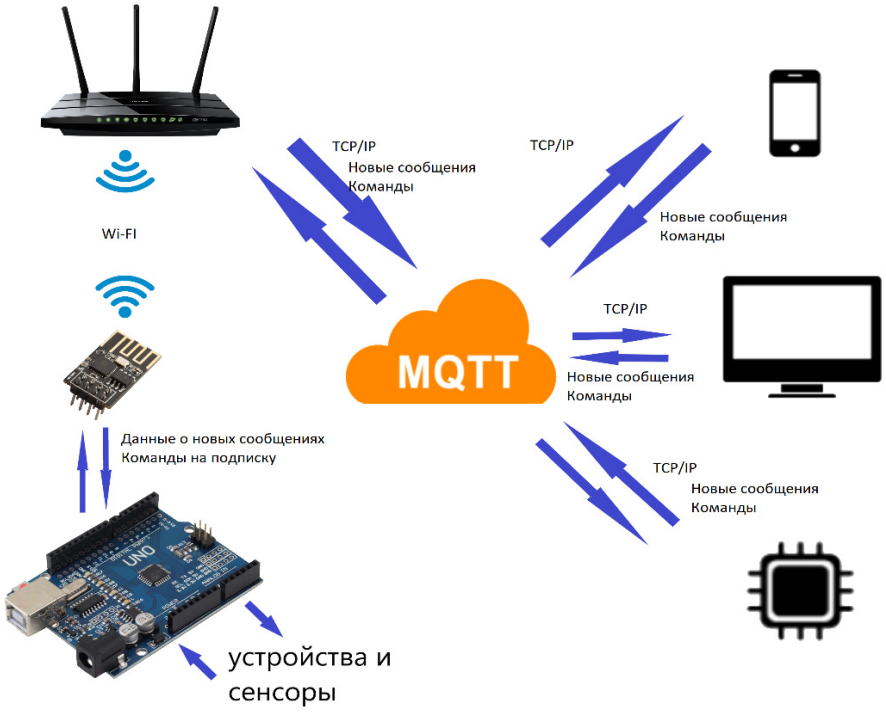


Рис. 2. Функциональная схема системы

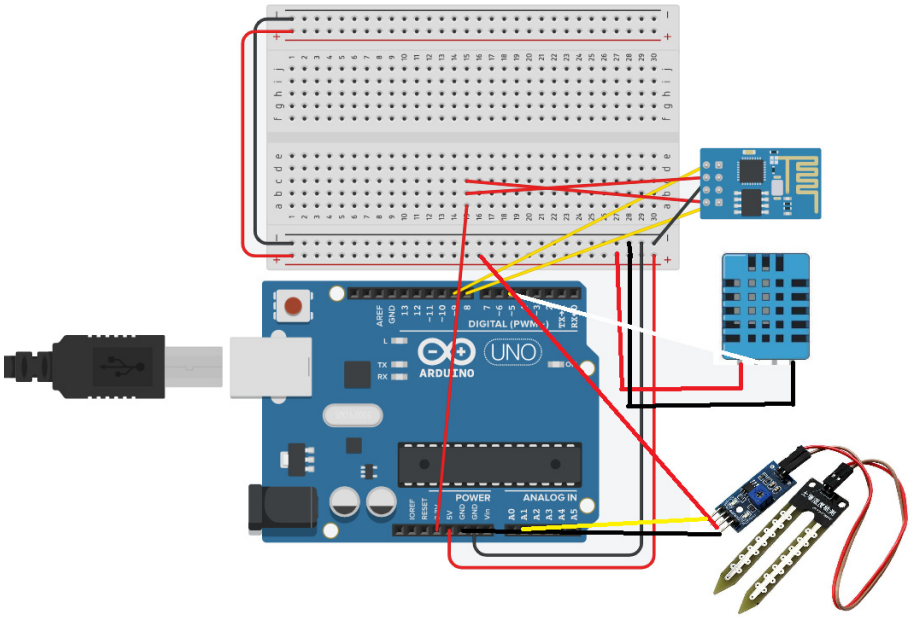


Рис. 3. Монтажная схема системы «умная теплица»

Алгоритм работы для ESP.

При включении он запускает последовательное соединение на скорости 9600 и далее подключается к сети WiFi и MQTT серверу и ожидает сообщения от Arduino или сервера для перенаправления их, соответственно, на сервер или Arduino.

Формат, используемый для взаимодействия с Arduino достаточно прост: [topic] [message]. Без квадратных скобок пишется имя топика для сообщения и само сообщение через пробел. Строка оканчивается символом переноса строки ‘\n’.

Arduino работает следующим образом: в начале запускает программное последовательное соединение (Software serial) и ждет подключения ESP. подключится. Далее выставляются режимы работы для необходимых пинов и производится подписка на соответствующие топики посредствам команды

sub [topic], отправляемой ESP, в цикле принимает сообщения от ESP и выполняет соответствующие команды. Далее собирает информацию с датчиков и отправляет ее в соответствующем формате в ESP.

На рисунках 4 и 5 представлены фотография рабочей системы «умная теплица» и скриншот из приложения на мобильном устройстве, принимающем данные непосредственно с сервера, на который они попадают через Интернет из ESP.

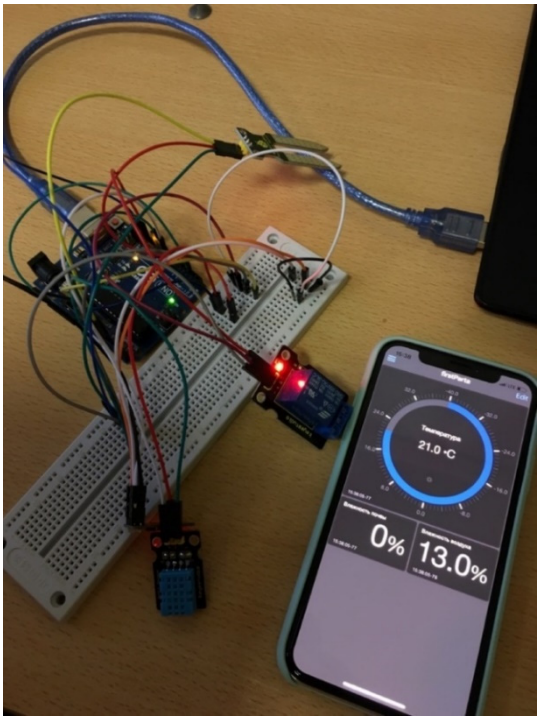


Рис. 4. Собранная схема

Также стоит обратить внимание на то, что интерфейс приложения на скриншоте отличается от того, который виден на фотографии, так как были использованы разные устройства, что демонстрирует гибкость спроектированной системы .

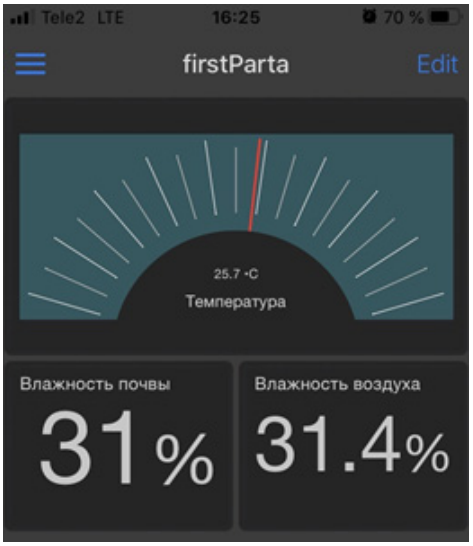


Рис. 5. Скриншот из приложения

Литература

1. Умные города [Электронный ресурс] // URL: https://center2m.ru/smart-city-about (дата обращения 09.01.2020).
2. Умные теплицы [электронный ресурс] // URL: https://www.cfo-russia.ru/issledovaniya/index.php?article=43926 (дата обращения 09.01.2020).
3. Протокол MQTT [электронный ресурс] // URL: https://www.google.ru/url?sa=i&url=https%3A%2F%2Ffirtec.com.ar%2Fcms%2Fcomponent%2Fcontent%2Farticle%2F10-notas-tecnicas%2F53-que-es-mqtt&psig=AOvVaw33m5QKVzuyV2OLZ69Rf3hr&ust=1607026126917000&source=images&cd=vfe&ved=0CAMQjB1qFwoTCPDu2v6MsO0CFQAAAAAdAAAAABAD (дата обращения 09.01.2020)
4. Что такое MQTT и для чего он нужен в IIoT? Описание протокола MQTT [электронный ресурс] // URL: https://ipc2u.ru/articles/prostye-resheniya/chto-takoe-mqtt/ (дата обращения 09.01.2020)

DEVELOPMENT OF THE SMART GREENHOUSE LAYOUT

Savin Vadim Evgenevich,
Student MTUCI, Moscow, Russia,
vadsavin@mail.ru

Pokutnyaya Ludmila Svyatoslavovna,
Student MTUCI, Moscow, Russia,
poctnyaya@yandex.ru

Kharlamova Irina Sergeevna,
Student MTUCI, Moscow, Russia,
kharlam905@mail.ru

Vovik Andrey Gennadievich,
Assistant of the Department of ISU&A, MTUCI, Moscow, Russia,
andreyvovik@gmail.com

Abstract
The article describes the design process and implementation of a smart greenhouse with the possibility of remote monitoring and control based on the Arduino microcontroller. The values from the smart greenhouse sensors are sent to the MQTT server using wireless communication technology based on the IEEE 802.11 standard. Algorithms for data exchange between the server, Arduino and other devices on the Internet have been developed, as well as an automatic watering algorithm with the ability to control soil moisture and other parameters remotely. A protocol has been developed for managing ESP subscriptions on the MQTT server over a serial connection.

Keywords: *IoT, ESP8266, Arduino, Internet of Things, smart greenhouse, automatic irrigation, remote control.*

ОБЗОР ПРОТОКОЛОВ СВЯЗИ ДЛЯ «УМНОГО ДОМА»

Федченков Дмитрий Сергеевич,
магистрант МТУСИ, Москва, Россия,
dimafed7@mail.ru

Шевелёв Сергей Владимирович,
доцент кафедры СИТиС, к.т.н., МТУСИ, Москва, Россия,
shevelev-s@yandex.ru

Аннотация
В статье описаны стандарты протоколов связи «Умного дома». Исследование проводилось на основе известных стандартов связи умного дома (таких как 1-Wire, ZigBee, Wi-Fi и т.д.) Также проведено сравнение протоколов по таким параметрам как радиус действия, максимальная скорость передачи данных, сложность установки оборудования и т.д. В результате сравнения выявлена применимость протоколов связи для решения конкретной задачи.

Ключевые слова: *протоколы связи, интернет вещей, проводные протоколы, беспроводные протоколы, автоматизация дома.*

Когда мы говорим об Интернете вещей, на ум приходит огромное количество устройств, подключенных к Интернету [1, 15, 16]. По данным организации Statista к 2025 году количество умных устройств перейдет за 75 миллиардов [2]. Большая доля умных устройств приходится на «умный дом». Под «умным домом и умным устройством» обычно понимается комплекс аппаратных и программных решений, призванных автоматизировать бытовые задачи.

Чтобы устройства «общались» между собой используются протоколы связи. Они постоянно дорабатываются и обновляются. На сегодняшний день разработано множество таких протоколов для «умных устройств». От их выбора зависит удобство и безопасность использования систем. Некоторые протоколы подходят как для частичной автоматизации в домах и жилых помещениях, так и для комплексной в офисах и на предприятиях. В данной статье предполагается рассмотреть некоторые протоколы связи, которые используются в системе «Умного дома».

Как и в традиционных компьютерных сетях, протоколы связи для умного дома делятся на проводные и беспроводные.

Проводные протоколы связи

Для начала рассмотрим проводные протоколы. Основным преимуществом проводных протоколов связи для «Умного дома» является безопасность (так как злоумышленнику обычно нужен физический доступ к сети) и стабильность работы. К недостаткам можно отнести то, что сложные протоколы связи требуют определённых изменений в проводке, а некоторые системы, основанные на проводных протоколах, желательно проектировать вместе с самим зданием. Стоит обратить внимание, что многие протоколы проводной передачи данных разрабатывались еще в прошлом веке. Однако большинство из них используется и по сей день. Рассмотрим 3 проводных протокола.

1-Wire

Самым простым протоколом проводной связи является 1-Wire (в переводе с английского «один провод»). Данный протокол был разработан в конце 90-х годах. 1-Wire представляет собой двунаправленную шину связи для устройств с низкоскоростной передачей данных, в которой данные передаются по цепи питания (для этого используются два провода – один для питания и данных, а второй провод – земля). В редких случаях, питание и данные – это два отдельных провода. Так как протокол 1-Wire работает в полудуплексном режиме, то в шине может быть только одно ведущее устройство.

Наибольшее расстояние передачи данных 1-Wire может составить до 300 метров, но при соблюдении некоторых условий:

- кабель типа «витая пара»;
- топология «общая шина» с единым стволом (IEEE1394).
- применение специального драйвера сети (активная подтяжка с учётом тока в линии);

Чаще всего 1-Wire используют для связи с простыми устройствами — измерителями параметров внешней среды, цифровыми термометрами и пр. Это обусловлено тем, что 1-Wire предназначен для передачи малых объемов информации. Данный протокол можно часто встретить в домофонах и в небольших любительских системах (например, системах полива).

X10

Стандарт X10 был разработан в 1975 году шотландской компанией PicoElectronics для управления домашними электроприборами. Главным отличием стандарта X10 от 1-Wire является то, что он не требует использование специального кабеля, так как для передачи сигнала применяется электропроводка здания (топология сети — общая шина). X10 также может взаимодействовать с датчиками и пультами ДУ. Данная функция осуществима благодаря трансиверам, способным принимать радиосигналы от беспроводных устройств, преобразовывать их в нужный формат и передавать в электрическую сеть.

X10 «общается» бинарными сигналами — бинарный ноль представлен как отсутствие импульса, единичный бит передается в виде трех импульсов с интервалом 3,33 мс (для сети с частотой напряжения 50 Гц), которые соответствуют нулям трех фаз трехфазной электрической сети. Для передачи команды X10 используется одиннадцать циклов (периодов) силового напряжения. Столько требуется, чтобы передать стартовый код вместе с кодом дома, а также кодом команды. Эта последовательность всегда передается дважды непрерывным блоком. Между блоками разных команд нужен перерыв в три цикла силового напряжения.

Основным преимуществом данного протокола является низкая стоимость и простая реализация (в редких случаях пользователям потребуется сделать небольшие изменения в проводке). Однако X10 имеет ряд недостатков: низкая скорость передачи данных, проблема ложного срабатывания, команды передаются последовательно (это мешает организации сложного динамического освещение). Существует несколько проблем, которые решаются с помощью электромеханических фильтров. К таким проблемам относятся несанкционированный доступ к электросети и низкая помехоустойчивость.

Несмотря на все недостатки, данный протокол имел большую популярность в 2умных домах». На сегодняшний день большинство пользователей X10 совмещают данный стандарт с протоколом Insteon (поскольку данный протокол совместим с X10). Insteon имеет смешанную проводную и беспроводную реализации.

KNX

KNX – протокол с большим количеством заложенных в него функций, пользующийся популярностью в Европе. При выборе данного стандарта следует учитывать высокую стоимость оборудования, его установки и настройки. Для передачи данных протокол KNX может использовать различные среды и топологии: шину, электрическую сеть или радиоканал (топологии: шина, звезда и дерево). Часто при реализации KNX необходимо закладывать проводку кабелей на этапе строительства, либо быть готовым вносить изменения в существующую электрическую линию. «Умный дом» на основе KNX предполагает наличие собственного источника питания с центральным контроллером или множеством распределенных сенсоров с исполнительными модулями. Протокол может использоваться для автоматизации крупных зданий, в одну сеть можно объединить до 57600 устройств (максимальное количество устройств при использовании топологии дерево). В таблице 1 приведены сравнительные характеристики проводных протоколов связи «Умного дома», дающие возможность аргументировано оценить возможность использования каждого из протоколов в конкретном случае [3-5].

Таблица 1.

Характеристики проводных протоколов связи «Умного дома»

Характеристики	1-wire	X10	KNX
Скорость передачи данных	Максимальная скорость – 125 кбит/с (режим overdrive) Стандартная скорость – 15,4 кбит/с	Около 100 бит/с (зависит от частоты напряжения сети)	от 1 200 бит/с до 10 МБит/с в зависимости от среды передачи
Топология сети	Общая шина	Общая шина	Линия, звезда и дерево
Зона действия	До 300 метров	Подходит как для малых помещений, так и для помещений площадью более 300 м^2 (при наличии ретрансляторов)	Расстояние ограничивается средой передачи данных
Достоинства	Простая реализация, низкая стоимость, большое расстояние передачи данных, изменяемость конфигурации	Простая реализация, низкая стоимость	Большой заложенный функционал, предусматривает различные варианты топологии сети, децентрализация системы
Недостатки	Чувствителен к помехам, не предназначен для передачи больших данных, полудуплексный протокол (т.е. на шине может быть только один ведущий)	Низкая скорость передачи данных, проблема ложного срабатывания, команды передаются последовательно, помехоустойчивость	Высокая стоимость оборудования, высокая стоимость монтажных работ
Применение	Элементы автоматизации дома	Автоматизация дома, автоматизация больших помещений	Автоматизация офисов, автоматизация жилых помещений

Беспроводные протоколы связи

Беспроводные стандарты гораздо более популярны из-за своей мобильности. Однако у них есть свои нюансы. Один из них – это обеспечение энергоэффективности. Данный критерий влияет на время жизни мобильного устройства. Еще немаловажным критерием является радиус действия беспроводных протоколов связи. У беспроводных протоколов связи имеются недостатки, которые отсутствуют в проводных протоколах, а именно помехоустойчивость и безопасность. Как пример ошибки пользователей «умных домов» – они доверяют систему охраны дома (камеры и уведомления) протоколам беспроводной связи, которые злоумышленники могут достаточно легко заглушить. Существует 2 вида беспроводных протоколов связи: основанные на стандартах IEEE (в данной статье будут представлены Wi-Fi и ZigBee), и не основанные на указанных стандартах (в качестве примера рассматривается протокол Z-Wave).

Wi-Fi (IEEE 802.11)

Как правило, данный стандарт используется для связи смартфона или персонального компьютера с готовой автоматизированной системой или ее компонентами.

Большинство мобильных телефонов и планшетов оснащены Wi-Fi модулем, а значит возможностью отправлять и получать данные с целью управления IoT устройствами. На сегодняшний день многие производителей интернет вещей создают веб интерфейсы и приложения для удобства взаимодействия пользователей со своими девайсами. Так как у большинства пользователей всегда под рукой одно или даже несколько мобильных устройств, протокол Wi-Fi них часто используется как пульт дистанционного управления. Несмотря на свою распространенность, беспроводной протокол связи Wi-Fi не очень подходит для устройств умного дома, так как Wi-Fi устройства потребляют много энергии и дорого стоят.

ZigBee (IEEE 802.15.4)

ZigBee является протоколом прикладной APS области и использует протоколы нижнего уровня (уровня управления доступом к среде MAC и физического уровня – регламентируется IEEE 802.15.4. – стандартом, который определяет физический слой и управление доступом к среде для беспроводных персональных сетей с низким уровнем скорости). ZigBee и IEEE 802.15.4 описывают беспроводные персональные вычислительные сети (WPAN, WirelessPersonalAreaNetwork).

Протокол ZigBee разрабатывался для сетевых устройств, работающих от аккумуляторов. Хотя стандарт ZigBee не имеет высокой скорости передачи данных, пакеты данных доставляются с повышенной безопасностью и гарантией.

ZigBee предусматривает использование топологий точка-точка, звезда и сложной ячеистую mesh топологии при малом энергопотреблении. В качестве преимуществ протокола можно отметить низкое энергопотребление устройств сети и быстрый отклик при mesh-топологии.

К серьёзным недостаткам данного протокола связи можно отнести плохую совместимость устройств друг с другом. Это связано с тем, что в 2006, 2007 и 2012 годах ZigBee обновлялся. При этом авторы новых спецификаций уделили внимание вопросам совместимости, однако практика показывает, что в рамках одной сети лучше не применять устройства разных стандартов. Разработчики данных обновлений провели большую работу по совместимости своего ПО, но как показывает практика, устройства разных стандартов, находящиеся в одной сети, использовать не рекомендуется. Более того, с последними обновлениями появились профили, которые определяют назначение устройств. К ним относятся HealthCare, HomeAutomation, LightLink, TelecomServices и другие. Таким образом, взаимодействие друг с другом устройств, назначенных разными профилями, дается с трудом, а в некоторых случаях совсем невозможно. Но даже совпадение по версии стандарта и профиля не может гарантировать полной совместимости. Это связано с тем, что большое количество компаний занимается производством модулей связи ZigBee и каждый производитель вносит свои оптимизации в работу протокола.

Как правило, на этом проблемы не заканчиваются: для протокола предусмотрено несколько профилей, определяющих назначение устройства. В их числе: Health Care, Home Automation, Light Link, Telecom Services и другие. Если одно из устройств поддерживает определенный профиль, а другое нет, то взаимодействовать друг с другом они не смогут. Благо, гаджеты, предназначенные для автоматизации дома, используют один конкретный профиль — HomeAutomation. Впрочем, даже совпадение по версии стандарта и профилю не гарантирует стопроцентной совместимости, поскольку производством коммуникационных чипов с поддержкой ZigBee занимается множество компаний. Каждая из них интерпретирует спецификации по-своему, а некоторые вендоры вносят определенные оптимизации в работу протокола.

Z-Wave

Z-Wave разработан датской компании Zensys в 1999 году, а в США данный стандарт стал массово использоваться в 2002 году. Z-Wave очень похож на ZigBee, однако он не основывается на стандартах IEEE. Z-Wave поддерживает только ячеистую mesh топологию и имеет ту же проблему с совместимостью устройств, что и ZigBee. Несмотря на это протокол

Z-Wave более распространен в Европе [6], по сравнению с ZigBee, так как разработчики чаще выпускают его обновления, в которых исправляют проблемы совместимости устройств. Протокол Z-Wave имеет открытый исходный код, что позволяет разработчикам программного обеспечения интегрировать Z-Wave в устройства с меньшими ограничениями, чем ZigBee и другие протоколы связи «умного дома». Таким образом, пользователи найдут гораздо большее количество устройств, которые полностью совместимы с Z-Wave.

В таблице 2 приведены сравнительные характеристики беспроводных протоколов связи «Умного дома», позволяющие оценить возможность использования каждого из протоколов в конкретном случае [6-8].

Таблица 2

Характеристики беспроводных протоколов связи «Умного дома»

Характеристики	Wi-Fi (IEEE 802.11)	ZigBee (IEEE 802.15.4)	Z-Wave
Диапазон частот	2,4 и 5 ГГц	2,4 ГГц /915 МГц (США)/ 868 МГц (Европа)	908.4 МГц (США)/ 868.4 МГц (Европа)
Количество каналов	Для 2,4 ГГц – 14 каналов, для 5 ГГц 8 каналов	Для 2,4 ГГц – 16 каналов для 915 МГц – 10 каналов Для 868 МГц – 1 канал	2 канала
Топология сети	Звезда, точка-точка	Звезда, точка-точка, ячеистая (mesh) топология	Ячеистая (mesh) топология
Скорость передачи данных	802.11n до 600 Мбит/с, 802.11ax до 11 Гбит/с	От 20 до 250 Кбит/с (в зависимости от диапазона частот)	От 9,6 до 100 Кбит/с
Зона действия	От 10 до 100 метров	От 10 до 300 метров	До 30 метров
Достоинства	Популярный протокол, высокая скорость передачи данных	Низкоепотребление энергии, быстрая скорость отклика у устройств, ячеистая топология, где отдельные компоненты могут выступать в роли ретранслятора	Низкое потребление энергии, быстрая скорость отклика у устройств, ячеистая топология, где отдельные компоненты могут выступать в роли ретранслятора, открытый исходный код
Недостатки:	Для сложных систем автоматизации Wi-Fi не подходит: модули связи этого стандарта дороги и имеют высокое потребление энергии	Проблемы с совместимостью устройств, Zigbee 3.0 работает в диапазоне 2,4 ГГц, поэтому он может столкнуться с некоторыми проблемами перегрузки Wi-Fсети	Проблемы с совместимостью устройств(однако из-за более простой структуры их меньше, чем у ZigBee)
Применение	Обычно служит как интерфейс для мобильных устройств и компьютеров	Активно применяется в автоматизации дома, работает с протоколами связи Wi-Fi, bluetoth и Insteon	Активно применяется в автоматизации дома, работает с протоколами связи Wi-Fi, bluetooth и Insteon

Insteon

Завершает данный обзор протокол Insteon, разработанный в 2005 году. Insteon представляет собой проприетарную двухдиапазонную сеть (более известную как dual-meshnetwork), которая передаёт сигналы проводным и беспроводным способами. С помощью данного протокола можно объединить линии электропередачи и радиосигналы в одну сеть. Сигналы Insteon проходят гораздо дальше без помех, по сравнению с другими технологиями. Пользователи Insteon могут рассчитывать на значительно более надежную связь, чем может обеспечить любая однополосная сеть.

Основные характеристики Insteon [9,10]:

- В двухдиапазонной сети Insteon сообщения передаются как с помощью беспроводных сигналов, так и по линии электропередачи. Хотя сегодня дома все меньше и меньше зависят от проводных соединений, двойная сетка может очень пригодиться в больших зданиях или при больших помехах. Использование двух с пособов связи означает повышенную надежность. Кроме того, поскольку каждое сообщение повторяется (simulcast) каждым сетевым устройством Insteon в сети, чем больше устройств пользователь добавляет в свою систему, тем более надежной становится сеть.
- Распространенным заблуждением является то, что Insteon сложно установить. Дело обстоит как раз наоборот. Поскольку коммуникация использует существующую линию электропередач вместе с беспроводными сигналами, пользователю не нужно будет беспокоиться об изменениях в проводке при установке устройств Insteon. С уникальным идентификатором на каждом устройстве он автоматически присоединится к сети после включения питания.

- Скорость передачи данных в беспроводной сети Insteon может составлять до 38 кбит/с. Сообщения от устройства к устройству достигают своей цели в обычное время за 0,05 секунды. Это означает, что пользователь не заметит задержек при использовании оборудования, работающего на данном протоколе связи.
- Все устройства Insteon, работающие в сети, действуют как одноранговые. Любое устройство может выступать в качестве контроллера, приемника или ретранслятора. Это дает устройствам возможность отправлять, получать и ретранслировать сообщения, что улучшает способ передачи сигнала по сети. Для экономии времени автономной работы устройства с батарейным питанием не являются частью этой одноранговой маршрутизации
- Уникальный идентификационный код для устройств Insteon защищает пользователя от прослушивания или внешнего управления устройствами. Все сообщения полностью зашифрованы для обеспечения максимальной безопасности.

Заключение

На данный момент не существует универсального протокола связи для устройств «Умного дома», который бы устраивал всех пользователей. Поэтому клиенты должны выбрать систему автоматизации дома на том или ином протоколе связи заранее. Если пользователю не нужна мобильность автоматизации дома и его не смущает стоимость и сложность реализации, то он может использовать проводной протокол KNX. При этом пользователь KNX получает высокую надежность и помехоустойчивость своей системы. Однако большинству пользователей нужна мобильность, поэтому все шире набирают популярность беспроводные протоколы связи. Беспроводные стандарты являются более универсальными и совместимыми, но у их пользователей часто возникают проблемы при попытке «подружить» устройства. Еще более универсальным решением будет соединить проводные и беспроводные решения протоколом Insteon, что обеспечит надежную и гибкую систему. В любом случае, имеется широкий ряд направлений исследований возможных комбинаций протоколов и поиск наиболее оптимальных решений для каждого конкретного случая [11]. Актуальное значение также приобретают вопросы информационной безопасности взаимодействия «умных устройств» и управления ими [12-14].

Литература

1. *Докучаев В.А., Ермалович А.В., Шведов А.В.*Концепция «Интернет Вещей» как основа развития информационно-коммуникационных технологий (ИКТ)[Печатный]-в сборнике: Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XV международной научно-практической конференции. Крымский федеральный университет им. В.И. Вернадского. 2016. С. 298-299.

2. Number-of-connected-devices-worldwide [Электронный ресурс] – https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide (дата обращения: 09.10.2020).

3.Guideto 1-Wirecommunication [Электронный ресурс] https://www.maximintegrated.com/en/design/ technical-documents/tutorials/1/1796.html (дата обращения: 13.09.2020).

4.Развернутое описание протокола X10 [Электронный ресурс] https://marketelectro.ru/content/razvernutoe-opisanie-protokola-x10 (дата обращения: 13.09.2020).

5.KNX Basics; Smart home and building solutions. Global. Secure. Connected.

6. Протокол ZigBee: беспроводные технологии на службе «умного» дома [Электронный ресурс] https://www.ferra.ru/review/smarthome/SmartHome-ZigBee.htm(дата обращения: 27.09.2020).

7. IEEE 33rd International Performance Computing and Communications Conference (IPCCC); ZigBee vs WiFi: Understanding issues and measuring performances of their coexistence.

8. Energies 2015; Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources.

9. SmartHome Protocols: ZigbeevsZ-WavevsInsteonvsX10 vs KNX vs Bluetooth [Электронныйресурс] https://www.safesmartliving.com/smart-home/protocols/(дата обращения: 25.09.2020).

10. InsteonvsZ-Wave [Электронный ресурс] https://www.smarthome.com/blogs/buyers-guides/insteon-vs-z-wave (дата обращения: 27.09.2020).

11. *Докучаев В.А., Мытенков С.В., Шевелёв С.В.* Совершенствованиеподходов к подготовке специалистов в отрасли ИТ и связи [Печатный] - в сборнике: II Научный форум телекоммуникации: теория и технологии ТТТ-2017. Проблемы техники и технологий телекоммуникаций ПТИТТ-2017 материалы XVIII Международной научно-технической конференции. 2017. С. 352-357.

12. *Пономарев А.А., Шевелёв С.В.* Информационная безопасность в сетях Интернета вещей // Вестник связи. № 9. 2019. С. 36-39.

13. *Пономарев А.А., Шевелёв С.В.* Классификация угроз для интернета вещей // Телекоммуникации и информационные технологии. №1. 2019. С.103-108.

14. *Гордеев Д.С., Шевелёв С.В.* Интернет вещей для «умной» городской среды // Вестник связи. №6. 2019. С. 3-7.

15. *Степанов С.Н., Степанов М.С., Маликова Е.Е., Цогбадрах А., Ндайикунда Ж.* Построение и анализ обобщенной модели разделения ресурса для LTE технологий с функциональностью NB-IOT // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 12. С. 71-77.

16. *Першина В.А., Титова Н.Д., Степанов М.С.* Построение автоматизированной системы сбора данных с приборов учета на базе стандарта LORAWAN // REDS: Телекоммуникационные устройства и системы. 2019. Т. 9. № 2. С. 3-9.

OVERVIEW OF COMMUNICATION PROTOCOLS FOR "SMART HOME".

Dmitry S. Fedchenkov,
Graduate MTUCI, Moscow, Russia,
dimafed7@mail.ru

Sergei V. Shevelev,
Associate Professor of Departmen of NITaS , PhD., MTUCI, Moscow, Russia,
shevelev-s@yandex.ru

Abstract

This article describes the standards of communication protocols of the "Smart Home". The study was carried out on the basis of established standards for smart home communication (such as 1-Wire, ZigBee Wi-Fi, etc.). Protocols were also compared in terms of such speed of action, maximum data transfer rate, complexity of equipment installation, etc. As a result of the comparison, the direction of communication protocols in specific tasks will be revealed.

Keywords: *communication protocols, internet of things, wired protocols, wireless protocols, home automation.*

ПРИНЦИПЫ ОРГАНИЗАЦИИ СИСТЕМЫ “УМНЫЙ ДОМ” НА ОСНОВЕ ТЕХНОЛОГИИ ZIGBEE ДЛЯ МАЛОМОБИЛЬНЫХ ГРУПП НАСЕЛЕНИЯ

Поскотин Леонид Сергеевич,
магистрант МТУСИ, Москва, Россия,
svp_vpl@yahoo.com

Тургут Тимур,
магистрант МТУСИ, Москва, Россия,
hinhardian@gmail.com

Шишкин Дмитрий Витальевич,
магистрант МТУСИ, Москва, Россия,
draknem@gmail.com

Степанов Михаил Сергеевич,
доцент кафедры ССиСК, к.т.н., МТУСИ, Москва, Россия,
mihstep@yandex.ru

Аннотация

Статья посвящена разработке системы “Умный дом” для маломобильных групп населения с использованием технологии ZigBee. Заданы основные и дополнительные требования, которые должны учитываться в данной системе. Приведено краткое описание последней версии протокола ZigBee 3.0. Представлены требования к оборудованию: серверу, видеокамерам, элементам сети ZigBee и устройствам измерения показателей здоровья. Даны рекомендации по реализации некоторых основных и опциональных требований к системе “Умный дом’ для пожилого человека.

Ключевые слова*: *Internet of Things, ZigBee, Умный дом, mesh-сети, пожилые люди.

Введение

На сегодняшний день Интернет Вещей перестал быть некой футуристической концепцией, и прочно вошел в нашу повседневную жизнь [10-13]. Автоматизация привычных процессов является одной из главных тенденций в современном телекоммуникационном мире. Новые технологии активно внедряют на опасных производствах, используют в здравоохранении, логистических процессах и т.д. Большую популярность набирают системы “Умный город”, “Умный офис” и “Умный дом”, где самые разнообразные функции, включая безопасность, климат-контроль, управление освещением, осуществляются без непосредственного участия человека. Данные системы относятся к концепции Интернета Вещей. При этом важно понимать, что в этой сфере не может быть единого унифицированного подхода, потому что при реализации каждого подобного проекта нужно учитывать индивидуальные особенности заказчика.

Особенно ярко это выражается в случае, когда система “Умный дом” организуется для нужд представителей маломобильных групп населения, к которым относятся, в частности, инвалиды и пенсионеры. Здесь, при подготовке технического решения нужно учесть большое количество факторов, некоторые из которых могут быть критичными для жизни и здоровья. Далее требуется определить наиболее оптимальную технологию для построения сети, подобрать необходимое оборудование, обеспечить резервирование наиболее важных функций и т.д. Решению перечисленных вопросов и посвящена данная статья. Принципы организации системы “Умный дом” для представителя маломобильной группы населения рассмотрим на следующем примере. Требуется развернуть сеть Интернета Вещей малого радиуса действия для нужд пожилого человека. Предъявляемые к системе требования приведены в таблице 1.

Таблица 1

Общие требования к системе “Умный дом для пожилого человека”

Основные требования	Опциональные требования
Мониторинг движения в квартире	Мониторинг состояния здоровья
Круглосуточные уведомления о протечках в санузле	Климат-контроль квартиры
Автоматизация освещения	Видеонаблюдение
Функция тревожной кнопки	Система “Анти-чужой”

В качестве основной технологии, используемой для построения рассматриваемой системы, использован протокол ZigBee. Выбор пал на эту технологию из-за её низкого энергопотребления и надёжности покрытия за счёт возможности построения многосвязной сети [9].

ZigBee – это протокол WPAN, основанный на стандарте IEEE 802.15.4, и предназначенный для организации коммерческих и жилых сетей Интернета Вещей (Internet of Things, IoT) в условиях ограниченных стоимости, мощности и пространства. Он позволяет создавать управлять ими ячеистые (mesh) сети, обнаруживать новые устройства и обеспечивать безопасность и самовосстановление [1-3].

На территории России ZigBee работает на частотах 2400-2483,5 МГц. Диапазон 2,4 ГГц сильно загружена такими сетями, как WiFi и Bluetooth, однако стандарт Zigbee предусматривает работу в условиях загруженного радиочастотного спектра.

Структура сети ZigBee включает в себя три типа устройств:

- координатор ZigBee (ZC) – центральный элемент, который запускает сеть;
- маршрутизатор ZigBee (ZR) – промежуточный маршрутизатор, осуществляющий транзит данных от других устройств, а также запуск функции приложения;
- оконечное устройство ZigBee (ZED) – устройство, которое обменивается данными только с родительским узлом (координатором или маршрутизатором).

Для организации системы “Умный дом для пожилого человека” был выбран стандарт ZigBee 3.0 который входит в спецификацию ZigBee Pro 2017 (R22).

Маршрутизация и коммутация

Проектируемая система требует стабильного подключения к сети Интернет для резервирования хранения видеозаписей в удалённом центре обработки данных и предоставления удалённого доступа к информации о состоянии здоровья пожилого человека и его имущества. Следовательно, для организации системы “Умный дом” для пожилого человека необходим маршрутизатор, подключенный к сети вышестоящего провайдера с использованием стандартных технологий доступа или мобильных сетей. В последнем случае необходимо обеспечить требуемую скорость передачи данных. Также, маршрутизатор должен предоставлять возможность удалённого подключения из сети Интернет (VPN Server) для осуществления настройки и администрирования, проверки состояния инженерных систем, просмотра видеозаписей и потокового видео с камер видеонаблюдения, а также мониторинга показателей здоровья пожилого человека.

При планировании системы коммутации необходимо соблюсти повышенные требования к ее надежности и отказоустойчивости. Кроме того, должны быть обеспечена достаточная пропускная способность для осуществления видеонаблюдения и функций “Умного дома”. Резервирование электропитания, подача которого осуществляться с использованием технологии PoE, также зависит от правильно организованной системы коммутации.

Базовые сетевые элементы

Схема размещения ZC и ZR показана на рисунке 1. Главной целью ZR является установление соединения с ZC и создание mesh-сети с не более 31 оконечным устройством. Предполагается размещение данных ZR во всех комнатах. Функционал сервера видеонаблюдения, а также хаба и кон-

троллера устройств ZigBee реализуется на одном устройстве. Для реализации программной части подсистемы ZigBee планируется адаптировать открытый исходный код проекта Zigbee2MQTT, который поддерживает интеграцию со всеми распространёнными сервисами домашней автоматизации за счёт использования стандартного протокола MQTT [5].

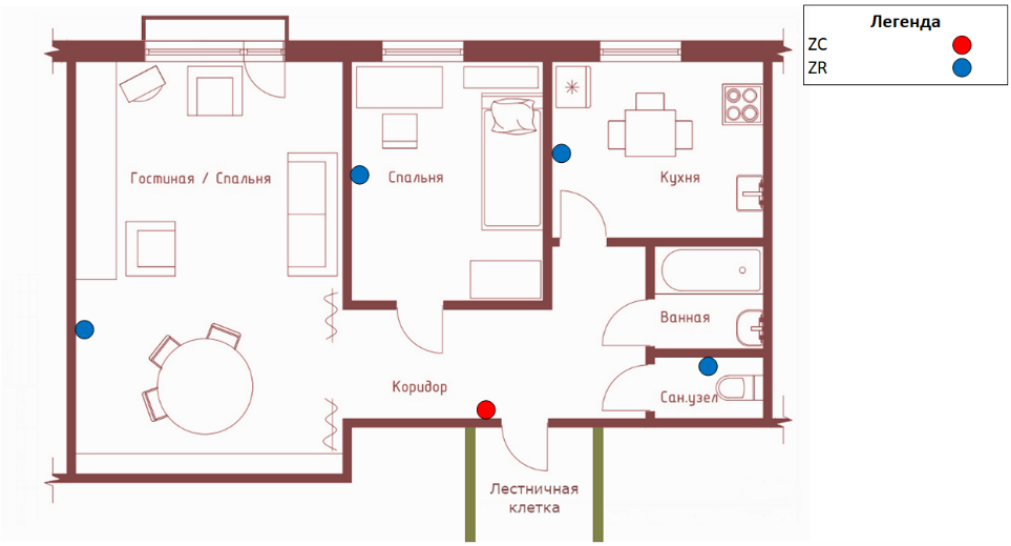


Рис. 1. Схема размещения координаторов (ZC) и маршрутизаторов (ZR) Zigbee.

Реализация основных и опциональных требований к системе “Умный дом” для пожилого человека

Видеонаблюдение. Видеонаблюдение планируется вести с целью записи потенциальных злоумышленников перед дверью квартиры. Записи планируется хранить локально в течение хотя бы 2 недель, по возможности – синхронизировать записи с удалённым хранилищем по протоколу NFSv4 с авторизацией и шифрованием с помощью Kerberos krb5p.

Планируется использовать 2 IP-камеры для установки в коридоре перед входной дверью и на лестничной клетке при входе в квартиру. Помимо основного функционала они должны также реагировать на движение в кадре для автоматического начала записи и работать в условиях плохой освещенности освещённостью. Камеры соединены с контроллером кабелями Ethernet (стандарт IEEE 802.3af или лучше), электропитание обеспечивается по технологии Power-over-Ethernet (PoE). Включение осуществляется по команде, катализаторами которой являются инфракрасные датчики, настроенные на радиус 1 метра от двери. Таким образом, запись видеоданных только при обнаружении активности в поле обзора камер.

Так как разрабатываемая система будет отвечать за жизнь и здоровье человека, а также за целостность и сохранность его имущества, необходимо обеспечить её надёжность и отказоустойчивость. Поэтому сервер системы видеонаблюдения должен обеспечить необходимую пропускную способность системы хранения данных для одновременной записи видеопотоков с двух камер, надежное локальное хранение данных в течение недели в случае записи 24/7 и резервное копирование видеозаписей в облачный сервис хранения данных.

Для оценки объема резервируемых данных предположим, что запись происходит 12 часов в день в разрешении 1920x1080, 30 кадров в секунду. Битрейт такого видео потока – в среднем 3 Мбит/с. Нагрузка на подсистему ввода-вывода от одной камеры - в среднем 60 IOPS, при этом размер блоков - 8 КБ и более. Следовательно, система хранения данных должна обеспечить резервированное хранение потока данных до 3*2/70% = 8.6 Мбит/с, с размером блоков от 8 КБ и 60*2/70% = 171.4 IOPS. Для таких требований достаточно производительности 2 жёстких дисков в RAID-1 (зеркало).

Для хранения информации в течение как минимум недели потребуется 7(дней)*12(часов)*3600(секунд)*2(камеры)*3(Мбит/с)/8(бит) = 226 800 МБ = 226.8 ГБ. Для повышения надёжности, компактности и производительности системы предлагается использовать 2

твердотельных SSD накопителя 2.5”, объёмом 480 ГБ.

В качестве локального сервера планируется использовать мини компьютер raspberry pi 4b с 8 ГБ оперативной памяти. Для реализации ZigBee функционала планируется применить микроконтроллер Texas Instruments CC2652R, который поддерживает протоколы Zigbee 3.0, Bluetooth mesh, Bluetooth 5.1 и другие. Для реализации программной части подсистемы ZigBee в этом проекте планируется адаптировать открытый исходный код проекта Zigbee2MQTT. Таким образом, и за локальное хранение данных, и за интеграцию системы Умного дома отвечает локальный сервер. В качестве устройства, обеспечивающего доступ системы к сети Интернет, планируется применить маршрутизатор Mikrotik hEX PoE. Он позволит поддерживать входящие VPN соединения, для безопасного удалённого администрирования системы [6,8].

Автоматизация освещения. Для автоматического управления освещением используются датчики движения, которые располагаются в пролетах комнат. Для повышения уровня надежности системы в комнатах устанавливаются датчики присутствия, которые фиксирует присутствие неподвижного живого объект, и ZR дают команду актуаторам на включение/выключения освещения. В Mesh-сети ZigBee лампы выступают в качестве ZR по умолчанию (в случае соблюдения требований по электропитанию), что позволяет улучшить связность и доступность Mesh-сети для оконечных устройств [8]. Система будет настроена таким образом, что свет будет гореть в комнате, где находиться человек и в соседней от него комнате. После выхода человека из комнаты, по истечении 2 минут, актуатору будет дана команда выключения света. Возможность управлять источниками света физическим путем остается, для этих целей используются отдельные выключатели [4,7].

Измерение показателей здоровья. Данная функция является одной из наиболее критически важных в рассматриваемой системе. Она может быть реализована с использованием смарт-часов, подключенных к смартфону по протоколу Bluetooth 5. Данное устройство должно осуществлять измерение пульса, измерение кровяного давления, температура тела и содержание кислорода в крови, отображение времени и создание заметок. В проектируемой системе планируется реализовать сбор исторических данных о показателях здоровья пожилого человека. Для этого требуется выбрать подходящее оборудование. Необходимо отслеживать:

- кровяное давление;
- пульс пожилого человека;
- содержание кислорода в крови.

Данные с устройств должны собираться и систематизироваться автоматически.

Мониторинг движения объекта. В трость пожилого человека устанавливается специальный маячок, который должен посылать эхо запросы каждые 30 секунд (при условии, что трость подключена к домашней сети на ZR). Время доставки эхо запросов будет обрабатываться на серверах, и получаемые в результате координаты нахождения трости визуализируются в специализированном интерфейсе мобильного приложения в виде карты квартиры.

Проверка санузла на протечки. Данную функцию осуществляет напольный детектор протечки, который можно установить под раковиной. При детектировании протечки датчик начнет издавать звуковой сигнал, а также сообщит об этом ZR, который в свою очередь запустит сценарий перекрытия воды с помощью автоматических кранов.

Тревожная кнопка. При ее активации, светильники во всех комнатах включается с помощью актуаторов, контактным лицам приходит срочное уведомление в мобильное приложение со всей необходимой информацией: местоположение и показатели здоровья.

Климат-контроль. В каждой жилой комнате и на кухне установлены счетчики измерения температуры, влажности, атмосферного давления. В зависимости от времени года и показателей счетчика, сервер будет давать команды климат устройствам. Для управления обогревателем и кондиционером планируется использовать ZigBee термостат. Для автоматизированного централизованного контроля за микроклиматом в квартире в систему также должны быть интегрированы средства кондиционирования и обогрева. Схема организации климат-контроля приведена на рисунке 2.

Безопасность. Для пожилого человека не предусмотрен процесс авторизации, так как в квартиру он получает доступ с помощью обычного ключа, а управление устройствами осуществляется с помощью пультов и выключателей и локальных средств, изолированных от доступа извне. Несанкционированный доступ к системе возможен в случае попадания в открытый доступ пароля для подключения во внутреннюю сеть с помощью VPN.

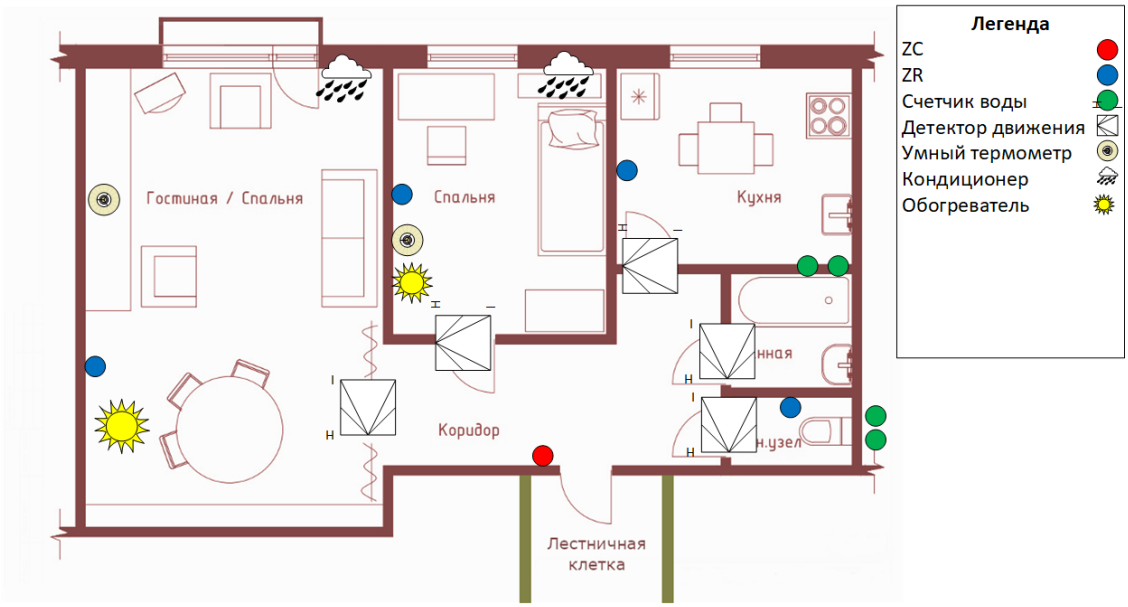


Рис. 2. Схема организации климат-контроля

Заключение

На сегодняшний день протокол ZigBee является одним из наиболее популярных решений для автоматизации жилых помещений. Построенные на его основе сети характеризуются mesh-топологией. К их главным преимуществам можно отнести быстрое развертывание, высокую надежность (по причине большого числа связей между элементами) и отсутствие необходимости постоянного администрирования. Это позволяет использовать протокол ZigBee при организации системы “Умный дом” для нужд маломобильных групп населения, в том числе, пожилых людей.

Литература

1. *Перри Л.* Архитектура интернета вещей / пер. с анг. М. А. Райтмана. М.: ДМК Пресс, 2019. 54 с.
2. https://habr.com/ru/post/535658/
3. *Степанов С.Н., Степанов М. С.* Учебное пособие для выполнения практических работ по дисциплине “Основы Интернета Вещей”. М.: МТУСИ, 2020. 77 с.
4. https://www.ti.com/product/CC2652R.
5. https://www.zigbee2mqtt.io.
6. https://mikrotik.com/product/RB960PGS.
7. https://gadget-freakz.com/xiaomi-gateway-3-highly-hackable.
8. https://github.com/Koenkk/zigbee2mqtt/issues/462
9. *Орлов В.Г., Тюмин С.Г.* Стандарты беспроводной связи для системы умный дом // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 20-28.
10. *Степанов С.Н., Степанов М.С., Маликова Е.Е., Цогбадрах А., Ндайикунда Ж.* Построение и анализ обобщенной модели разделения ресурса для LTE технологий с функциональностью NB-IOT // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 12. С. 71-77.
11. *Першина В.А., Титова Н.Д., Степанов М.С.* Построение автоматизированной системы сбора данных с приборов учета на базе стандарта LORAWAN // REDS: Телекоммуникационные устройства и системы. 2019. Т. 9. № 2. С. 3-9.
12. *Степанов М.С.* Использование калькулятора расчета характеристик гетерогенных беспровдоных сетей для разработки учебно-лабораторного практикума по дисциплине "основы интернета вещей" в МТУСИ // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2020. Т. 9. № 4. С. 9-14.
13. *Артвел Р.М., Степанов М.С.* Разработка функциональной модели сети интернета вещей на основе технологии narrow band internet of things (NB-IOT) // Телекоммуникации и информационные технологии. 2020. Т. 7. № 2. С. 39-44.

THE PRINCIPLES OF ORGANIZATION OF THE "SMART HOME" SYSTEM BASED ON ZIGBEE TECHNOLOGY FOR ELDERLY POPULATION

Leonid S. Poskotin,
Graduate MTUCI, Moscow, Russia,
svp_vpl@yahoo.com

Timuк Turgut,
Graduate MTUCI, Moscow, Russia,
hinhardian@gmail.com

Dmitry V. Shishkin,
Graduate MTUCI, Moscow, Russia,
draknem@gmail.com

Mikhail S. Stepanov,
Associate Professor of the Department of CN&CS, PhD, MTUCI, Russia,
m.s.stepanov@mtuci.ru

Abstract

Machine-to-machine communication is one of the main trends in the modern telecommunications world. In the concept of the Internet of Things, there are two main areas - long-range and short-range networks. among which there are popular systems "Smart Office" and "Smart Home". Various technologies help to automate the processes of managing security, climate control, lighting, etc. The aim of the article is to develop a "Smart Home" system for elderly using ZigBee technology. Basic and additional requirements that must be taken into account in this system are specified. A brief description of the latest version of the ZigBee 3.0 protocol is provided. Requirements for equipment are presented. The recommendations are given on the implementation of some basic and optional requirements for the Smart Home system for an elderly person.

Keywords: *Internet of Things, ZigBee, Smart home, mesh networks, elderly people*

АНАЛИЗ АРХИТЕКТУРЫ СИСТЕМЫ УПРАВЛЕНИЯ И АЛГОРИТМА ПРОЕКТИРОВАНИЯ БЕСПИЛОТНОГО НАДВОДНОГО АППАРАТА

Сорокин Александр Юрьевич,
магистрант МТУСИ, Москва, Россия,
sorokin.alexandr.2018@yandex.ru

Саксонов Евгений Александрович,
профессор кафедры МКиИТ, д.т.н., МТУСИ, Москва, Россия,
saksmiem@mail.ru

Аннотация

В данной статье приведён обзор развития беспилотных технологий на сегодняшний день. Обоснована их актуальность, показаны сфера применения и вектор дальнейшего развития. Представлен анализ архитектуры системы управления автономного надводного аппарата, предназначенного для использования на пространствах акваторий. Рассмотрены модули системы управления автономного надводного аппарата: блок управления, система навигации, система движения и система связи. Представлен общий алгоритм проектирования беспилотного надводного аппарата.

Ключевые слова*: система управления, управление надводным аппаратом, беспилотные надводные аппараты, управление беспилотным аппаратом, архитектура системы управления.*

Введение

На сегодняшний день одним из самых быстроразвивающихся и перспективных направлений является сфера беспилотных технологий. В разработках с применением этих технологий Россия принимает непосредственное участие наравне с другими государствами. В перспективе, использование полученных достижений позволит улучшить безопасность, а также закрепить планомерное увеличение экономического роста в стране.

Традиционно научно-исследовательские суда были и остаются важнейшей наблюдательной площадкой, на которой проводятся междисциплинарные исследования. Высокая стоимость их использования не позволяет получать данные с необходимым пространственным и временным разрешением. Недавний альтернативный способ, который позволяет проводить наблюдения за водной акваторией с хорошим пространственным и временным разрешением одновременно, а также с меньшими затратами, – это применение планеров и автономных надводных аппаратов.

Создание более новых, совершенных, в том числе и интеллектуальных, а также информативных систем автопилотирования надводных аппаратов стало возможным благодаря использованию различного типа сенсорного оборудования, такого как: устройства фото- и видео- фиксации, ультразвуковые датчики и локаторы, радары, лидары и др., в частности, используемые в беспилотных аппаратах как источники данных машинного зрения [1- 4].

Проектирование систем управления беспилотными надводными аппаратами

Системы управления беспилотных надводных аппаратов в основном проектируются вендорами по модульному принципу с различными подсистемами, управляемыми модульным блоком управления, базирующимся на встроенном компьютере (на пример, в США Diamond Systems Corporation «Phodeus», с возможностью расширения (добавление новых плат) посредством использования шины расширения, например «PC104»).

Можно выделить следующие базовые модули беспилотных устройств:

1. блок управления;

2. система навигации;
3. система движения;
4. система связи;
5. система безопасности;
6. система сбора данных.

Приведём описание данных систем более подробно, за исключением систем безопасности и сбора данных.

Основные модули системы управления беспилотным надводным аппаратом

Блок управления.

Блоком управления может является одноплатный компьютер стандарта «PC104+», так как его использование позволит обеспечить возможность подключения новых плат, посредством использования шины того же стандарта, и периферийных устройств, при константных размерах пространства размещения. Всё это позволяет создавать и применять различные конфигурации используемых подсистем. Примером такого компьютера, может являться модель упомянутого выше одноплатного компьютера «Phodeus» (рис. 1), производителем которого является США, Diamond Systems Corporation [5]. Компьютер «Phodeus» выполнен на процессоре AMD® Geode™ LX800, 500 МГц. Процессор имеет низкое энергопотребление (максимум 12 Вт) при достаточно малых габаритах (92x98 мм), что является неоспоримым преимуществом в сфере проектирования беспилотных надводных аппаратов.

Работа компьютера может осуществляться под следующими операционными системами, что обусловлено установленной версией BIOS, Phoenix-Award PnP Flash BIOS:

1. Windows 2000;
2. Windows XP;
3. Windows CE 5.0;
4. Linux.

Поддержка одноплатным компьютером различных операционных систем даёт возможность снизить материальные затраты при производстве беспилотных надводных аппаратов, так как не будет необходимости закупать новые лицензии операционных систем, при наличии уже поддерживаемых.

Система хранения данных «Phodeus» представляет собой компактную флеш-память, в виде двух накопителей IDE Flash Disk, имеющую хорошую защиту от вибрации.

Для реализации программирования на одноплатном компьютере «Phodeus» можно использовать такой графический инструмент программирования, как США, NI «LabVIEW» (рисунок 2). Программирование с его использованием будет выполняться на языке «G». Среда разработки «LabVIEW» хорошо зарекомендовала себя в таких сферах [6,7], как:

1. управление техническими объектами;
2. управление технологическими процессами;
3. сбор и обработка данных.

Одноплатный компьютер также оснащён 2-мя последовательными портами RS232 (COM1) и RS232/RS422/RS485 (COM2) для управления различными устройствами.

Базовую конфигурацию можно оснастить картой сбора данных «PC104-DAS16JR/12» («PC104-DAS16JR/16») с аналоговыми входами и разрешением 12 бит, 150 кбит/с и 8 цифровыми входами для получения данных с аналоговых и цифровых датчиков.

Система навигации.

Система навигации может быть представлена гибридной системой GPS/ГЛОНАСС, для достижения связи с максимально возможным количеством спутников, что позволит с большей точностью и скоростью определять местоположение беспилотного надводного аппарата.

Для реализации гибридной системы GPS/ГЛОНАСС на беспилотном надводном аппарате можно использовать двухчастотный мультисистемный высокоточный навигационный приёмник Россия, «NV08C-RTK-M L1/L2». Его использование позволит обеспечить навигацию с точностью до сантиметра благодаря фазовым измерениям сигналов L1/L2 систем ГЛОНАСС и GPS соответственно, получаемым с включённых сигнальных спутниковых систем функционального дополнения (SBAS),

позволяющих проводить оптимальную навигацию в реальном времени. Взаимодействие с системой навигации происходит через стандартный порт RS232. Неоспоримым преимуществом использования данного приёмника является и то, что вендоры, в ближайшей перспективе, обещают поддержку следующих систем: GALILEO и BeiDou. Помимо обеспечения высокоточной навигации, приёмник также имеет низкое энергопотребление (< 600 мВт), компактный формфактор и высокую производительность [8,9] .

Для приёма сигналов со спутников можно использовать, например, антенну Россия, «TW3882 L1/L2 ГЛОНАСС/GPS/GALLILEO/BeiDou» (рис. 3). Её преимуществами являются низкий уровень шума (2,5 дБ), коэффициент усиления (35 дБ), а также поддержка систем GALILEO и BeiDou. Также она имеет круговую поляризацию высокого уровня и защиту от многолучёвости. Исполнение корпуса соответствует стандарту IP67 [10].

Оснастить навигационную систему цифровым компасом и 3-х осевым указателем высоты позволит установка модуля США, «TCM-2.6» (рисунок 4). «TCM-2.6» – это 3-х осевой компас с компенсацией наклона (известной как тангаж, рыскание и крен) с диапазоном наклона ± 80°. Расширение системы навигации данным модулем позволит обеспечить ещё более высокие точность (0,8°), разрешение (компас 0,1°) при низком энергопотреблении (< 20 мА).

Система движения.

Силовая установка может включать в себя:

1. Главный двигатель – для обеспечения движения;
2. Два боковых двигателя – для осуществления контроля над направлением движения беспилотного надводного агрегата;

Главным двигателем может быть Seaeye Thruster «SI-MCT01-B» (рисунок 5), обеспечивающий номинальную мощность от 300 Вт до 960 об/мин благодаря интегрированным драйверам управления мощностью.

Боковые двигатели могут быть представлены двигателями Seabotix Thruster «BTD150» (рисунок 6). Модель Seabotix Thruster «BTD150» обеспечивает максимальную тягу от 25 Н до максимальной мощности 80 Вт под контролем интегрированных драйверов управления мощностью.

Система связи

При использовании вышеописанных систем, управление основным двигателем может осуществляться блоком управления напрямую через протокол последовательной связи RS485. Для управления боковыми двигателями можно установить модуль Lynxmotion «SSC-32» (рисунок 7), представляющий собой серво контроллер, использующий связь RS232 [7,9].

Модуль «SSC-32» позволяет управлять выходами, в количестве до 32-х, через последовательную связь RS232. Эти выходы выдают сигнал с переменной шириной импульса, определяемой пользователем, от 500 до 2500 пс с определенной частотой. Интегрированный драйвер может преобразовывать эти переменные в сигнал широтно-импульсной модуляции (PWM), подходящий для управления двигателем.

Рис. 1. Одноплатный компьютер США, «Phodeus» Diamond Systems Corporation

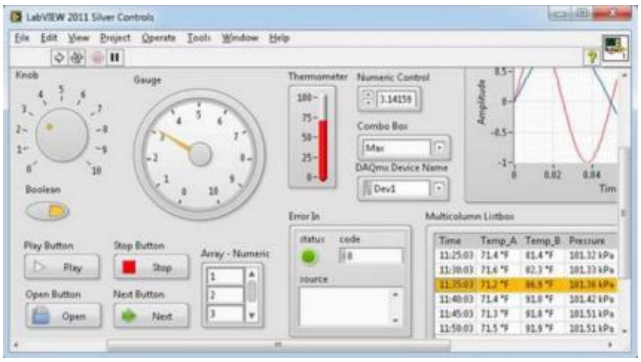


Рис. 2. Интерфейс среды разработки США, NI «LabVIEW»

Рис. 3. Антенна Россия, «TW3882 L1/L2 ГЛОНАСС/GPS/GALLILEO/BeiDou»

Рис. 4 – Модуль США, «TCM-2.6»

Рис. 5. Основной двигатель Seaeye Thruster «SI-MCT01-B»

Рис. 6. Боковой двигатель Seabotix Thruster «BTD150»

Рис. 7. Модуль Lynxmotion «SSC-32»

Этапы проектирования беспилотного надводного аппарата

Надводный беспилотный аппарат проектируется в соответствии с общим алгоритмом, включающим в себя пять этапов [8-10]:

1. В соответствии с установленными массой полезной нагрузки и значением автономности необходимо выбрать главные размерения и водоизмещения с учётом статистических зависимостей;
2. Для обеспечения расчётного водоизмещения нужно установить некоторый диапазон главных размерений, а также произвести расчет нагрузки масс с последующим уточнением водоизмещения;
3. Осуществить прямой расчёт массы корпуса возможных к применению компоновок;
4. Рассчитать полное сопротивление компоновок, произвести уточнение необходимых мощности и энергоемкости элементов ДРК и АКБ соответственно;
5. Выбрать наиболее подходящий вариант для реализации.

Четвёртый этап проектирования беспилотного надводного аппарата требует особого внимания, так как достижение максимального значения скорости хода, необходимого для работы в условиях течений, напрямую зависит от производимого на данном этапе расчёта полного сопротивления агрегата, а также выбираемой для него формы корпуса.

Чтобы упростить процесс вычислений, можно прибегнуть к использованию вычислительных комплексов. Так, для вычисления полного сопротивления, можно использовать вычислительный комплекс «Michlet» (расчёт производится с применением модифицированного интеграла Митчелла). А для расчётов гидродинамических параметров вычислительный комплекс «OpenFOAM», являющегося open-source software – свободно распространяемым программным обеспечением вычислительной гидродинамики.

Реализация проектной задачи посредством применения вышеописанного алгоритма не предполагает объёмных трудозатрат.

Для создания в дальнейшем математической модели уже спроектированного беспилотного надводного агрегата необходимо произвести корректировку результатов, которые будут получены после проведения статических и динамических испытаний, в соответствии с вышеописанным алгоритмом.

Заключение

На сегодняшний день область беспилотных технологий является одним из самых перспективных направлений. Развитие сферы разработки сенсорного оборудования различного типа позволяет создавать всё более совершенные и интеллектуальные беспилотные надводные агрегаты. Установка на беспилотные надводные агрегаты таких модулей как: локаторы, лидары, устройства видео- и фото- фиксации, позволит использовать машинное зрение на борту, что многократно расширит сферу применения беспилотных надводных аппаратов. Это в совокупности может стать наиболее финансово выгодной и функционально эффективной альтернативной применяемым на сегодняшний день научно-исследовательским судам для проведения междисциплинарных исследований.

Литература

1. *Лавриненко А.В. и др.* Выбор формы корпуса автономного необитаемого надводного аппарата с помощью современных средств вычислительной гидродинамики // Морские интеллектуальные технологии. 2018. № 4(42). Т. 1. С. 71-75.
2. *Гайкович А.И.* Теория проектирования водоизмещающих кораблей и судов. В 2 т. Т. 1. Описание системы «Корабль». СПб.: Моринтех, 2014. 822 с.
3. *Гайкович А.И.* Теория проектирования водоизмещающих кораблей и судов. В 2 т. Т. 2. Анализ и синтез системы «Корабль». СПб.: Моринтех, 2014. 874 с.
4. *Кожемякин И.В, Рождественский К.В., Рыжов В.А.* Вопросы гидродинамического проектирования надводных глайдеров нового поколения. Морские интеллектуальные технологии. 2018. № 2(24). Т. 2. С. 45-51.
5. *Франк М.О. и др.* Определение главных размерений автономного необитаемого надводного аппарата на ранних стадиях проектирования // Морские интеллектуальные технологии. 2019. № 2(44). Т. 1. С. 55-60.
6. *Кожемякин И.В. и др.* Перспективные платформы морской робототехнической системы и некоторые варианты их применения // Известия ЮФУ. Перспективные системы и задачи управления. 2019. № 1(174). С. 59-77.
7. *Кожемякин И.В. и др.* Надводные глайдеры: вчера, сегодня, завтра. Часть 1 // Морской вестник. 2013. № 1(45). С. 113-117.
8. *Занин В.Ю. и др.* Разработка автономных необитаемых надводных аппаратов класса микро с функцией группового управления // Известия ЮФУ. Тематический выпуск. Перспективные системы и задачи управления. 2017. № 1(186). С. 55-74.
9. *Кожемякин И.В. и др.* Разработка автономных необитаемых надводных глайдеров // Известия ЮФУ. Тематический выпуск, Перспективные системы и задачи управления. 2013. № 3(140). С. 31-39.
10. The Conceptual Shape Of The Robotic Underwater - Surface Vehicle Of The Increased Autonomy With Changeable Geometry Of The Hull For The System Of Robotized Underwater Seismic Exploration In Subglacial Water Areas / *V.S. Taradonov [et al.]* // Extreme Robotics: Proceedings of the International Scientific and Technological Conference. St. Petersburg: Gangut, 2019. P. 241-247.

ANALYSIS OF THE MANAGEMENT SYSTEM ARCHITECTURE AND THE DESIGN ALGORITHM UNMANNED SURFACE VEHICLE

Alexander Y. Sorokin,
Graduate MTUCI, Moscow, Russia,
sorokin.alexandr.2018@yandex.ru

Evgeny A. Saxonov,
Professor of the Department of MK&IT, D.Sc. (Technology), Moscow, Russia,
saksmiem@mail.ru

Abstract

This article provides an overview of the development of unmanned technologies to date. Their relevance is justified, the scope of application and the vector of further development are shown. The article presents an analysis of the architecture of the control system of an autonomous surface vehicle designed for use in water areas. The modules of the control system of an autonomous surface vehicle are considered: the control unit, the navigation system, the motion system and the communication system. A general algorithm for designing an unmanned surface vehicle is presented.

Keywords: *vehicle, control, control system, surface vehicle control, vehicle control, unmanned surface vehicles, unmanned vehicles, unmanned vehicle control, control system architecture.*

ИССЛЕДОВАНИЕ АЛГОРИТМОВ МАТЕМАТИЧЕСКОГО ПРОГНОЗИРОВАНИЯ ОТТОКА КЛИЕНТОВ (CHURN PREDICTION) С ОЦЕНКОЙ ЭФФЕКТИВНОСТИ ОБУЧЕННОЙ МОДЕЛИ И ИНТЕГРАЦИЕЙ ПРОГНОЗА В ЭКОНОМИЧЕСКИЙ ЭКСПЕРИМЕНТ

Рубенчик Марк Ильич,
студент МТУСИ, Москва, Россия,
markrubenchik@gmail.com

Скородумова Елена Александровна,
доцент кафедры ТВиПМ, к.ф.-м.н., МТУСИ, Москва, Россия,
eas@mtuci.ru

Аннотация

Цель исследования – анализ стандартных предиктивных алгоритмов в рамках востребованной задачи в современных сферах, таких как телекоммуникации, маркетинг и банковская сфера. В расчетах используется датасет компании Orange, на базе которого будет проведено базовое статистическое исследование для выбора метрик, алгоритмов и методов оптимизации. Для получения информации об эффективности обученных алгоритмов используется тестовая выборка, по которой определяется наиболее приемлемая модель.

Ключевые слова: *математическое прогнозирование, экономический прогноз, нейронные сети, линейная модель, оптимизация, исследование датасета, гиперпараметры.*

Важным элементом в ведении бизнеса является выстраивание взаимоотношений с нынешними клиентами или customer relationship management (CRM). От качества работы с аудиторией зависит успех компании. Одним из элементов CRM является прогнозирование оттока клиентов или churn prediction. Задача заключается в предварительном нахождении пользователей, склонных к будущему отказу от каких-либо продуктов или услуг. Точное нахождение покупателей такого рода помогает эффективно препятствовать их уходу, а также выявлять причины этого и принимать меры по удержанию. Эта задача актуальна для современных сфер, оказывающих услуги в сегменте B2C, и областей, где распространение близко к 100%, таких как телекоммуникации, маркетинг и банковская сфера. В работе будут использоваться данные французской телекоммуникационной компании Orange. Так как задача связана с клиентскими данными, они анонимизированы и обфусцированы: из набора данных удалена любая информация, позволяющая идентифицировать пользователя. Также неизвестны названия (кроме их алиасов типа “VarN” где N – номер показателя) и описания аналитик, предоставленных для прогноза.

Цель работы – анализ стандартных предиктивных алгоритмов (в данном случае классификации данных). Для исследования важно:

- подготовить датасет и проанализировать его на значимость признаков для того, чтобы в дальнейшем исключить из модели зависимые признаки и избежать построения избыточной (переобученной) модели;
- исследовать разные подходы для написания моделей (случайный лес, нейронные сети);
- изучить внутренние параметры моделей и проанализировать подобранные показатели и методы регуляции и оптимизации алгоритма;
- обучить модель и проанализировать ее работу на тестовой выборке;
- интегрировать модель в экономический эксперимент и оценить возможность применимости модели в реальной жизни.

Изучение датасета

В выборке, предоставленной компанией Orange, имеется 50 тысяч записей пользователей, покупающих услуги компании. База состоит из 230 переменных (190 – числовых и 40 категориальных). Выходной поток представляет собой бинарный код из значений “–1” – “churn” и “1”– “nochurn”. Для очевидного удобства –1 заменен на 0.

Вычислимдоли классов “отток” и “не отток”:

- доля класса "отток": 0.074275;
- доля класса "не отток": 0.925725.

Данные показатели говорят нам о том, что выборка сильно не сбалансирована. Анализ датасета показал, что выборка имеет много пропусков, и, следовательно, ее нужно будет заполнять самостоятельно, а также менять размер выборки. После изучения показателей, имеющих пропуски (> 50 %), и сортировки выборки была подготовлена новая версия выборки (со сбалансированными классами) из порядка 6 тысяч элементов. После удаления 154 параметров с пропусками (больше 50 %) остались 42 вещественных и 34 категориальных признака. Оставшиеся параметры имеют около 95% заполнения. Оставшиеся пропуски можно заполнить:

- вещественные признаки – средними значениями;
- категориальные – дефисами.

Поскольку целевая функция бинарная применение коэффициента корреляции Пирсона невозможно. Поэтому в качестве коэффициента корреляции будем использовать другой показатель, подходящий для стандартных бинарных классификаторов. Для этого для каждой пары признак/метка [1;0] рассчитаем следующую статистику:

$E(X1|X2=1) – E(X1|X2=0)$,

где E – математическое ожидание X1 при условии X2 = 1 или X2 = 0, соответственно.

Данное отклонение от нуля будет соответствовать определенному уровню корреляции (+/–)[1], то есть чем дальше от нуля находится значение отклонения, тем сильнее коррелируют данные вещественных параметров, и мы можем говорить об их взаимосвязи с целевой функцией. Проведенные расчёты указанных отклонений показали, что количество подходящих вещественных параметров для классификатора можно сократить до 20.

Анализ имеющейся базы показал, что часть категориальных признаков имеют одинаковое значение вне зависимости от других параметров. Эти признаки в дальнейшей обработке рассматриваться не будут. Также не подлежат рассмотрению признаки с равномерно распределенными значениями. Для построения модели будут использоваться те признаки, значениями которых могут быть не менее двух категорий, имеющих разные частоты. Таковыми являются признаки Var201, Var203, Var205 (рис. 1). На рисунке 2 изображена полная схема процесса отбора признаков для построения модели [3].

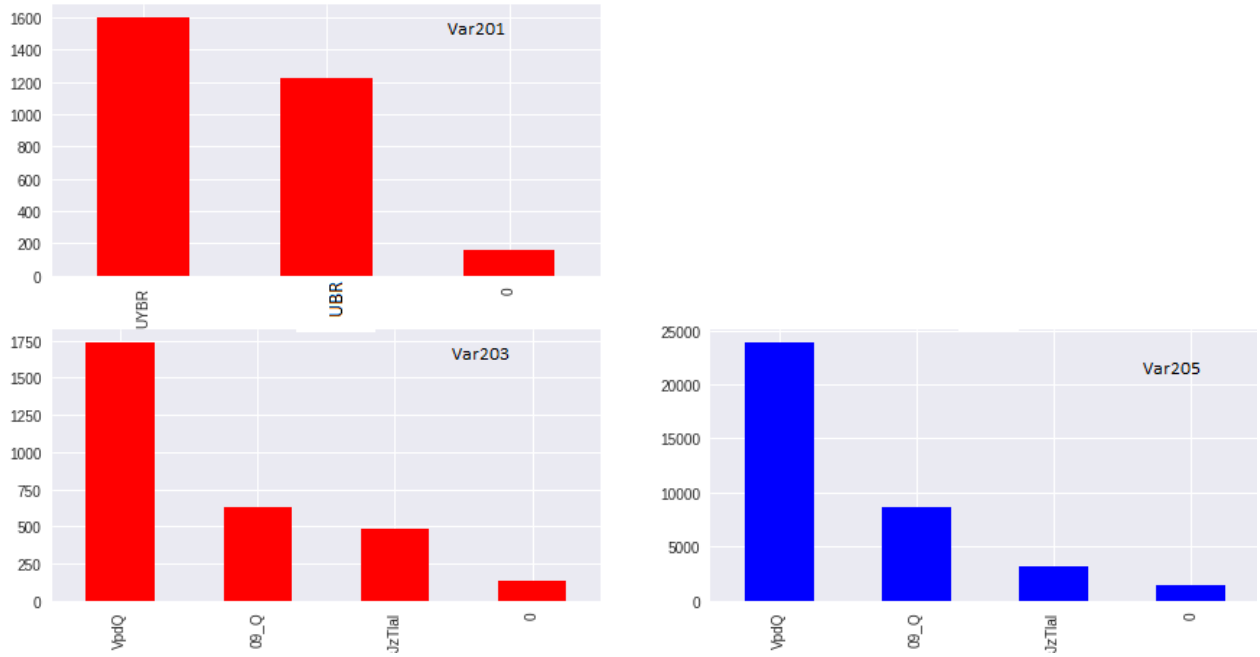


Рис 1. Гистограммы значимых категориальных признаков

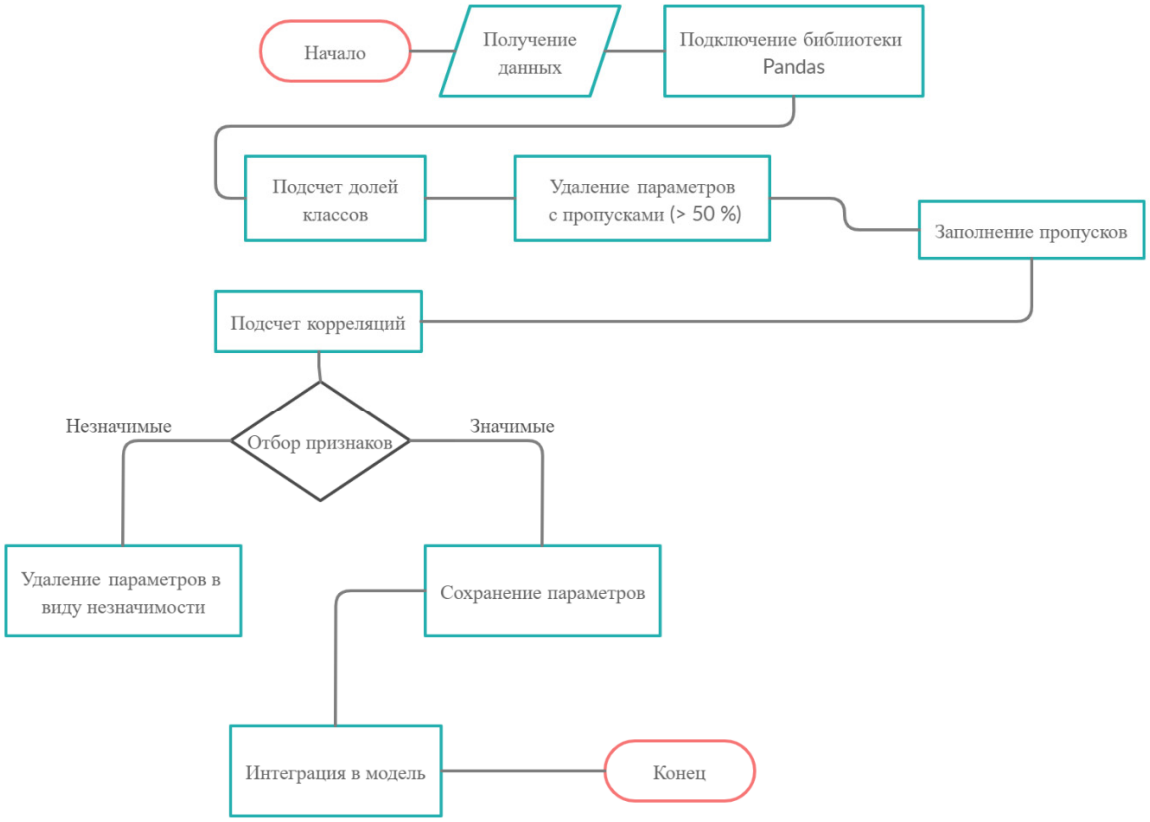


Рис. 2. Блок-схема процесса отбора признаков

Построение Baseline – модели

Проведя логирование категориальных признаков, мы можем перейти к оценке некоторых стандартных алгоритмов построения модели. Т. к. изначальная выборка (к которой необходимо будет вернуться при тестировании модели) несбалансированная, мы будем использовать стандартную метрику AUC-Roc-кривую ошибок, которая эффективна при несбалансированных классах. Как вспомогательную метрику выберем F-меру, точность (precision) и полноту (recall) [1]. Рассмотрим данные метрики.

$$\text{precision} = \frac{TP}{TP+FP},$$

$$\text{recall} = \frac{TP}{TP+FN},$$

где *TP*,*TN* – число истинно положительных и отрицательных результатов, и *FP* и *FN* – число ложно положительных и ложно отрицательных результатов, соответственно.

Precision –это доля объектов, названных классификатором положительными и при этом действительно являющимися положительными, а recall – доля объектов положительного класса из всех объектов положительного класса, которые нашел алгоритм. Именно введение precision не позволяет нам записывать все объекты в один класс, т.к. в этом случае мы получаем рост уровня False Positive. Recall демонстрирует способность алгоритма обнаруживать данный класс вообще, а precision — способность отличать этот класс от других классов. Ошибки классификации бывают двух видов: False Positive и False Negative. В статистике первый вид ошибок называют ошибкой I-го рода, а второй — ошибкой II-го рода. В нашей задаче по определению оттока абонентов ошибкой первого рода будет принятие лояльного абонента за уходящего, а ошибкой второго рода - "пропуск" уходящего абонента.

Precision и recall, в отличие от accuracy (доля правильно предсказанных алгоритмом ответов), задаваемой соотношением:

$$\text{accuracy} = \frac{TP+TN}{TP+TN+FP+FN},$$

не зависят от соотношения классов и потому применимы в условиях несбалансированных выборок. Также часто в реальной практике стоит задача нахождения оптимального для заказчика баланса между precision и recall.

F-мера (в общем случае Fβ) — это среднее гармоническое precision и recall:

$$F\beta = 2 \cdot \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}}.$$

Множитель 2 здесь нужен для нормировки, т.е. для того чтобы максимум F-меры был равен 1, а минимум 0. F-мера достигает максимума при полноте и точности, равными единице, и близка к нулю, если один из аргументов близок к нулю.

Одним из способов оценить модель в целом, не привязываясь к конкретному порогу, является AUC-ROC (или ROC AUC) — площадь (*A*rea *U*nder *C*urve) под кривой ошибок (*R*eceiver *O*perating *C*haracteristic curve). Данная кривая представляет собой линию от (0,0) до (1,1) в координатах True Positive Rate (TPR) и False Positive Rate (FPR):

$$TPR = \frac{TP}{TP+FN},$$

$$FPR = \frac{FP}{FP+TN}.$$

TPR– это полнота, а *FPR* показывает, какую долю из объектов negative класса алгоритм предсказал неверно. В идеальном случае, когда классификатор не делает ошибок (*FPR* = 0, *TPR* = 1) мы получим площадь под кривой, равную единице. В противном случае, когда классификатор случайно выдает вероятности классов, AUC-ROC будет стремиться к 0.5, так как классификатор будет выдавать одинаковое количество *TP* и *FP*. Каждая точка на графике кривой ошибок (рис. 3) соответствует выбору некоторого порога. Площадь под кривой в данном случае показывает качество алгоритма (больше – лучше). Кроме этого, важной является крутизна самой кривой – мы хотим максимизировать *TPR*, минимизируя *FPR*, а значит, наша кривая в идеале должна стремиться к точке (0,1).

Рис. 3 Пример Кривой ошибок

Проведем исследование стандартных алгоритмов: линейной модели (Ridge) и логической регрессии. Рассмотрим тренировочную сбалансированную выборку и проверим результаты обучения данных моделей при разных разбиениях данных на обучающую и контрольную выборку, не касаясь отдельной тестовой выборки, которая хранится отдельно. В случае линейной модели (Ridge), разделяющей поверхности, как видно из кривой ошибок бинарной классификации, изображенной на рисунке 4, при разных разбиениях обучающей выборки, мы получили результаты между 62% и 66% точности модели при тестировании. Однако применять данную модель дальше невозможно ввиду проблемы перемешивания классов данных, что не позволяет правильно разделить выборку. Данная проблема связана в первую очередь с самими данными и невозможностью построения разделяющей поверхности для классификации [2].В связи с этим в дальнейшем мы полностью откажемся от данной модели. При использовании Логической регрессии обнаружилась похожая проблема. Также проведя тестирование, мы получили точность между 58% и 60% (см. рис. 3).Поэтому стоит отбросить и это baseline – решение [3].

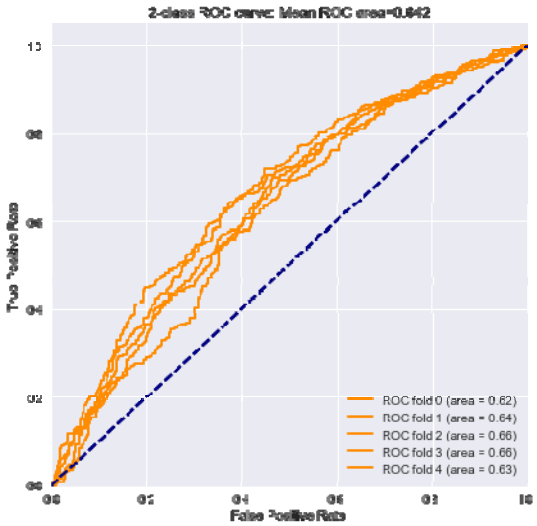


Рис. 4а. Кривая ошибок при использовании **Линейной модели**

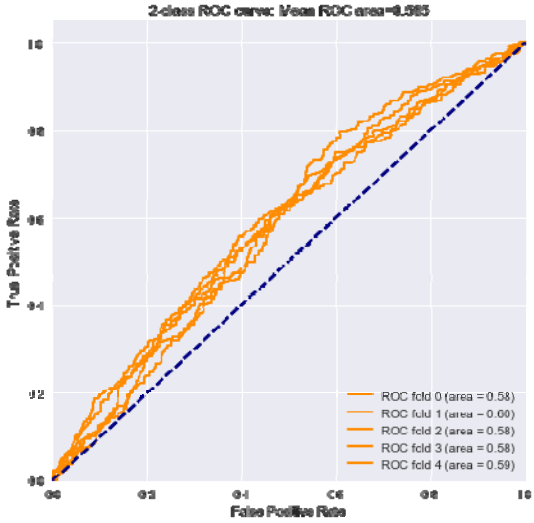


Рис. 4б. Результаты тестирования **Логической регрессии**

Проверив эти два “простых” метода, перейдем к более сложным структурам: случайному лесу и нейронной сети. Также стоит заострить внимание на том, что F-меру нельзя использовать в случайных лесах в виду того, что случайный лес не поддерживает возможность оценки вероятности оттока – не оттока клиента [1]. Проведем тестирование обученных моделей на разных разбиениях обучающей выборки. В таблице 1 представлены лучшие результаты тестирования этих двух моделей. Параметр ROC-AUC в таблице – это доля правильно выявленных данных, а PR-AUC – доля неправильно выявленных данных.

Таблица 1

Лучшие данные тестирования моделей на основе случайного леса и градиентного бустинга.

Параметры	Случайные Леса	Градиентный бустинг
ROC-AUC	0.6734	0.7022
PR-AUC	0.3266	0.2978

Как мы видим из таблицы, и случайный лес, и градиентный бустинг показали лучшие результаты, чем предыдущие две модели. Проанализировав оба этих параметра, мы приходим к выводу, что Случайный лес незначительно проигрывает модели с градиентным спуском.

Рассмотрим возможности для улучшения модели градиентного бустинга. Для этого оптимизируем данную модель, скорректировав внутренние гиперпараметры. Это можно сделать, например, с помощью одной из самых популярных и эффективных реализаций алгоритма градиентного бустинга – XGBoost. Этот алгоритм обладает большим количеством гиперпараметров и большей скоростью обучения по сравнению с обычным градиентным спуском. Кроме того, этот метод более удобен для данных с большим количеством параметров в целевой функции, а также с несбалансированными классами [5]. Также рассмотрим гипотезу об использовании в качестве входных параметров не только значимых признаков. В результате такой оптимизации мы сможем корректировать влияние категориальных параметров, которые также участвуют в классификации.

Оптимизация модели нейронной сети при помощи внутренних гиперпараметров

Входе baseline тестирований для решения задачи прогнозирования выбрана модель на основе алгоритма XGBoost.

Ввиду большого количества удалённых параметров из модели по причине пропусков или низкой значимости помимо тестирования модели на основе только значимых признаков стоит также протестировать модель на всех параметрах, которые не вошли в список значимых. Параметры, имевшие больше 50% пропусков, не учитывались. При тестировании моделей использовался набор метрик, по которым можно локализовать наилучший вариант как в поделённой тренировочной выборке, так и в тестовой, также почищенной от пропусков и с теми же параметрами, что и тренировочная.

Проведя первичное тестирование модели на значимых признаках, мы получили результаты по кривым ошибок. Как видно из таблицы 2, в сравнении с первоначальной версией градиентного бустинга мы улучшили результаты по обоим показателям. Новая модель стала более точной в выявлении положительных классов и меньше ошибается в сравнении с предыдущей версией. Замер показателей ROC-AUC и PR-AUC на тестовой выборке показал, что обученная и оптимизированная модель с более глубоким контролем гиперпараметров работает лучше стандартной. Следовательно, в дальнейшем мы будем использовать ее в качестве экспериментальной для выявления уходящих абонентов.

Таблица 2

Данные тестирований XGBoost-модели при значимых параметрах.

Параметры	Тренировочный датасет	Тестовый датасет
ROC-AUC	0.714	0.683
PR-AUC	0.286	0.317

Проверим, как поведет себя модель в случае, если на вход пойдет выборка, не очищенная от незначимых признаков. Это означает, что мы увеличиваем размерность входного потока с 23 параметров до 76. Проведем тестирование на непрореженной выборке. В данном случае модель обучилась на всех 76 признаках, где количество пропусков было минимально. Получив данные тестирований (таблица 3), мы можем видеть, что оптимизированная модель XGBoost показывает хорошие результаты. Также был замечен небольшой рост показателя ROC-AUC при использовании выборок с 76 периметрами при тестировании на обоих выборках. Однако вырос и показатель PR-AUC, который показывает, насколько ошибочно алгоритм находит негативный класс выборки или “отток”.

Таблица 3

Данные тестирований XGBoost-модели при всех параметрах.

Параметры	Тренировочный датасет	Тестовый датасет
ROC-AUC	0.728	0.692
PR-AUC	0.272	0.308

Как видно из значений показателей в таблицах 2–3, в случае прореживания параметров нейронная сеть незначительно отстает от модели, которую мы получили при использовании не 23, а 76 параметров, среди которых имеются“ шумовые” параметры с малой корреляцией. Отметим, что важным плюсом прореженной модели является простота и скорость обучения. Однако показатели модели на 76 признаках лучше за счет того, что модель учитывает также некоторые параметры, не вошедшие в набор 23 наиболее значимых. Данный эффект связан с несбалансированностью классов в начальной выборке, а также большим количеством переменных.

Описание эксперимента и оценка эффекта применения модели

Рассмотрим гипотетический эффект от внедрения модели. Так как нет данных о размерах доходов и расходов, мы проведем экономический эксперимент с введением некоторых параметров (расходы на удержание клиентов, а также средние доходы с каждого среднестатистического абонента). Однако удерживают не все клиентов. В данной задаче компании важно удержать наиболее прибыльную и массовую группу клиентов. Кроме того, надо учитывать затраты на маркетинг и удержание каждого выбранного клиента, а также невозможность проинформировать всех о дополнительных услугах и тарифах и т. п. Идеализируем ситуацию и предположим, что в случае принятого решения, позвонив клиенту и для проведения так называемого “удерживающего процесса”, предложить новые продукты и услуги клиенту, вероятность того, что абонент остался в базе компании (т. е. продолжит пользоваться ее услугами) равна 1. В реальности данная вероятность, от которой зависит дополнительная прибыль, неизвестна. Для ее расчетов проводятся дополнительные исследования по типу социальных опросов или фокус-групп, при помощи которых можно оценить среди людей разных возрастов доли тех, кто, возможно, останется в случае предложения тех или иных новых услуг и скидок. Средний доход от пользователя можно считать фиксированным в течение определенного периода (месяц-квартал), т. к. он постоянно пользуется конкретным тарифом и редко переплачивает за звонки и Интернет, и не зависящим ни от курсов валют, ни от экономической ситуации и т. д.

Дополнительный доход от внедрения можно вычислить следующим образом:

$$S = nd \cdot (p - q), \tag{1}$$

где d – число выявленных пользователей, склонных к уходу, p – средний доход от пользователей, полученный статистически за период (месяц-квартал), q – стоимость услуг по удержанию.

Так как мы не проводим 100% удержание, в эту формулу следует ввести дополнительный параметр n – процент звонков клиентам, который позволит снизить расходы на удержание путем уменьшения числа заявок. Используя формулу (1) и понимая количество клиентов в доле “Оттока”, можно оптимально подобрать параметры nи q для повышения доходности компании.

На практике также стоит учитывать психологическую проблематику удержания клиентов в будущем при помощи звонков, т. е. ввести вероятности того, что человек уйдет или не уйдет после того, как ему предложили более выгодный тарифный план. Для этого необходимо рассматривать иные способы изучения аудитории и, следовательно, менять способы удержания клиентов в зависимости от полученных данных. Также следует модернизировать предиктивную модель, чтобы знать не только уйдет или не уйдет абонент, но и вероятность его ухода для оптимизации обратной связи с аудиторией. Помимо этого, в самой формуле дополнительного дохода стоит учитывать не только описанные частные вероятности оттока клиентов, но и время, которое надо затратить на конкретного клиента, чтобы учитывать расходы на его удержание, а также затраты на персонал, участвующий в удержании.

Как указано выше, использование прогнозной модели может оказаться экономически выгодным. Однако на практике все оказывается несколько иначе. Поэтому стоит обратить внимание на решение следующих задач при использовании описанной модели:

- "Средний" абонент. При построении прогнозной модели все пользователи усреднялись. Без сомнений, это весьма грубое допущение, потому как потребности у абонентов разные. Например, у кого-то может быть в приоритете стоимость сообщений, у кого-то Интернет для планшета на дополнительном номере, а для кого-то важна бесперебойная связь в роуминге. Поэтому каждому надо делать предложение, которое может заинтересовать именно его, а не "среднего" абонента. Отсюда вывод о необходимости сегментации абонентов;

• A/A тестирование – контрольное тестирование модели на данных из одной группы (только “отток” или не “отток”). При наличии достаточного количества данных можно провести A/A тестирование и узнать, например, как сильно могут отличаться доли в двух группах абонентов, которым мы не делаем никакого предложения. Если результаты существенно различаются, то, вероятно, мы некорректно делим пользователей на группы или упускаем некоторые важные аналитики [4];

• Разбиение пользователей для A/B тестирования (сравнение разных групп пользователей). Здесь кажется логичным делать стратифицированные разбиения. Например, отбор абонентов, которые останутся с высокой вероятностью, и абонентов, которые скорее всего уйдут. Тогда абоненты 1, 3, 5, ... попадут в группу A, а абоненты 2, 4, 6, ... попадут в группу B. Здесь мы полагаем эту выборку стратифицированной, основываясь на результатах прогнозной модели (сначала идут те абоненты, предсказанная вероятность для которых больше) [3].

• Профиль пользователя. Для каждого абонента можно анализировать историю звонков, поскольку кто-то может пользоваться услугами преимущественно в рабочее время или наоборот. Так же, может оказаться полезным вычислять местоположение абонента, что тоже расскажет об абоненте, и т.д. Профилирование и сегментация могут взаимно дополнять друг друга (и, вообще говоря, грань между ними может быть условной);

• Наблюдение за ключевыми параметрами. Построение и использование модели может оказаться полезным и выгодным, но, скорее всего, она не будет корректной на долговременном периоде в виду, к примеру, развития конкурентов. Поэтому периодически необходимо проверять, как модель работает, как она описывает отток пользователей, постепенно набирая статистику как бизнес-показателей, так и метрик модели. Получая все больше и больше новых данных, можно дообучать модель, выявлять ее слабые и сильные стороны;

• Выявление ошибок классификации. Для объектов, где модель ошибается сильно, можно найти наиболее близкие (например, использовать косинусную меру) и попытаться выявить, что приводит к ошибке. Однако может оказаться, что эти объекты аномальные, и нет разумных объяснений, почему допускается ошибка. В этом случае можно разметить дополнительный признак [5];

• Обновление модели. Рано или поздно настанет момент, когда модель перестанет давать заявленное качество. Это может быть вызвано разными изменениями: ситуация на рынке, новые предложения компании и т.д. Поэтому необязательно дожидаться падения метрик модели, если в работе компании произошли или планируются перемены.

Заключение

В ходе исследования были построены и протестированы модели прогнозирования оттока клиентов, проведен анализ их эффективности на метриках качества и выбрана наиболее эффективная модель. Также рассмотрена задача о практическом применении модели и методика расчета прибыльности от ее применения в идеальных условиях. В заключение сформулированы задачи, решение которых позволит получить более эффективные результаты прогнозирования оттока клиентов и их удержания.

Литература

1. *Гудфеллоу Я., Бенджио И., Курвилль А.* Глубокое обучение/ пер. с анг. А.А. Слинкина. 2-е изд., испр. М.: ДМК Пресс, 2018. 652 с.
2. *Тревор Хасти, Роберт Тибширани, Джером Фридман.* Основы статистического обучения: интеллектуальный анализ данных, логический вывод и прогнозирование / пер. с англ. Д.А. Клюшина. М.: ООО «И.Д. Вильямс», 2020. 768 с.
3. *Хайкин Саймон.* Нейронные сети: полный курс, 2-е изд.: Пер. с англ. М.: ООО «И.Д. Вильямс», 2016. 1104 с.
4. *Редько В.Г.* Эволюция, нейронные сети, интеллект. Модели и концепции эволюционной кибернетики, изд. 10, стереотип. М.: URSS, 2019. 224 с.
5. *Рутковская Д., Пилиньский М., Рутковский Л.* Нейронные сети, генетические алгоритмы и нечеткие системы: Пер. с польск. И. Д. Рудинского. 2-еизд., стереотип. М.: Горячая линия – Телеком, 2013. 384 с.

RESEARCH OF ALGORITHMS FOR MATHEMATICAL FORECASTING OF CLIENT CHURN PREDICTION WITH ESTIMATION OF THE EFFICIENCY OF THE TRAINED MODEL AND INTEGRATION OF FORECAST INTO AN ECONOMIC EXPERIMENT

Mark I. Rubenchik,
Student MTUCI, Moscow, Russia,
markrubenchik@gmail.com

Skorodumova Al. Elena,
Associate Professor of Department PT&AM, PhD., MTUCI, Moscow, Russia,
eas@mtuci.ru

Abstract

The aim of the research is to analysis of standard predictive algorithms (in our case, data classification) within the scope of a demanded task in modern areas such as telecommunications, marketing, and banking. The calculations use the Orange dataset, based on which a basic statistical study will be carried out to select metrics, algorithms, and optimization methods. To obtain information about the effectiveness of the trained algorithms, a test sample is used, according to which the most acceptable model is determined.

Keywords: *mathematical forecasting, economic forecast, neural networks, linear model, optimization, dataset research, hyperparameters.*