ФАКУЛЬТЕТ
ИНФОКОММУНИКАЦИЙ

Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИНФОКОММУНИКАЦИИ

Сборник материалов 58-ой научной конференции аспирантов, магистрантов и студентов

Минск 2022

Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИНФОКОММУНИКАЦИИ

**58-я научная конференция
аспирантов, магистрантов и студентов**

Сборник материалов

18–22 апреля 2022 года
Минск, БГУИР

УДК 621.391

58-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 18-22 апреля 2022 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2022. – 235 с.; ил.

В сборнике опубликованы материалы докладов, представленных на 58-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.
Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

СОДЕРЖАНИЕ

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

УДК 004.056.53

ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Алейникова Д.И., студентка гр.961402

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В работе описаны технологии аутентификации пользователей в беспроводных сетях. Изучены основные протоколы аутентификации, авторизации и учёта, их особенности и основные отличия. Проведен анализ использования протокола RADIUS для контроля доступа в беспроводных сетях.

Ключевые слова. Беспроводные сети, контроль доступа, аутентификация, AAA, TACACS+, RADIUS.

В настоящее время технологии беспроводной передачи данных являются очень востребованными, что обусловлено сравнительно невысокой стоимостью и простотой построения беспроводных сетей, связанные с отсутствием кабелей, а также возможностью подключения к сети не только стационарного компьютера, но и других устройств. Беспроводные сети легко масштабируемы и не требуют больших затрат на обслуживание. Следует отметить, что использование беспроводной среды передачи данных приводит к возникновению вопроса о защите передаваемой информации и инфраструктуры сети в целом. Данные передаются по воздушному каналу и для перехвата трафика злоумышленнику достаточно использовать приёмник, установленный в радиусе действия сети, в то время как в кабельных сетях ему необходимо получить физический доступ к кабельной системе или оконечному устройству. При развертывании беспроводной сети следует уделять внимание обеспечению конфиденциальности и целостности передаваемых данных, проверке подлинности беспроводных клиентов и точек доступа.

В предыдущей работе [1] уже были рассмотрены основные принципы построения беспроводной локальной сети и организации VLAN на базе контроллеров Cisco WLC. В данной работе внимание уделяется процессам аутентификации беспроводных клиентов.

Для обеспечения контроля доступа к информационным ресурсам сети через беспроводное подключение можно воспользоваться технологией AAA (Authentication Authorization Accounting), которая основывается на трёх принципах: аутентификация, авторизация и учёт. Аутентификация – проверка подлинности клиента по его идентификатору, таким образом подключиться к сети смогут только разрешенные клиенты. Авторизация – определение и предоставление прав доступа клиента. Учёт – отслеживание действий клиента в сети. Следует отметить, что AAA можно использовать не только для контроля доступа пользователей к сети, но и для дистанционного администрирования сетевых устройств.

Для реализации технологии AAA существуют такие протоколы как RADIUS (Remote Authentication Dial-In User Service) и TACACS+ (Terminal Access Controller Access Control System), которые используются при взаимодействии WLC и AAA-сервера.

Протокол RADIUS был создан независимой группой разработчиков. На транспортном уровне использует протокол UDP, порты 1812 – для аутентификации, 1813 – для учёта. Следует отметить, что процессы аутентификации и авторизации совмещены, существует поддержка учёта действий пользователя в сети. Нет возможности разделить три основных процесса технологии AAA, их обработкой занимается одно устройство. Однако протокол позволяет проектировать гибкую распределенную систему, включающую в себя несколько RADIUS-серверов, которые перенаправляют запросы друг другу в случае отсутствия данных пользователя в локальной базе данных. Протокол поддерживает ограниченное число типов аутентификации (Clear text и CHAP). Характеризуется средней степенью защищенности: в отправляемых пакетах шифруется только поле с паролем. RADIUS позволяет обслуживать только одного клиента в каждый момент времени. Протокол допускает использование брандмауэра между клиентом и сервером, а также технологий трансляции IP-адресов. Это обусловлено тем, что IP-адрес клиента содержится не только в заголовке, но и в теле пакета.

TACACS+ был разработан компанией Cisco Systems, которая периодически выпускает его модификации. На транспортном уровне использует протокол TCP, порт 49. TACACS+ позволяет обслуживать несколько пользователей в каждый момент времени. Протокол предоставляет возможность разделить процессы аутентификации, авторизации и учёта по отдельным серверам.

Поддерживает такие типы аутентификации как: CHAP, ARAP, Clear text. Характеризуется высокой степенью защищенности в силу того, что шифруется всё тело отправляемого пакета. TACACS+ поддерживает аутентификацию внешнего типа: сервер аутентификации отправляет клиенту приложения пароль и клиент самостоятельно сравнивает полученный пароль и введенный пользователем. Такой тип авторизации является уязвимостью протокола. Злоумышленник может скомпрометировать данные пользователя при следующих условиях: на сервере включена функция внешней аутентификации пользователя; сервер аутентификации не производит проверку IP-адресов клиентов или злоумышленник произвел атаку IP-spoofing; злоумышленник узнал некоторое количество логинов пользователей и секретный ключ клиента и сервера, который хранится в открытом виде и на сервере, и у клиента. Решением проблемы может быть отказ от поддержания такого типа авторизации. TACACS+ не допускает наличие брандмауэра между клиентом и сервером, потому что найти соответствующий ключ можно только по IP-адресу клиента, а при работе через брандмауэр IP-адрес клиента будет изменяться по технологии трансляции сетевых адресов. Протокол TACACS+ не поддерживает возможность перенаправления запроса на другие серверы аутентификации.

Таким образом, для аутентификации пользователей в беспроводной сети предпочтительнее применять RADIUS. Используя UDP на транспортном уровне, он работает быстрее TACACS+, которому перед отправкой запроса необходимо каждый раз устанавливать TCP-соединение через процесс трёхстороннего рукопожатия. Так же RADIUS позволяет проектировать гибкую распределенную систему, что предпочтительно в случае, если пользователь захочет авторизоваться в системе, физически перемещаясь по разным регионам. В отличие от TACACS+ протокол RADIUS допускает наличие брандмауэра и применение технологий трансляции сетевых адресов без использования дополнительных настроек.

На рисунке 1 представлен пример построения безопасной инфраструктуры беспроводной сети на базе концепции AAA с использованием программного обеспечения Cisco Packet Tracer.

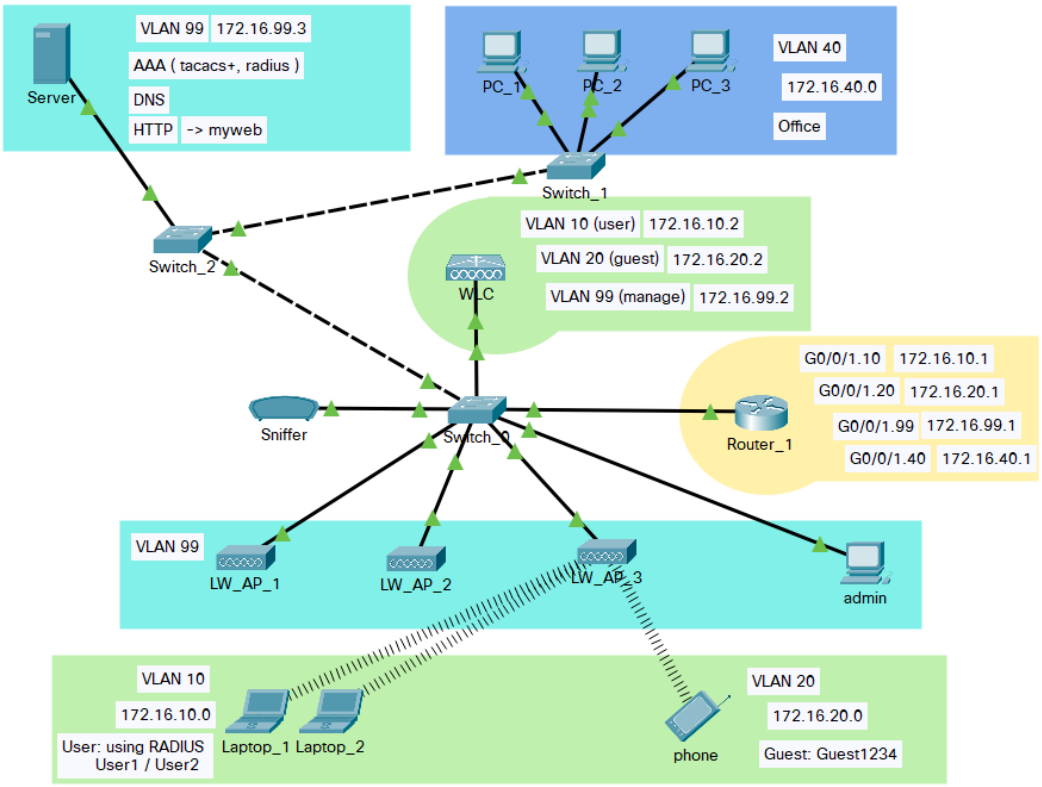


Рисунок 1 – Построение локальной сети в Cisco Pocket Tracer

В моделируемой сети было сконфигурировано два VLAN для беспроводной сети: гостевой и пользовательский, для рабочих организации. Для аутентификации и авторизации клиентов из VLAN для сотрудников организации используется удаленный RADIUS-сервер, а для гостевого – локальная база данных WLC. Рассмотрим процесс взаимодействия WLC и RADIUS-сервера, при попытке пользователя подключиться к сети:

– клиент отправляет запрос на аутентификацию, включающий такие идентификаторы пользователя как логин и пароль;

– точка доступа перенаправляет запрос на адрес WLC;

– WLC получает запрос клиента, формирует запрос аутентификации данного пользователя и отправляет его на RADIUS-сервер. Запрос включает в себя ключ симметричного шифрования, который используется для установления соединения с сервером;
– WLC ожидает ответ в течение определенного времени, по истечению которого, если ответ не был получен, запрос будет отправлен повторно;
– RADIUS-сервер проверяет IP-адрес WLC и ключ симметричного шифрования в своем конфигурационном файле, при соответствии адреса и ключа соединение между устройствами считается установленным;
– RADIUS-сервер проверяет подлинность логина и пароля пользователя, если данные неверны, то отправляет пакет «Доступ запрещен» на WLC, содержащий код ошибки, но если данные верны, то отправляется пакет «Доступ разрешён»;
– на основе полученного ответа WLC предоставляет или запрещает доступ пользователя к сети.
Таким образом, использование в беспроводных сетях протокола RADIUS для аутентификации пользователей на базе технологии AAA является более предпочтительным, в виду гибкости, быстродействия и безопасности процесса аутентификация пользователя посредством RADIUS-сервера.

Список использованных источников:

1. Алейников, Д.И. Принципы построения безопасной инфраструктуры беспроводных сетей на базе контроллеров Cisco WLC / Д.И. Алейникова // Технические средства защиты информации: тез. докл. XIX Белорусско-российской науч.-техн. конф. / редкол.: Т.В. Борботько, [и др.]: Минск: БГУИР, 2021. – С. 15-16.
2. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=tXprJgbEWXg&list=PLQQoSBmrXmrysEaVNia7KVwf85qATIi1V&index=78 – Дата доступа: 01.04.2022
3. Ettrecap manual [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/ru_ru/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html – Дата доступа: 01.04.2022

UDC 004.056.53

AUTHENTICATION PROTOCOLS IN WIRELESS NETWORKS

Aleinikova D.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD in technical sciences, associate professor

Annotation. User authentication technologies in wireless networks are described in this research. The basic authentication, authorization and accounting protocols, their features and main differences are studied. The use of the RADIUS protocol for access control in wireless networks is analyzed.

Keywords. Wireless networks, access control, authentication, AAA, TACACS+, RADIUS.

УДК 537.531

РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ УГЛЕНАПОЛНЕННЫХ КОМПОЗИТОВ НА ОСНОВЕ СУЛЬФАТА КАЛЬЦИЯ ДЛЯ ОСЛАБЛЕНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Ахмединова Е.С.[1], студент гр. 861401

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В статье представлены результаты исследования частотных характеристик коэффициентов отражения и передачи для угленаполненных композитов на основе сульфата кальция с добавлением активированного кокосового или березового угля или неактивированного древесного угля. По результатам анализа полученных экспериментальных данных составлены рекомендации по использованию угленаполненных композитов на основе сульфата кальция с добавлением активированного кокосового или неактивированного древесного угля.

Ключевые слова. Коэффициент отражения электромагнитного излучения, коэффициент передачи электромагнитного излучения, активированный уголь, кокосовый уголь, древесный уголь, сульфат кальция, угленаполненный композит.

Для организации защиты информации о наземных объектах от добывания с помощью технических средств разведки используются методики, основанные либо на выполнении расчетов, либо на применении специальных конструкций и материалов для снижения отражения электромагнитной волны от поверхности объекта. Как правило, рабочий диапазон технических средств разведки составляет 8,2–12,4 ГГц (X диапазон). В нем функционируют не только указанные средства, но и доплеровские и метеорологические радиолокационные станции, системы передачи телевизионного изображения, радиорелейные аппараты. Использование для организации защиты информации о наземных объектах методик, основанных на применении специальных конструкций и материалов, направлено на снижение заметности этих объектов для технических средств разведки, т. е. по сути, на снижение коэффициента отражения электромагнитного излучения поверхности этих объектов в X-диапазоне.

В результате обзора современных методов скрытия объектов от средств радиолокационной разведки [1–2] установлено, что в качестве пассивных средств применяют рассеивающие и поглощающие конструкции и материалы, которые не только поглощают и ослабляют электромагнитное излучение, но и снижают коэффициент отражения.

В работе [3] автором статьи были представлены экспериментальные результаты исследования свойств ослабления и отражения электромагнитного излучения X диапазона угленаполненными композитами на основе смеси сульфата кальция и кокосового угля. Было установлено, что угленаполненный композит толщиной 30 мм характеризуется значением коэффициента отражения 9 дБ, угленаполненный композит толщиной более 50 мм – –7,5 дБ в диапазоне частот 8–12 ГГц. Значения коэффициентов передачи для образца угленаполненного композита толщиной 30 мм составляют –5,6 дБ, толщиной более 50 мм – –27 дБ в диапазоне частот 8–12 ГГц. В продолжении исследования были изготовлены образцы угленаполненных композитов на основе смеси сульфата кальция и активированного и неактивированного древесного угля толщиной от 0,3 до 1 см.

Результаты исследований, представленные в данной статье, получены в рамках научно-исследовательской работы «Разработка радиопоглощающих композиционных структур на основе порошкообразных углесодержащих материалов» по заданию № 1.5 «Разработка новых материалов и технологий для систем электромагнитной защиты радиоэлектронного и информационного оборудования, биологических объектов от воздействия широкого спектра электромагнитных излучений, обеспечения электромагнитной безопасности населения и электромагнитной совместимости электро-, радиотехнических средств и оборудования» ГПНИ «Материаловедение, новые материалы и технологии» на 2021–2025 гг.

С целью изучения изменения частотных характеристик коэффициентов отражения и передачи при добавление разного вида угля в состав угленаполненных композитов на основе смеси сульфата кальция были изготовлены образцы с добавлением активированного березового угля и неактивированного древесного угля толщиной 0,3–1 см.

На рисунке 1 представлены результаты измерения коэффициента передачи и отражения в режиме короткого замыкания с помощью панорамного измерителя SNA 0,01–18 для следующих образцов угленаполненных композитов на основе смеси сульфата:

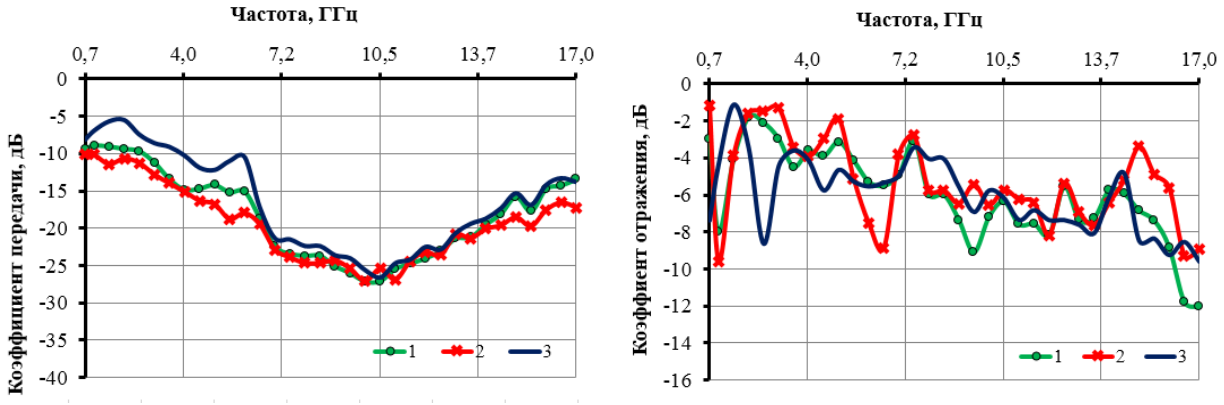
– образец с добавлением активированного кокосового угля толщиной 1 см (кривая 1);

– образец с добавлением активированного березового угля толщиной 0,5 см (кривая 2);

– образец с добавлением неактивированного древесного угля толщиной 1 см (кривая 3).

Установлено, что минимальное значение коэффициента отражения, измеренного в режиме короткого замыкания, получено для образца угленаполненного композита на основе активированного берёзового угля толщиной 0,3 см (–14 дБ) и для образца толщиной 1 см (–8,5 дБ) в диапазоне частот 4–12 ГГц, при этом коэффициент передачи для данных образцов изменяется в пределе –4,8… –11,7 дБ и –15,1… –26,9 дБ соответственно.

Коэффициент отражения ЭМИ для образца на основе неактивированного древесного угля толщиной 0,5 см, измеренный в режиме короткого замыкания, составил –4,5… –9,2 дБ, а коэффициент передачи – –3,9… –9,2 дБ в диапазоне частот 0,7–17 ГГц. У образца на основе неактивированного древесного угля толщиной 1 см коэффициент отражения изменяется в пределе –5,2… –8,1 дБ, коэффициент передачи – 9,4… –26,5 дБ.



а б

Рисунок 1 – Частотные зависимости коэффициентов отражения и передачи для образцов угленаполненных композитов на основе смеси сульфата кальция и угля

Таким образом, все образцы угленаполненных композитов на основе смеси сульфата кальция и угля толщиной более 1 см ослабляют электромагнитное излучение более чем в 100 раз, коэффициент передачи имеет значения –25… –31 дБ в диапазоне частот 7–13 ГГц. Минимальными значениями коэффициента отражения характеризуются образцы угленаполненных композитов на основе смеси сульфата кальция и активированного кокосового (–10 дБ для толщины 0,3–0,5 см) или древесного угля (–9 дБ для толщины 0,5–1 см). Также необходимо отметить, что у образцов угленаполненных композитов на основе смеси сульфата кальция и кокосового угля имеются резонансы в частотных характеристиках коэффициентов отражения, достигающих значения –8 дБ на частоте 1 ГГц при толщине образца 1 см и –12,5 дБ на частоте 2 ГГц при толщине образца 0,5 см. У образцов угленаполненных композитов на основе смеси сульфата кальция и березового угля на частотах 1 ГГц (для толщины 0,3 см) и 4 ГГц (для толщины 0,5 см) имеются резонансы частотной характеристики коэффициента отражения порядка –9,5 и –13,5 дБ соотвественно.

Изготовленные экраны могут иметь обширную сферу применения в различных отраслях. Для уменьшения электромагнитных помех и для обеспечения электромагнитной совместимости оборудования, для защиты здоровья рабочего персонала от вредного электромагнитного излучения, в медицине, для экранирования помещений, в военной деятельности и радиолокационной разведке. В радиоэкранирующей отделке зданий и помещений объектов информатизации, осуществляется покрытиями на основе применения экранирующих гипсовых смесей с добавлением угля для пола и стен в сочетании (при необходимости) с металлической

сеткой. Преимуществом использования экранов и применения данной технологии является возможность экранирования зданий и помещений любой конфигурации без нарушения архитектурного стиля и планировки. Самой важной частью является военная деятельность и скрытие объектов от средств радиолокационной разведки. Данные экраны могут использоваться для защиты радиолокационного оборудования, как покрытие на различные военные объекты (танки, самолеты), от внешних воздействий, или обеспечить скрытие объектов от радиолокационной разведки.

Список использованных источников:

1. Способ маскировки военной автомобильной техники: пат. RU2324136C2 [Электронный ресурс]. – Режим доступа: https://patents.s3.yandex.net/RU2324136C2_20080510.pdf.

2. Способ скрытия мобильного объекта от радиолокационного наблюдения из космоса: пат. RU2312297C1 [Электронный ресурс]. – Режим доступа: https://patents.s3.yandex.net/RU2312297C1_20071210.pdf.

3. Ахметдинова, Е.С. Угленаполненные композиты на основе сульфата кальция для радиоэлектронной защиты наземных объектов / Е.С. Ахметдинова, Е.С. Белоусова, О.В. Бойправ // Современные средства связи : материалы XXVI Междунар. науч.-техн. конф., 21–22 окт. 2021 года, Минск, Респ. Беларусь. – Минск : Белорусская государственная академия связи, 2021. – С. 92–93.

УДК 537.531

СИСТЕМА РАСПОЗНАВАНИЯ ЛИЦ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ

Балецкий М. И., студент гр. 861402

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук, доцент

Аннотация. Представлены основные типы и сущности методов распознавания лиц на основе нейронной сети.

Ключевые слова. Нейронная сеть, распознавание лица, оптимизация, обучение.

В настоящее время существует около десятка разновидности нейронных сетей (НС). Одним из самых широко используемых вариантов являться сеть, построенная на многослойном перцептроне, которая позволяет классифицировать поданное на вход изображение/сигнал в соответствии с предварительной настройкой/обучением сети.

Обучаются нейронные сети на наборе обучающих примеров. Суть обучения сводится к настройке весов межнейронных связей в процессе решения оптимизационной задачи методом градиентного спуска. В процессе обучения НС происходит автоматическое извлечение ключевых признаков, определение их важности и построение взаимосвязей между ними. Предполагается, что обученная НС сможет применить опыт, полученный в процессе обучения, на неизвестные образы за счет обобщающих способностей.

Наилучшие результаты в области распознавания лиц (по результатам анализа публикаций) показала Convolutional Neural Network или сверточная нейронная сеть (рисунок 1) [1-3], которая является логическим развитием идей таких архитектур нейронных сетей, как когнитрона и неокогнитрона. Успех обусловлен возможностью учета двумерной топологии изображения, в отличие от многослойного перцептрона.

Отличительными особенностями СНС являются локальные рецепторные поля (обеспечивают локальную двумерную связность нейронов), общие веса (обеспечивают детектирование некоторых черт в любом месте изображения) и иерархическая организация с пространственными сэмплингом (spatial subsampling). Благодаря этим нововведениям СНС обеспечивает частичную устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям.

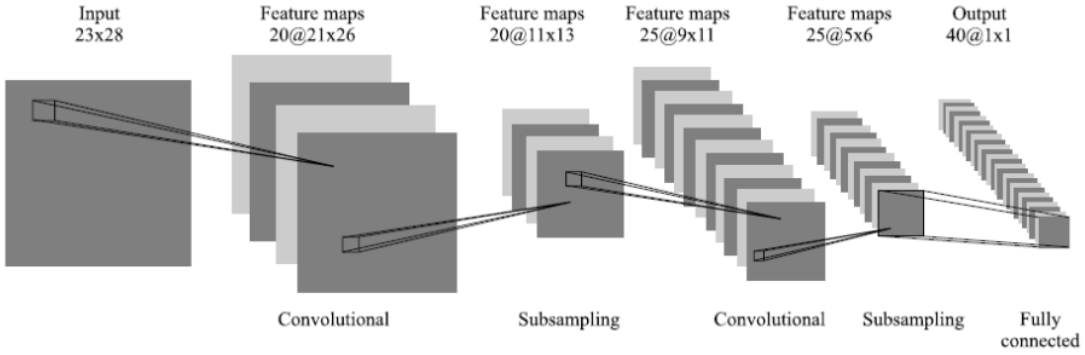


Рисунок 1 – Схематичное изображение архитектуры сверточной нейронной сети

Тестирование СНС на базе данных ORL, содержащей изображения лиц с небольшими изменениями освещения, масштаба, пространственных поворотов, положения и различными эмоциями, показало 96% точность распознавания.

Свое развитие СНС получили в разработке DeepFace [4], которую приобрел Facebook для распознавания лиц пользователей своей социальной сети (рисунок 2). Все особенности архитектуры носят закрытый характер.

Недостатки нейронных сетей: добавление нового эталонного лица в базу данных требует полного переобучения сети на всем имеющемся наборе (достаточно длительная процедура, в зависимости от размера выборки). Проблемы математического характера, связанные с обучением: попадание в локальный оптимум, выбор оптимального шага оптимизации, переобучение и т. д. Трудно формализуемый этап выбора архитектуры сети (количество нейронов, слоев, характер связей).

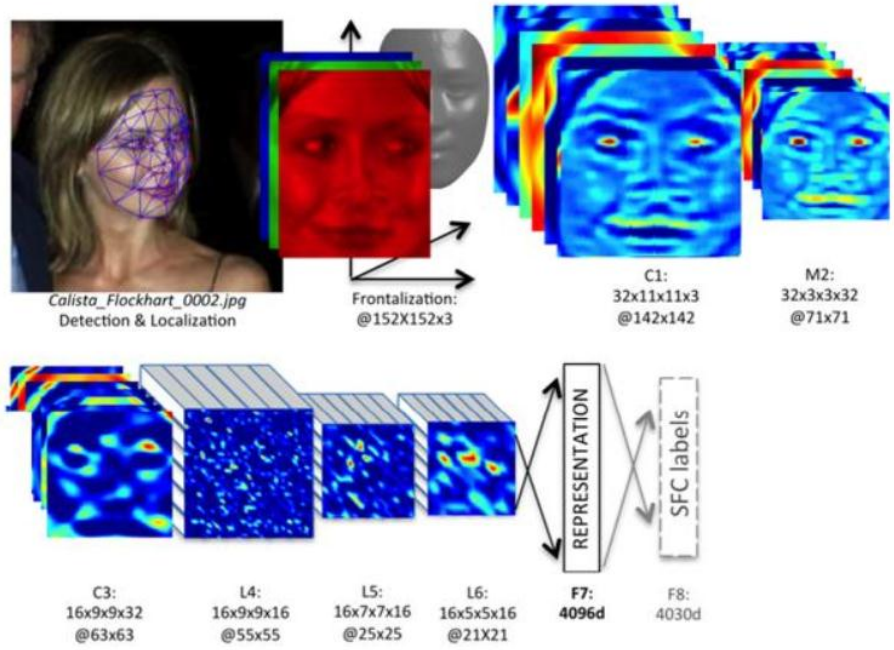


Рисунок 2 – Принцип работы DeepFace

В работе предлагается реализовать метод распознавания с использованием языка программирования Python с библиотекой OpenCV (Open Source Computer Vision Library). OpenCV - это библиотека программного обеспечения для компьютерного зрения и машинного обучения с открытым исходным кодом. Библиотека содержит более 2500 оптимизированных алгоритмов, которые включают в себя полный набор как классических, так и самых современных алгоритмов компьютерного зрения и машинного обучения.

Эти алгоритмы могут быть использованы для обнаружения и распознавания лиц, идентификации объектов, классификации действий человека на видео и многих других целей.

Чтобы построить систему распознавания лиц OpenCV будем применять глубокое обучение на двух этапах: распознавание лиц, которое обнаруживает присутствие и местоположение лица на изображении, но не идентифицирует его; извлечение 128-разрядных векторов признаков, которые количественно определяют каждое лицо в образе. Для работы с массивами данных используется язык программирования Python, включая библиотеку scikit-learn для извлечения объектов из набора данных

Проект включает 3 этапа:

– Распознавание лиц и сбор данных.

– Обучение распознавателя.

– Распознавание лиц..

Создается набор данных (датасет), в котором хранятся группы фотографий серого цвета с той частью, которая использовалась для распознавания лиц. Набор из 30 выборок для каждого идентификатора можно считать оптимальным.

На этапе обучения берутся все пользовательские данные из набора данных и библиотеки OpenCV – Recognizer instructor. Это делается с помощью специальной функции OpenCV. Чтобы обучить модель распознавания лиц с помощью глубокого обучения, каждая выборка данных включает в себя три изображения: якорь (текущее лицо); положительное изображение (изображение человека с той же идентичностью, что и якорь); отрицательное изображение (не имеет той же идентификации, что и якорь). Нейронная сеть вычисляет 128-мерный вектор признаков для каждой изображения грани,

а затем настраивает веса сети. На этапе распознавания распознаватель (Recognizer) выполнит обработку.

Список использованных источников:

[1] Face Recognition A Convolutional Neural Network Approach [Электронный ресурс]. – Режим доступа: https://clgiles.ist.psu.edu/papers/IEEE.TNN.face.recognition.hybrid.nn.pdf

[2] Face Recognition using Convolutional Neural Network and Simple Logistic Classifier [Электронный ресурс]. – Режим доступа: https://dap.vsb.cz/wsc17conf/Media/Default/Page/online_ wsc17_submission_59.pdf

[3] Face Image Analysis With Convolutional Neural Networks [Электронный ресурс]. – Режим доступа: https://lmb.informatik.uni-freiburg.de/papers/download/du_diss.pdf

[4] DeepFace Closing the Gap to Human-Level Performance in Face Verification [Электронный ресурс]. – Режим доступа: https://www.cv-foundation.org/openaccess/content_cvpr_2014/papers/Taigman_ DeepFace_Closing_the_2014_CVPR_paper.pdf

УДК 537.531

УСОВЕРШЕНСТВОВАНИЕ ВХОДНОГО ТРАКТА ШИРОКОПОЛОСНОГО РАДИОПРИЕМНИКА ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ СВЧ ДИАПАЗОНА

Булавко Д.Г., Лисов Д.А., Кузюков А.Н.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Гусинский А.В. – канд. технических наук, доцент

Показаны пути усовершенствования входного тракта широкополосного приемника измерительной системы СВЧ диапазона позволяющее защитить входные каскады приемника от выхода из строя при приеме сигналов с большим уровнем мощности, а также обнаруживать сигналы, разнесенные по частоте и непостоянных во времени.

В настоящее время приемо-передающие устройства различных радиоэлектронных систем развиваются в направлении смещения несущих частот в область СВЧ частот и использования широкополосных сигналов. Это влечет за собой дополнительные сложности при проектировании входных каскадов, преселекторов, каскадов усиления и схем частотного преобразования радиоприемника.

В статье приводится описание путей усовершенствования входного тракта широкополосного радиоприемника измерительной системы СВЧ диапазона позволяющих решить проблемы защиты входных цепей приемника от мощных входных сигналов и оперативного реагирования на сигналы, поступающие на приемник.

К широкополосным радиоприемникам СВЧ диапазона помимо типовых требований, таких как высокая чувствительность, широкий диапазон частот входного сигнала, широкая полоса частоты, большой динамический диапазон, невысокий коэффициент шума тракта, предъявляется и ряд других требований. К наиболее важным из них следует отнести уменьшение времени перестройки по частоте для поиска полезного сигнала на входе радиоприемника, минимизация пропусков импульсов полезных сигналов малой длительности, возможность обнаружения других сигналов, появляющихся на входе приемника во время приема и обработки сигнала определенной частоты. Так же необходимо предусмотреть меры по защите входных каскадов приемника от выхода из строя при приеме сигналов с большим уровнем мощности и значительного увеличения нелинейных искажений при приеме таких сигналов.

Для решения указанных выше задач предлагается изменить структуру входного тракта приемника как показано на рисунке 1.

На входе классической схемы обычно используют малошумящий усилитель (МШУ), который в зависимости от типа имеет коэффициент шума порядка 1-3 дБ. Так же на входе приемного тракта возможно размещение частотного преселектора, что позволяет обеспечить приемлемую защиту входных каскадов, однако отрицательно влияет на коэффициент шума приемника. В таких схемах он достигает значение порядка 10-15 дБ. Два описанных подхода не дают полной защиты приемника в комплексе с приемлемым коэффициентом шума.

В предложенной схеме на входе приемника размещается ограничитель мощности, СВЧ ключ, широкополосный МШУ и направленный ответвитель. Ограничитель мощности имеет следующие характеристики: максимальная входная мощность 5 Вт, уровень компрессии 18 дБм, уровень вносимых потерь – не более 1,2 дБ. СВЧ ключ имеет следующие характеристики: максимальная входная мощность 24 дБм, уровень вносимых потерь – не более1,7 дБ. Широкополосный МШУ – максимальная входная мощность 17 дБм, усиление сигналов в полосе частот 2-18 ГГц – не менее 17,5 дБ, коэффициент шума – не более 3 дБ. Направленный ответвитель – вносимые потери не более 1,7 дБ, переходное ослабление минус 10 дБ.

Ключ СВЧ служит для двух целей. Первая – тестовый режим, вторая – защитный режим. В тестовом режиме он по внешней команде подключает внутренний генератор, управляемый напряжением (ГУН) с известным откалиброванным значением уровня мощности на частоте 4860 МГц и на первых двух гармониках 9720 МГц и 14580 МГц соответственно к МШУ. Этот режим работы позволяет производить внутреннее тестирования и калибровку приемника. В защитном режиме в основной

тракт радиоприемника вносится ослабление порядка 50-60 дБ, что позволяет защитить последующие каскады.

Со вторичного канала направленного ответвителя часть сигнала из основного тракта поступает через МШУ и делитель мощности на детектор защиты и три вспомогательных канала. Каждый канал содержит полосовые фильтры соответственно на полосы частот: 2-8 ГГц, 8-12 ГГц, 12-18 ГГц, управляемый аттенюатор, усилитель мощности и быстродействующий детектор. С помощью этих каналов реализуется возможность обнаружения кратковременных импульсов сигналов на входе приемника и сужается частотный диапазон поиска этого сигнала для дальнейшего его исследования.

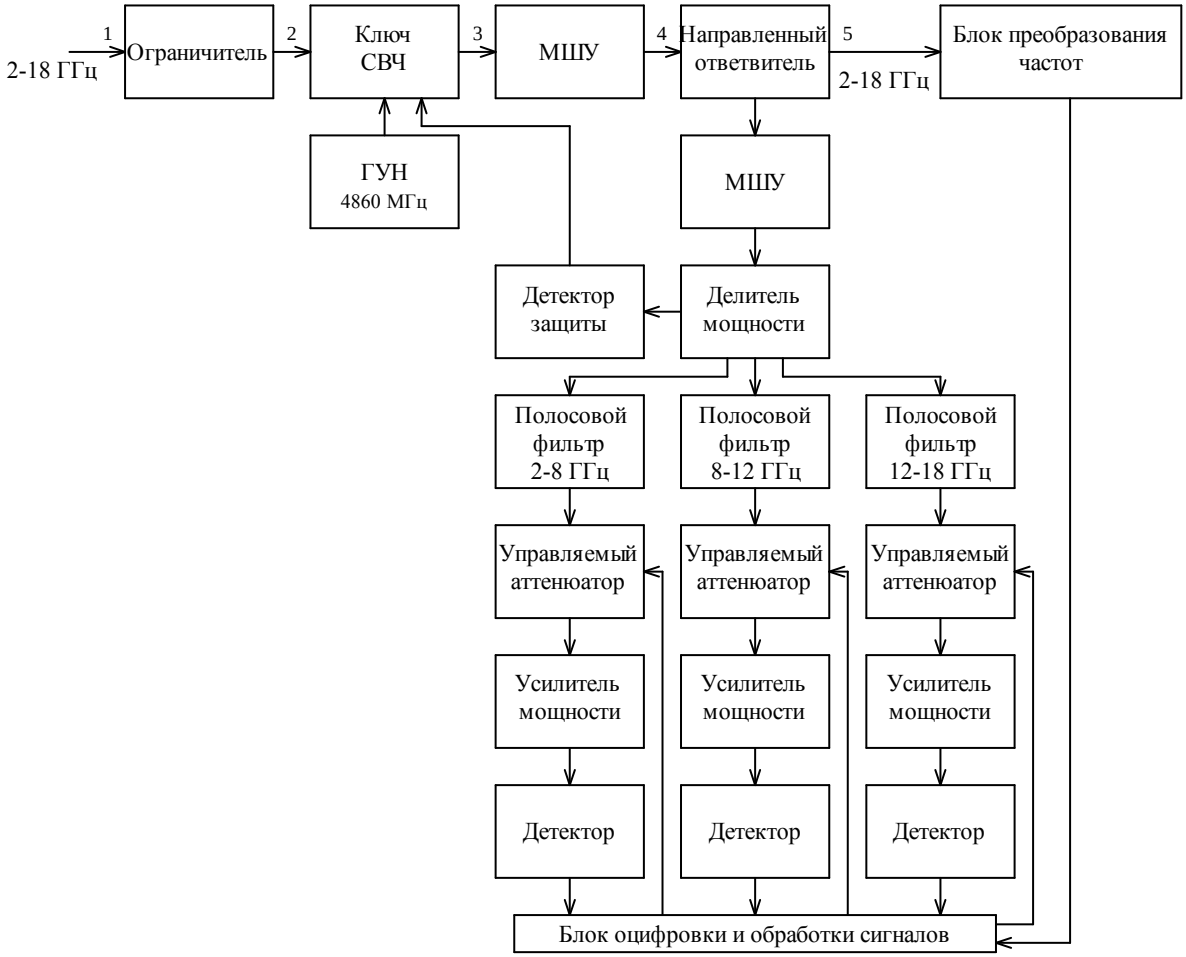


Рисунок 1 – Структурная схема входного тракта широкополосного приемника

На детектор защиты подается сигнал без предварительной фильтрации, и при его уровне более 10 дБм выдается сигнал на ключ СВЧ для перехода его в защитный режим.

Введение дополнительных компонентов во входной тракт радиоприемника несколько увеличивается коэффициент шума (до 6 дБ, как показано на рисунке 2), однако частотный и динамические диапазоны не ухудшаются.

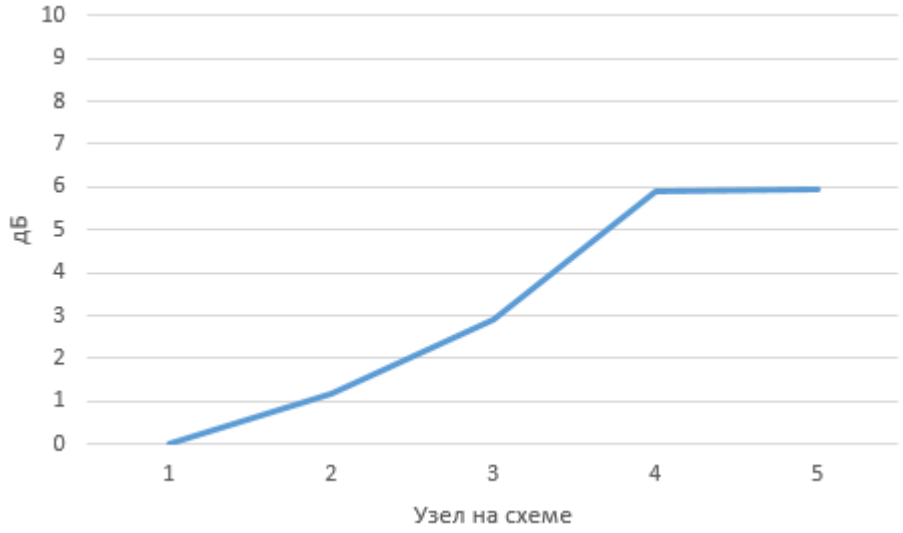


Рисунок 2 – График зависимости коэффициента шума входного тракта радиоприемника

Описанные выше пути усовершенствования входного тракта широкополосного радиоприемника СВЧ диапазона позволяют решить задачи обнаружения сигналов, разнесенных по частоте и непостоянных во времени, а также защитить входные каскады приемника от выхода из строя при приеме сигналов с большим уровнем мощности. Схема приемника при этом несколько усложняется, а также незначительно увеличивается коэффициент шума.

УДК 004.732 (076.5)

ОСОБЕННОСТИ ИЗУЧЕНИЯ ПРИНЦИПОВ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ В СИМУЛЯТОРАХ CISCO И ENSP

Дедюль П.Ю., студент гр 961401

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. технических наук

Аннотация. В данной работе были исследованы отличия симуляторов Packet Tracer и eNSP, также реализована простейшая сеть на основе чего выделены отличия синтаксиса команд данных симуляторов сетевого оборудования.

Ключевые слова. компьютерная сеть, симулятор, сетевое оборудование, среда разработки, синтаксис команд.

До недавнего времени по многим специальностям первой ступени высшего образования и курсах повышения квалификации изучение принципов коммутации и маршрутизации осуществляется на основе материалов академии Cisco. Однако в виду изменения экономических взаимоотношений стран СНГ и США возникли сложности с доступом к учебному материалу Cisco, закупке оборудования данной компании для оснащения компьютерных классов. Наиболее альтернативным вариантом для изучения конфигурации сетевого оборудования является продукция компании Huawei, за счет своей относительно низкой стоимости и возможности приобретения. Соответственно необходимо внедрять в учебный процесс изучение симулятора данного оборудования, а именно симулятор eNSP.

В данной статье рассмотрены следующие вопросы: особенности установки и использования в учебном процессе симуляторов Cisco и eNSP, различия их интерфейсов, возможность изучения принципов конфигурации разного типа оборудования, отличия синтаксиса команд.

В начале изучения среды eNSP автор статьи столкнулась с проблемой совместимости оборудования и сложностью установки симулятора eNSP [1]. Для активации программы требуется установить не только eNSP, но и сторонние программы такие как библиотеку WinPcap 4.1.3, сетевой анализатор Wireshark и Oracle VM VirtualBox. Сложности возникают при установке библиотеки WinPcap 4.1.3: разработка данного проекта прекращена, а WinPcap больше не поддерживаются. Так же производитель предупреждает о возможных ошибках в работе с последней доступной версией. Еще одна сложность при загрузке симулятора eNSP это необходимость устанавливать дополнительные программы в определенном порядке, для правильного функционирования симулятора. Также при установке Oracle VM VirtualBox следует обратить внимание на версию симулятора eNSP. При запуске система может выдать сообщение об ошибке о том, что версия Oracle VM VirtualBox не поддерживается, в этом случае рекомендуется обновить VirtualBox, но не рекомендуется ставить версию VirtualBox 6 и выше.

После успешной установки симулятора eNSP необходимо изучить его интерфейс. На рисунке 1 представлен интерфейс с пояснениями: 1 – панель выбора типа оборудования; 2 – выбор вида сетевого оборудования; 3 – панель инструментов; 4 – рабочая зона для создания сети.

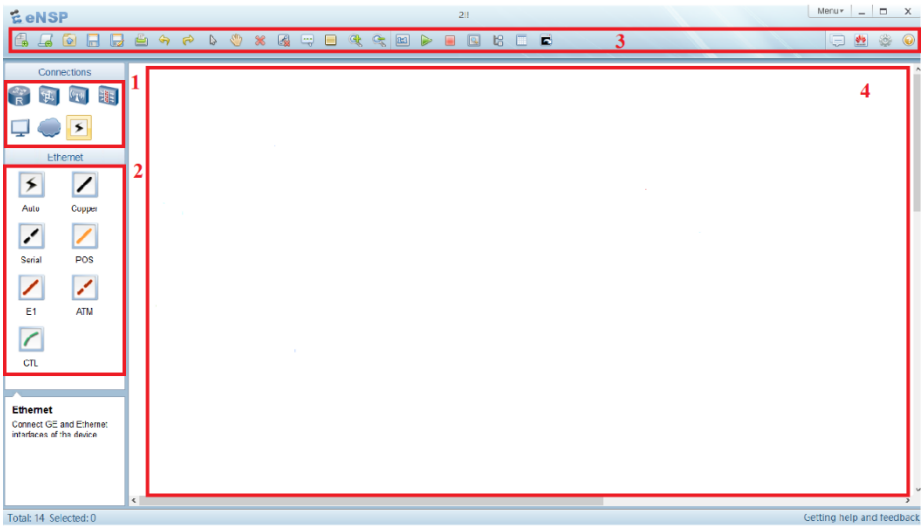


Рисунок 2 – Внешний вид интерфейса симулятора eNSP

Интерфейс симулятора eNSP аналогичен рабочему пространству Cisco Packet Tracer, за исключением расположениях некоторых элементов, что не вызывает трудностей при его изучении.

При изучении разнообразия оборудования в симуляторах Cisco и eNSP замечено, что в симуляторе eNSP небольшой выбор маршрутизаторов (серия AR: 201, 1220, 2220, 2240, 3260); коммутаторов (серия S: 5700, 3700, 5700-28C-HI); беспроводных устройств, среди которых только одна вариация точки доступа, без возможности выбора разных диапазонов частот. А также различные оконечные устройства, межсетевые экраны и устройства для облачных технологий. Однако разнообразие сетевого оборудования в симуляторе оборудования Cisco значительно больше, например, там представлены маршрутизаторы большего количества линеек компании, выполняющие самые разные функции, что удобнее при проектировании реальных компьютерных сетей.

Изучая различия симуляторов невозможно не заметить различия в синтаксисе команд, которые выполняют аналогичные функции. В таблице 1 приведены различия команд необходимых для простейшей настройки сети.

Таблица 1– различия команд в разных симуляторах сетевого оборудования

Назначение команды	Симулятор Cisco	eNSP
Просмотр настроек	Show	Display
Переход в режим глобальной конфигурации(сетевой режим)	Configure terminal	System-view
Выход из данного режима симуляции	Exit	Quit
Отмена настроек	No	Undo
Перезагрузка устройств	Reload	Reboot
Просмотр таблицы маршрутизации	Show ip route	Display ip routing-table
Очистить/ перезапустить процесс	Clear	Reset
Команда для настройки пароля	Enable secret	Authentification pass cipher
Сброс настроек интерфейса	Clear interface	Reset counters interface

Административное выключение/включение интерфейса	Shutdown/ no shutdown	Shutdown/ undo shutdown
Сохранение текущей конфигурации устройства в стартовую	Copy running-configure	Save
Настройка статической маршрутизации	Ip route	Ip route-static

Помимо различия синтаксиса команд есть и сходства конфигурирования. Так, например, для задания IP-адреса интерфейсу необходимо прописать в системном режиме команду *ip address <адрес интерфейса> <маска подсети>.* [2]

Необходимо отметить, что при конфигурировании сетевого оборудования в симуляторе eNSP необходимо сохранять текущую конфигурацию в стартовую, командой *save* в противном случае все настройки данного устройства сбросятся до настроек по умолчанию. Когда в Cisco Packet Tracer аннулируются далеко не все настройки, однако пренебрегать сохранением конфигурации в симуляторе Cisco не следует.

На основе изучения интерфейса симулятора eNSP и синтаксиса команд для конфигурации оборудования Huawei была реализована простейшая сеть.

Таким образом, можно сделать вывод, что при переходе на оборудование компании Huawei с использованием симулятора eNSP необходимо учитывать особенности именного этой среды, однако для опытного администратора многие отличия являются не существенными. Так как принцип работы и построения топологий в симуляторах Packet Tracer и eNSP не отличается. Каждый из представленных программных продуктов имеет свои достоинства и недостатки на всех этапах работы с данными средами разработки. Что касается учебного процесса: существенным плюсом симулятора eNSP является его полностью бесплатное распространение, понятный графический интерфейс и возможность реализации всех основных настроек компьютерных сетей.

Список используемых источников:

1. Huawei [Электронный ресурс]. – Режим доступа: https://forum.huawei.com/enterprise/en/resource-downloading-for-ensp/thread/750163-861

2. Wordpress [Электронный ресурс]. – Режим доступа: https://khlebalin.wordpress.com/2019/05/08/%D1%81%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4-cisco-huawei/amp/

УДК 004.056

ПРОГРАММНЫЙ МОДУЛЬ ВЫДЕЛЕНИЯ РАДУЖНОЙ ОБОЛОЧКИ ГЛАЗА НА ИЗОБРАЖЕНИИ

Ибрагимов И.В.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Предложен модуль выделения радужной оболочки глаза на изображении, позволяющий выявить и отделить радужную оболочку на изображении. Данный модуль позволяет работать с изображениями разных форматов и размеров.

Задачей работы была разработка программного модуля выделения радужки на фотоснимке для дальнейшей обработки и построения системы распознавания человека. Данный метод биометрической идентификации личности основывается на уникальных характерных признаках и особенностях радужной оболочки человеческого глаза.

Выделение радужки на изображении, по сути, является поиском на изображении относительно темного объекта, близкого по форме к кругу, содержащего внутри себя концентрический еще более темный объект (зрачок). В большинстве систем добавляется еще одно условие: внутри зрачка должен находиться яркий блик определенной формы (блик от осветителя). Данная задача может быть решена многими способами, например, поиск концентрических окружностей посредством преобразования Хафа, или использования коррелятора для поиска блика заданной формы с последующим обнаружением контуров содержащего этот блик зрачка и далее концентрической зрачку радужки [1]. Специфичным является наличие век, в большинстве случаев закрывающих верхнюю и нижнюю части радужки. Некоторые системы, например Iridian, выделяют веки явным образом и отбрасывают ложные данные с закрытых участков.

В результате выполнения работы был разработан программный модуль выделения радужной оболочки глаза на изображении. Работа данного модуля состоит из следующих основных этапов.

1. Эрозия изображения. Позволяет усилить границу перехода яркости на изображении и сделать контур радужной оболочки более четким.

2. Медианная фильтрация. Используется для уменьшения шума в изображении, в частности вокруг контура радужной оболочки.

3. Бинаризация методом выделения границ Canny. Позволяет получить контуры радужной оболочки.

4. Выделение окружностей с помощью алгоритма Хафа [2].

Программный модуль был реализован на языке программирования C++ в среде Visual Studio с использованием библиотеки ltilib. Пример результата работы модуля представлен на рисунке 1.

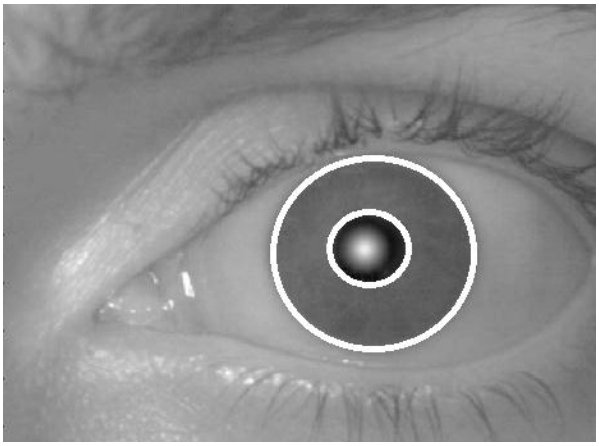


Рисунок 1 – Пример результата работы модуля выделения радужной оболочки глаза на изображении

Данный модуль позволяет работать с изображениями разных форматов, таких как bmp, jpeg, и разных размеров.

Список использованных источников:

1. Р. Гонсалес, Р. Вудс “Цифровая обработка изображений”, Москва Техносфера 2005.

2. Olivier Ecabert, Jean-Philippe Thiran, "Adaptive Hough transform for the detection of natural shapes under weak affine transformations" Pattern Recognition Letters (25).

УДК 004.056

СОПОСТАВЛЕНИЕ ПОПУЛЯРНОГО СОФТА ДЛЯ ОРГАНИЗАЦИИ ЗАШИФРОВАННЫХ КРИПТОКОНТЕЙНЕРОВ

Калько А.И., аспирант

Барановичский государственный университет

г.Барановичи, Республика Беларусь

Бобов М.Н. – док. тех. наук, профессор

Аннотация. В данной статье рассмотрено сравнение криптоконтейнеров TrueCrypt и VeraCrypt. Требовались достаточно надежные, но при этом легкодоступные криптографические алгоритмы. Долгое время востребованная в большей степени в военной среде, теперь криптография широко используется в дипломатической, коммерческой, банковской, государственной и иных сферах.

Ключевые слова: криптоконтейнеры, TrueCrypt, VeraCrypt, шифрование

Введение. На сегодняшний день тема конфиденциальности и защиты данных является наиболее актуальной и широко обсуждаемой. Одним из способов хранения наиболее ценной информации является использование криптоконтейнеров (от английского Crypt — шифровать). Сейчас на информационном пространстве существует достаточно большое множество программного обеспечения на различные платформы для создания зашифрованных контейнеров. Наиболее известными среди них являются TrueCrypt, VeraCrypt и Bitlocker. Среди менее известных аналогов вышеперечисленных можно выделить AxCrypt, DiskCryptor, FreeOTFE, Cryptic Disk. В данной статье будет произведено объективное сравнение TrueCrypt и VeraCrypt, описаны преимущества и недостатки каждого программного обеспечения.

Основная часть. Прежде чем начать сравнение, познакомимся с довольно интересной и загадочной историей TrueCrypt.

Первая версия была выпущена в 2004 году, и в то время TruCrypt была единственной программой шифрования сценариев Quick Go с открытым исходным кодом. С 2004 по 2014 год TruCrypt регуля рно обновлялся. Некоторые функции были исключены. Например, была удалена поддержка гибких дисков и некоторых протоколов шифрования. Поэтому в последней и седьмой версиях TrueCrypt б ыли удалены криптографические протоколы, использующие 64-битный (Тройной DES, Blowfish, CAST5).

За десять лет проект TrueCrypt был разработан и преобразован в надежную систему защиты данн ых. Все это время имена разработчиков программы держались в секрете, что привело к появлению ряда слухов об участии частных сервисов в разработке приложения. Одни говорят, что программа была разработана ФБР, другие говорят, что если бы не ФБР, в программе обязательно были бы ф ичи и баги.

Популярность TrueCrypt росла до беспрецедентного события весной 2014 года. Проект TrueCrypt закрылся 28 мая 2014 года. Точные причины закрытия проекта пока не раскрываются. Сами разработчики заявили на официальном сайте, что использование TrueCrypt небезопасно, они рекомендуют перейти на BitLocker, над которым всегда высмеивают.

Есть 4 версии случившегося. Первая гласит, что разработчикам угрожали спецслужбы. Во-вторых, они были склонны работать на Microsoft, как объясняется в объявлении BitLocker. В-третьих, они устали продвигать l Поддерживать проект, который не приносит денег. В-четвертых, они обнаружили потенциальную уязвимость системы безопасности в продукте, которую не смогли устранить.

Интернет-сообщество вступило в дебаты по поводу безопасности TrueCrypt, и в начале апреля 2015 года был завершен независимый аудит TrueCrypt, на который было пожертвовано более 60 000 долларов США. Он не выявил никаких дыр в безопасности или серьезных недостатков в архитектуре приложения и продемонстрировал, что TrueCrypt - это хорошо разработанная программа шифрования.

В 2013 году французский разработчик Мунир Идрасси летом 2013 года представил миру проект IraCrypt - самый популярный форк TrueCrypt на сегодняшний день. Форк (от англ. Fork - форк, форк) или форк - использует кодовую базу программного проекта как начало другого проекта, при этом основной проект продолжает или прекращает свое существование [1]. Разветвленный или разветвленный проект может поддерживать контент и делиться с ним основным проектом, либо он может приобретать совершенно другие функции, не имея ничего общего с исходным проектом. Основная идея заключалась в создании более безопасного решения TrueCrypt.

Особенности TrackCrypt и отличия от TrueCrypt [2]:

1. TrueCrypt выполнил недостаточное количество итераций для PBKDF2 (стандарт генерации паролей для ключа шифрования), количество дубликатов системного раздела в VeraCrypt увеличилось с 1000 до 327 661, а для других разделов и держателей файлов с 2000 до 655 331, т. е. ключ сопротивления значительно увеличился.

2. IraCrypt исправил ошибки, улучшил загрузчик и позволил использовать алгоритм SHA-256 в качестве хэш-функции при шифровании системного раздела жесткого диска, в то время как TrueCrypt использовал менее надежный алгоритм RIPEMD-160.

3. Драйверы VeraCrypt имеют цифровую подпись Microsoft, которая необходима для правильной установки в Windows 10.

4. Версии 1.18 и более ранние позволяют переводить компьютеры с Windows с использованием UEFI вместо BIOS и устранять риски, связанные с отображением скрытых разделов.

5. Начиная с версии 1.0f, IraCrypt поддерживает множество разделов и контейнеров, включенных в TrueCrypt, а также возможность конвертировать скрытые индексы TrueCrypt и недисковые разделы в форматы IraCrypt.

6. Исправлено множество программных ошибок: утечка памяти, перегрузка из-за ошибок и загрузка dll.

7. Был проведен полный анализ и рефакторинг кода.

8. Доступны версии для MACOS и Linux.

Сравнение VeraCrypt и TrueCrypt:

Скорость шифрования и дешифрования криптоконтейнеров. Тесты проводились на ноутбуке с процессором Intel Core i3-8600(2.0GHz, 3MB L3 Cache), 16GB Ram и 128GB SSD с операционной системой Windows 10 Профессиональная Service Pack 3. На рисунках 1 и 2 представлены результаты тестов скорости алгоритмов шифрования.

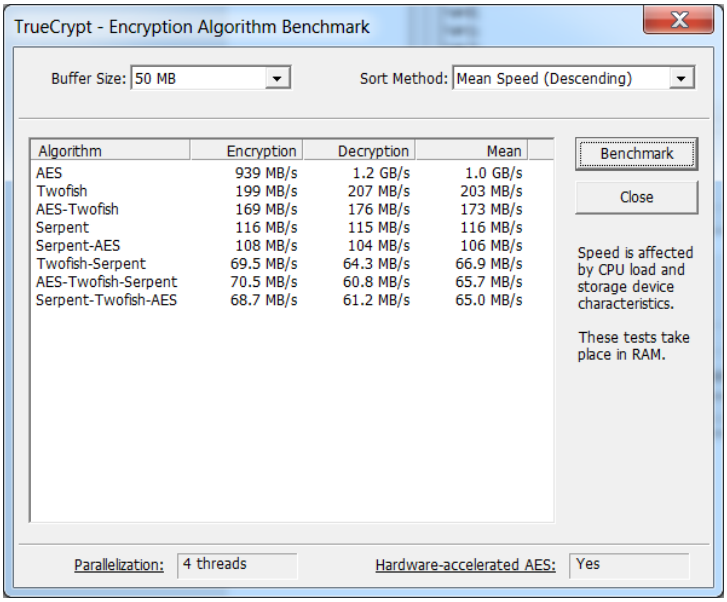


Рисунок 1 – Тест скорости алгоритмов шифрования TrueCrypt

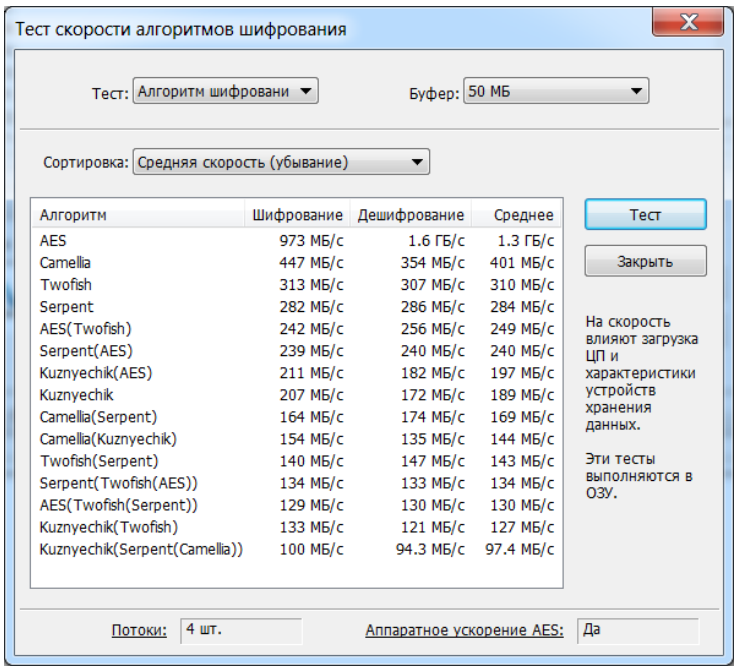


Рисунок 2 – Тест скорости алгоритмов шифрования VeraCrypt

Как можно видеть из результатов тестов, большинство алгоритмов работают быстрее в VeraCrypt. Также можно отметить и более широкий набор алгоритмов в VeraCrypt, чем в TrueCrypt.

Уязвимости. 13 марта 2015 года на сайте Open Crypto Audit Project был опубликован финальный отчет о проведении аудита TrueCrypt. Результаты отображены на рисунке 3.

Application Summary	
Application Name	TrueCrypt
Application Version	7.1a
Application Type	Disk encryption software
Platform	Windows, C / C++

Engagement Summary	
Engineers Engaged	Three (3)
Engagement Type	Cryptographic Review
Testing Methodology	Source Code Review

Vulnerability Summary	
Total High severity issues	2
Total Medium severity issues	0
Total Low severity issues	1
Total Undetermined severity issues	1
Total vulnerabilities identified:	4

See section 3.1 on page 10 for descriptions of these classifications.

Category Breakdown:	
Access Controls	0
Auditing and Logging	0
Authentication	0
Configuration	0
Cryptography	4
Data Exposure	0
Data Validation	0
Denial of Service	0
Error Reporting	0
Patching	0
Session Management	0
Timing	0

Рисунок 3 – Результаты аудита TrueCrypt

В результате было выявлено 4 уязвимости, связаных с математической защитой данных: 2 уязвимости тяжелой сложности, 1 уязвимость средней сложности и 1 незначительная уязвимость.

В сентябре 2016 года команда Quarkslab провела аудит VeraCrypt, в ходе которого было выявлено 36 весовых коэффициентов, из которых 8 были оценены как критические, 3 - как посредники и 15 - как малые веса. Большинство проблем затрагивает сторонние библиотеки сжатия с загрузчиком VeraCrypt UEFI [3]. Наиболее важным фактором риска является загрузчик UEFI, который позволяет восстановить содержимое загрузочного пароля. Разработчики VeraCrypt адаптировали большинство проблем, выявленных при проверке в VeraCrypt 1.19.

Из вышеперечисленных результатов следует, что уровень команды разработчиков TrueCrypt намного выше, нежели VeraCrypt.

Устойчивость к брутфорсу. Благодаря передовому методу генерации ключей VeraCrypt в 10–300 раз более устойчив к атакам с применением насилия.

Быстрая установка контейнеров шифрования. Когда пользователь указывает правильный пароль в TrueCrypt, время ожидания перед доступом к зашифрованным данным на современном компьютере составляет одну десятую секунды. С iracrypt вам придется подождать еще немного [4].

Поддержка разработчиков. TrueCript больше не поддерживается разработчиками, используемые решения устаревают каждый день, а потенциальные уязвимости безопасности не исправляются. Это определенно плюс для VeraCript, который активно поддерживается и развивается.

Заключение. Проанализировав оба инструмента для создания криптоконтейнеров, можно отметить, что каждый имеет как свои преимущеста, так и свои недостатки. Однозначно определить победителя затруднительно. По этой причине некоторые специалисты по информационной

безопасности рекомендуют использовать оба инструмента. К примеру, создание криптоконтейнера TrueCrypt, в него положить криптоконтейнер VeraCrypt, а уже в нем размещать данные. Такая связка в разы надежнее каждой из программ в отдельности.

Список использованных источников:

1. The VeraCrypt Audit Results. URL: https://ostif.org/the-veracrypt-audit-results/ (дата обращения: 13.03.2022)
2. Balducci, A. Open Crypto Audit Project TrueCrypt: Cryptographic Review. NCC Group, Inc, 2015. – 20 с.
3. Сандруцкий Д. И., Колдушко С. Д., Калько А. И. Применение криптографических систем при создании мессенджера //Студенческий. – 2017. – №. 16. – С. 14-16.
4. Сандруцкий, Д. И. Криптографические сервисы Java / Д. И. Сандруцкий, С. Д. Колдушко, А. И. Калько // Содружество наук. Барановичи-2017 : материалы XIII Междунар. науч.-практ. конф. молодых исследователей, Барановичи, 18 мая 2017 г. : в 3 ч. / М-во образования Респ. Беларусь, Барановичский гос. ун-т ; редкол.: В. В. Климук (гл. ред.) [и др.]. – Барановичи : БарГУ, 2017. – Ч. 2. – С. 130–133.

UDC 004.056

MAPPING OF POPULAR SOFTWARE FOR ORGANIZATION OF ENCRYPTED CRYPTOCONTAINERS

A.I. Kalko, PhD student

Baranavichy State University

Baranovichi, Republic of Belarus

M.N. Bobov - doc. those. sciences, professor

Annotation. This article discusses the comparison of TrueCrypt and VeraCrypt crypto containers. Rather reliable, but easily accessible cryptographic algorithms were required. For a long time in demand more in the military environment, now cryptography is widely used in diplomatic, commercial, banking, state and other spheres.

Keywords: cryptocontainers, TrueCrypt, VeraCrypt, encryption

УДК 330.4:330.46

ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ VPN-СЕРВИСА

Капусто Р.А., магистрант гр. 167241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В работе приведены статистические данные использования VPN-сервисов; выделены основные показатели безопасности VPN-сервисов; приведено краткое описание каждого показателя.

Ключевые слова. Технология VPN, KillSwitch, утечка персональных данных, утечка DNS.

Согласно отчету портала security.org за 2021 год [1], 85 % респондентов знают, что такое технология VPN (Virtual Private Network), и 41 % использует VPN в личных или рабочих целях. Основной целью использования технологии более чем половины участников опроса является общая безопасность использования сети Интернет и приватность. При этом из тех, кому VPN нужен не для работы, 41 % доверяет бесплатным сервисам.

Некоторые бесплатные VPN-сервисы экономят на инфраструктуре и конфиденциальности пользователей. Халатность и беспечность в вопросе безопасности приводит к утечке персональных данных пользователей [2]. Также некоторые VPN-провайдеры собирают клиентскую информацию на продажу третьим лицам, рекламодателям [3].

К основным показателям безопасности, характеризующим заслуживающий доверия VPN-сервис, относятся: надежный VPN-протокол, отсутствие отслеживания данных, отсутствие утечек адресов, отсутствие утечек DNS и поддержка KillSwitch.

VPN-протокол является базисом безопасности VPN-соединения. Протокол должен быть проверен временем, не должен иметь известных уязвимостей. Важно, чтобы он обеспечивал надежное шифрование передаваемых данных. Поэтому следует обращать внимание, какой протокол использует VPN-сервис. Например, протоколы L2TP/IPsec и PPTP считаются устаревшими, поэтому рекомендуется использовать OpenVPN или WireGuard.

Интернет-трафик, передаваемый по VPN-туннелю, зашифрован и маршрутизируется через VPN-сервер, поэтому интернет-активность остаётся скрытой от провайдера. При этом компания, контролирующая сервер, может видеть трафик и распоряжаться им по своему усмотрению. VPN-сервис со строгой политикой поможет уберечь личные данные от отслеживания.

Одна из функций VPN-сервиса является скрытие реального IP-адрес. Утечка данной информации приводит к нарушению конфиденциальности, поскольку раскрывает местоположение пользователя. VPN-сервис может стать виновником утечки в том случае, если он не поддерживает IPv6. В случае использования веб-ресурсом IPv4-адресации проблем не возникает, однако когда пользователь пытается зайти на ресурс, работающий по протоколу IPv6, VPN-сервис не может создать туннель для запроса, и браузер отправляет данные без скрытия IP-адреса.

Если VPN-сервис не поддерживают проверку DNS-запросов клиента, то происходит «утечка DNS». В таком случае интернет-провайдер или оператор DNS-сервера получают информацию о посещаемых веб-сайтах и используемых приложениям. У многих VPN-провайдеров есть собственные выделенные DNS-серверы. Важно при использовании VPN-сервиса проверить, что нет возможности отправлять DNS-запросы за пределами VPN-туннеля или через VPN-туннель, но на сторонний сервер.

KillSwitch – это функция экстренного разрыва интернет-соединения в случае непредвиденной потери VPN-соединения. Это значит, что не произойдёт утечка адресов или DNS и, как следствие, утечка персональных данных, если VPN резко перестанет работать.

Таким образом, проведенный анализ показателей безопасности VPN-сервисов показал, что приватность и конфиденциальность в сети обеспечивается не самим фактом использования VPN, но его качеством. Выбор надежного VPN-провайдера является важной задачей.

Список использованных источников:

1. VPN Consumer Usage, Adoption, and Shopping Study: 2021 [Электронный ресурс]. – 2021. – Режим доступа: https://www.security.org/resources/vpn-consumer-report-annual/.

2. Breaking News: 45 Million VPN User Records Have Been Leaked [Электронный ресурс]. – 2021. – Режим доступа: https://www.vpnunlimited.com/blog/freevpn-dashvpn-leak.

3. How FREE VPNs Sell Your Data | TheBestVPN.com [Электронный ресурс]. – 2018. – Режим доступа: https://thebestvpn.com/how-free-vpns-sell-your-data/.

УДК 330.4:330.46

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОЦЕССА ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Касьян А.С.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Бойправ О.В. – канд. техн. наук

Современные информационные системы (ИС) не могут работать изолированно. Взаимодействие между ИС – важная часть жизненного цикла каждой из них. Одним из требований, предъявляемым к такому взаимодействию, – его безопасность. Безопасность может быть реализована на уровне межсетевых коммуникаций или на уровне сервисов и приложений. Первое является более фундаментальным аспектом защищённого взаимодействия и поэтому всё внимание в рамках данной работы будет уделено именно ему.

Большинство угроз, реализуемых на уровне сетевого взаимодействия ИС, связаны с перехватом сетевого трафика и просмотром его содержимого или подменой доверенного участника взаимодействия. В результате чего нарушаются такие аспекты информационной безопасности (ИБ), как конфиденциальность и подлинность (неразрывно связано с целостностью) информации. В рамках противодействия нарушению этих аспектов ИБ, были разработаны специализированные протоколы безопасности сетевого взаимодействия.

Основными протоколами обеспечения безопасности процесса взаимодействия информационных систем являются SSH, IPsec и SSL/TLS. Сравнение данных протоколов приведено в таблице 1.

Таблица 1 – Сравнение протоколов обеспечения безопасности процесса взаимодействия информационных систем

	SSH	IPsec	SSL/TLS
Основное назначение	Обеспечение защищённого удалённого управления операционной системой и защищённого туннелирования TCP-соединений	Обеспечение защиты данных, передаваемых по протоколу IP	Обеспечение защиты данных, передаваемых протоколами уровня приложений модели OSI
Конфиденциальность	Симметричные алгоритмы шифрования	Симметричные алгоритмы шифрования	Симметричные алгоритмы шифрования
Аутентификация	Сервер – по ключу. Клиент – по паролю либо по ключу	По общему ключу либо по сертификатам	В основном по сертификатам SSL
Масштабируемость	Нет	Да, для VPN	Да
Поддержка VPN	В виде туннелирования TCP-соединений	Да	Да
Поддержка протоколов с клиент-серверной архитектурой	В виде туннелирования TCP-соединений	Прозрачен для уровня приложений	Да

Из данных таблицы можно заключить, что каждый из протоколов обладает своими преимуществами и недостатками и подходит для реализации вполне конкретных задач. Механизмы безопасности всех рассмотренных протоколов имеют схожие черты. Однако более продуманным и универсальным протоколом из всех является именно SSL/TLS. С помощью него можно организовывать как легко масштабируемые VPN туннели, так и взаимодействие протоколов клиент-серверной архитектуры, а аутентификация по сертификату представляется наиболее надёжной на сегодняшний день.

Стоит понимать, что SSL/TLS достаточно сложный протокол и обладает большим количеством параметров. Правильная настройка этих параметров позволит защитить ИС от атак, направленных на нарушение конфиденциальности и подлинности (целостности) информации.

Список использованных источников:

1. Bulletproof SSL and TLS / Ivan Ristic // Feisty Duck Limited, 2014. – P. 23-63, 247-269.
2. Компьютерные сети / Э. Танненбаум, Д. Уэзеролл – СПб.: Питер, 2012. – С. 854-871, 896-910.
3. SSL, SSH and IPsec [Электронный ресурс]. – Режим доступа: https://www.cs.swarthmore.edu/~mgagne1/teaching/2016_17/cs91/SSL_IPsec.pdf

УДК 004.056.53

БЕЗОПАСНОСТЬ ОСУЩЕСТВЛЕНИЯ БАНКОВСКИХ ТРАНЗАКЦИЙ ПОСРЕДСТВОМ NFC, ВСТРОЕННЫХ В ФИТНЕС-БРАСЛЕТЫ

Кондрашук О.А.[1], студент гр.961402

Белорусский государственный университет информатики и радиоэлектроники1

г. Минск, Республика Беларусь

Белоусова Е.А. – кандидат. технических. наук

Аннотация. В данной статье рассматриваются принцип работы модуля NFC в фитнес-браслетах, возможные случаи получения несанкционированного доступа злоумышленника к фитнесс-браслету, способы их предотвращения.

Ключевые слова. Фитнес-браслет, модуль NFC, метка, ридер.

В современном мире новые технологии все чаще помогают людям следить за здоровьем и физической формой. Одними из таких устройств являются фитнес-браслеты. Однако технологии стремительно развиваются и если раньше фитнес-браслеты могли всего лишь собирать статистику физической активности человека, то есть измерять пульс, количество шагов, пройденное расстояние, продолжительность сна, то сейчас на фитнес-браслет могут приходить уведомления, с помощью его можно отвечать на звонки и даже совершать банковские транзакции по оплате товаров и услуг. В последнее время всё большую популярность набирают бесконтактные платежи. Поэтому эта функция теперь есть на многих моделях фитнес-браслетов.

За бесконтактную оплату в фитнес-браслетах отвечает чип NFC (Near Field Communication – в переводе с англ. «коммуникация ближнего поля»). Эта технология активно разрабатывалась еще с середины 1990-х годов. Первый стандарт такого беспроводного соединения появился 8 декабря 2003 года. На сегодняшний день технология NFC работает по стандарту RFC 4729 [1]. Технология беспроводной передачи данных на малом расстоянии характеризуется следующими особенностями: радиус связи не превышает 10 см; информация с объектов считывается посредством радиосигнала.

NFC представляет собой радиочастотный обмен данными на частоте 13,56 МГц (рисунок 1), таким образом, для ее работы не требуется подключение к интернет. Устройства NFC состоят из считывателя (ридера) и антенны, либо из метки и антенны. Ридер генерирует радиочастотное поле, которое может взаимодействовать с меткой или с другим ридером, он работает в режиме активной коммуникации. Этот тип коммуникации используется при одноранговом режиме. Метками называются информационные зоны с NFC-чипами, которые можно программировать [2]. Метка работает в режиме пассивной коммуникации. Это означает, что устройство с меткой использует поле, которое сгенерировало устройство-инициатор. Такой вид коммуникации используется во всех режимах работы NFC.

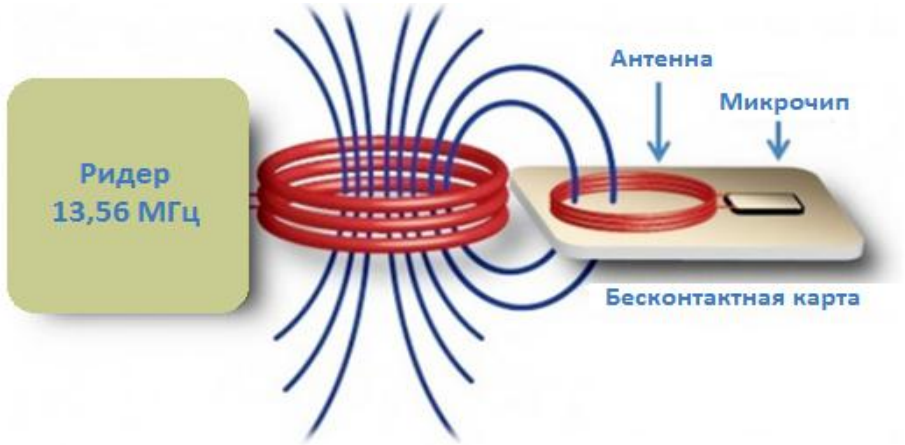


Рисунок 1 – Принцип работы NFC модуля в фитнес-браслетах [3]

Модули NFC интегрируют в платежные терминалы, турникеты, замки, банковские карты, смартфоны, смарт-часы и с каждым днем область применения технологии постоянно расширяется.

Достоинства технологии NFC:

– быстрота установки связи между объектами (процесс занимает доли секунды);

– небольшой размер устройства;

– низкий уровень энергопотребления.

Фитнес-браслет с модулем NFC позволяет выполнять такие функции как создание и сканирование меток, оплата товаров и услуг [4].

NFC-метки [2] можно увидеть на афишах, рекламных баннерах, в супермаркетах на полках возле товара, а также в современных музеях около экспонатов. Чтобы получить дополнительную информацию о товаре, нужно поднести часы или смартфон с модулем NFC к метке, и устройство выполнит нужную команду. Также с помощью NFC-меток можно включить GPS, отправить сообщение, включить аудиоплеер и т.д.

Также NFC выполняет функции Bluetooth, то есть обеспечивает передачу радиосигнала на частоте 13,56 МГц. Для обмена данными используется программа Android Beam, которая установлена на всех устройствах Android в версии не ниже 4.0. Стандарт связи NFC [1] позволяет передавать контакты, координаты местоположения, ссылки на веб-страницы.

Рассмотрим процесс оплаты покупок на примере фитнес-браслета Mi Smart Band 4. В первую очередь необходимо установить мобильное приложение и активировать в нём свою учётную запись. Во вкладке «Мои устройства» нужно выбрать модель своего браслета. Затем во вкладке «Банковская карта» заполнить информацию о своей карте и подтвердить авторизацию с помощью смс-сообщения. Для того, чтобы оплатить какую-либо покупку нужно всего лишь в меню на дисплее выбрать нужную карту, активировать её нажатием на кнопку и поднести как можно ближе к считывателю карт. Важно отметить, что карту нужно поднести к считывателю в течение минуты после активации карты. Транзакция будет завершена, когда браслет завибрирует. Также можно отметить то, что за данный сервис не нужно платить и для покупок с использованием «Mi Band Pay» доступ к сети интернет в момент покупки не требуется. В результате можно выделить множество преимуществ фитнес-браслетов с NFC. Они удобны в эксплуатации; обладают низкой стоимостью; защищены от влаги и пыли по стандартам IP68 и IP4x [5].

При этом возникает вопрос безопасности реализации оплаты посредством технологии NFC. Рассмотрим наиболее опасные уязвимости данных устройств и способы их решения.

Один их самых распространённых недостатков использования фитнес-браслета для оплаты покупок и услуг заключается в том, что при его потере злоумышленник может легко воспользоваться им. Чтобы этого не произошло, необходимо сразу после оплаты заблокировать карту или использовать функцию автоблокировки браслета при его снятии с запястья, однако такая функция по умолчанию не установлена.

Злоумышленники с помощью специальных считывателей карт могут незаметно коснуться браслета и списать с карты определённую сумму. Однако, чтобы это произошло, необходимо, чтобы на устройстве был активирован режим оплаты. Предположим, что режим оплаты случайно активировался на устройстве. Для предотвращения такого исхода событий, на фитнес-браслетах установлен таймер, равный 1 минуте. Если в течение 1 минуты оплата не произведена, то данный режим выключается. Злоумышленнику необходимо очень постараться, чтобы незаметно списать деньги в течение данного промежутка времени.

Многие считают, что данные карты можно считать с помощью NFC-ридера. Однако это невозможно, информация, необходимая для создания виртуальной карты, хранится в зашифрованном виде на сервере Google и не поступает на терминал. А в приложении формируется секретный ключ – токен, в котором зашифрован номер банковского счёта.

Таким образом, можно уверенно сказать, что использование фитнес-браслетов для оплаты товаров и услуг является не только удобным, экономичным и быстрым решением, но и безопасным, если использовать дополнительные функции настройки блокировки карты и самого фитнес-браслета при его снятии.

Список использованных источников:

1. A Uniform Resource Name (URN) Namespace for the Near Field Communication (NFC) Forum / IETF Datatracker. – Режим доступа: https://datatracker.ietf.org/doc/html/rfc4729. – Дата доступа: 04.04.2022.

2.. NFC-метки. – Режим доступа: https://www.kp.ru/guide/nfc-v-smartfone.html. – Дата доступа: 04.04.2022.

3. Технология NFC. – Режим доступа: https://trends.rbc.ru/trends/industry/6148a1459a79479f4328c2f8. – Дата доступа: 04.04.2022.

4. Функции фитнес-браслетов. – Режим доступа: https://gercules.fit/sportivnye-gadzhety/fitnes-braslet-s-nfc-android-pay.html. – Дата доступа: 04.04.2022.

5. Стандарты IP68 и IP4x – Режим доступа: https://smartchasy.com/sovety-i-instrukcii/zashhita-ot-vody-i-pyli-tablica-zashhity-ip-i-atm-dlja-chasov-i-fitnes-brasletov/. – Дата доступа: 04.04.2022.

UDC 004.056.53

SECURITY BANKING TRANSACTIONS USING FITNESS TRACKER WITH BUILT-IN NFC MODULE

Kondrashuk O.A.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Belousova E.S. – PhD in technical sciences, associate professor

Annotation. The principle of NFC module operation in fitness tracker, possible cases of obtaining unauthorized access to a fitness tracker by an attacker, and ways to prevent it are provided in article.

Keywords. Fitness tracker, NFC module, tag, reader.

УДК 537.531

УНИВЕРСАЛЬНАЯ ФОНОВАЯ МОДЕЛЬ ДЛЯ ЗАДАЧ ВЕРИФИКАЦИИ ДИКТОРА

Крищенович В.А., магистрант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Захарьев В.А. – канд. техн. наук, доцент

Аннотация. Доклад посвящен роли универсальной фоновой модели в системах голосовой верификации диктора.

Ключевые слова. Голосовая верификация, голосовые признаки, универсальная фоновая модель, обучение УФМ.

Область речевых технологий на протяжении многих лет остается одной из самых актуальных направлений исследований. Это связано с широким кругом ее применимости в жизнедеятельности человека. Еще ни один компьютер не способен так быстро распознавать звуки, как это может делать человеческое ухо. И даже этот один факт говорит о том на сколько существующие системы не совершенны и требуют доработок.

Одной из наиболее сложных задач в области обработки речи является верификация диктора. Голос уступает по надежности идентифицирующего признака отпечаткам пальцев или сетчатки глаза. Но в качестве дополнительного фактора верификации в реальных система разграничения доступа, голосовая верификация дает ощутимые преимущества: возможность выполнения процедуры верификации без непосредственного визуального контакта с системой, отсутствие необходимости тактильного взаимодействия с системой – свободные руки, и пр.

Современные системы голосовой идентификации и верификации работают в двух режимах: обучение и рабочий режим.

В режиме обучения выделяются характерные признаки голоса диктора. Далее на основе этих признаков формируется его голосовая модель (голосовой отпечаток) и затем данная модель сохраняется в базе данных.

Кроме того, в режиме обучения на основе выделенных признаков голоса диктора также составляется так называемая универсальная фоновая модель -- УФМ (Universal Background Model -- UBM), которая описывает некоторые усредненные голосовые характеристики всех дикторов, находящихся в базе[2].

В рабочем режиме выделяются характерные признаки голосового сигнала диктора, затем выполняется проверка принадлежности признаков к конкретной заданной голосовой модели - верификация диктора. Также в этом режиме на основании универсальной фоновой модели проводится вычисление степени уникальности голосового сигнала. Данная степень уникальности позволяет судить о достоверности верификации и является частью аппарата принятия конечного решения.

Функциональная схемы работы такой системы представлена на рисунке 1.

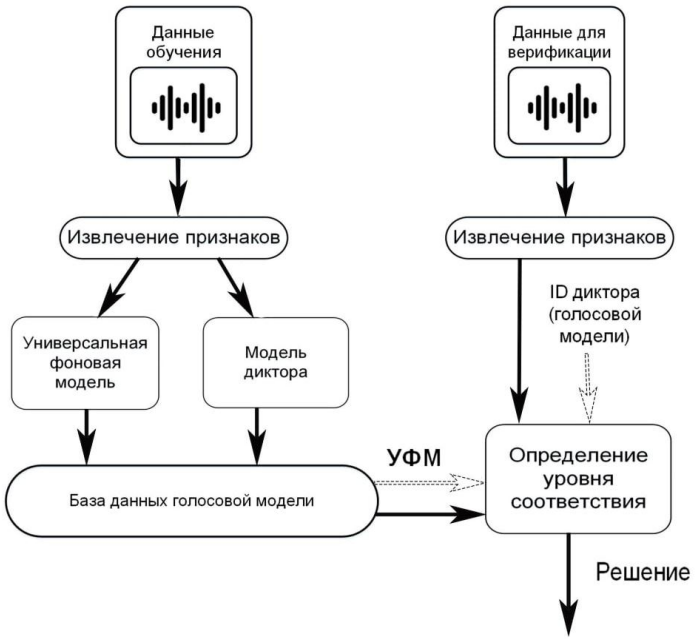


Рисунок 1 – Функциональная схема системы голосовой верификации диктора

При извлечении признаков голоса диктора обычно производится обработка сигнала: разбиение всего сигнала на отрезки и другие действия, в зависимости от типа извлекаемых признаков. Эти признаки используются для обучения универсальной фоновой модели. После обучения универсальной фоновой модели производится обучение моделей дикторов, зарегистрированных в системе, с помощью адаптации от универсальной фоновой модели. Для тестирования модели вычисляется логарифм отношения правдоподобия между заданной моделью диктора и универсальной фоновой моделью для заданного речевого сигнала [2, 4].

Также при создании универсальной фоновой модели необходимо помнить, что данные, используемые для обучения модели, должны быть сбалансированными по отношению к дальнейшему применению системы: сбалансированы по гендерному типу, оборудованию и стандартным условиям. Т.е. длительность обучающей выборки для дикторов мужчин и дикторов женщин должна быть примерно одинаковой для системы голосовой верификации [2]. Аналогичным образом, обучающие данные должны быть сбалансированы и по типу используемых при записи дикторов микрофонов [2].

Для обучения универсальной фоновой модели используется речевой корпус, который содержит аудиозаписи большого количества дикторов. Т.к. универсальная фоновая модель – это большая модель Гауссовой смеси, обученная для представления дикторонезависимого распределения признаков, то системы использующие данные модели, называются системами верификации диктора на основе модели Гауссовых смесей и универсальной фоновой модели (GMM-UBM) [1, 3].

Обучение универсальной фоновой модели возможно методом объединения результатов обучения отдельных моделей для разных выборок в одну. Например, объединение отдельных модели, обученные на выборках с дикторами мужчинами и дикторами женщинами, или обучение отдельных моделей для записей на различные типы микрофонов [2]. Также известны другие подходы, связанные с обучением моделей для групп дикторов [3, 4].

Простое обучение универсальной фоновой модели возможно на всей обучающей выборке с помощью метода максимального правдоподобия - EM (Expectation-Maximization) алгоритма [5].

Задача метода состоит в нахождении по заданным обучающим данным таких параметров модели, при которых функция правдоподобия модели достигает максимума.

На первом шаге алгоритма вычисляется ожидаемое значение функции правдоподобия. На втором шаге вычисляется оценка максимального правдоподобия для каждой компоненты модели. Затем вычисляются новые параметры модели, которые используются на первом шаге следующей итерации алгоритма [5].

В GMM-UBM системе для создания модели диктора производится адаптация параметров универсальной фоновой модели на обучающих данных конкретного диктора. Данная адаптация

известна также как Байесово обучение или оценка апостериорного максимума. Это позволяет не только увеличить точность распознавания диктора по сравнению с неадаптированными моделями, но и ускорить оценку соответствия моделей [7].

Также, как и в EM-алгоритме, адаптация состоит из двух шагов, однако на втором шаге вычисленные параметры смешиваются с исходными параметрами, взятыми из универсальной фоновой модели, по определенному коэффициенту[5].

Для существующих систем верификации используются базы речевых данных в несколько сотен часов, при этом обучение универсальной фоновой модели даже на современном оборудовании может длиться ни одну неделю [6]. Также погрешность вычислений влияет на качество записанных голосовых данных.

Таким образов, в настоящее время существует потребность в разработке качественного метода обучения универсальной фоновой модели на основе GMM-UBM модели с более высокой скоростью вычислений и меньшей погрешностью, способной работать с голосовыми материалами среднего качества (например, запись телефонного разговора) и менее чувствительной к изменению условий регистрации голосового сигнала, что повлияет на улучшение надежности системы.

Список использованных источников:

1. Bimbot F. et al. A tutorial on text-independent speaker verification // EURASIP J. on Applied Signal Processing. – 2004. – No. 4. – P. 430–451.

2. Reynolds D., Quatieri T.F., Dunn R.B., Speaker Verification Using Adapted Gaussian Mixture Models, Digital Signal Process. 10 (2000), pp 19-41.

3. Reynolds D., Rose R. Robust text-independent speaker identification using Gaussian mixture speaker models // IEEE Trans. On Speech and Audio Processing. – 1995. – No. 3. – P. 72–83.

4. Rosenberg A. E., Parthasarathy S. Speaker background models for connected digit password speaker verification // Acoustics, Speech, and Signal Processing (ICASSP-96), IEEE International Conference on. – 1996. – Т. 1. – С. 81-84.

5. Sadjadi S.O., Slaney M., Heck L. MSR identity toolbox v1.0: A MATLAB toolbox for speaker-recognition research // Speech and Language Processing Technical Committee Newsletter. – 2013. – Т. 1. – № 4. – С. 1–32.

6. Габдуллин, В.В. Применение технологии CUDA для задач голосовой биометрии на примере построения универсальной фоновой модели диктора / В.В. Габдуллин, А.И. Капустин, А.И. Королев // Параллельные вычислительные технологии (ПаВТ'2011). – СпБ., 2011. – С. 107-116.

7. Рохманенко, И.В. Алгоритмы и программные средства верификации диктора по произвольной фразе / И.В. Рахманенко; науч. рук.Р.В. Мещеряков; ТУСУР. – Томск, 2017. – 111 с.

УДК 537.531

МЕТОДИКА РАЗРАБОТКИ ЗАЩИЩЕННОГО ПРИЛОЖЕНИЯ ДЛЯ СИСТЕМЫ ИНТЕРНЕТ-БАНКИНГА

Кукла Д.С.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Бойправ О.В. – канд. техн. наук

За последние несколько лет в сфере информационной безопасности наметилась четкая тенденция, большая доля веб-приложений находятся под атакой. Веб-приложения продолжают оставаться основным вектором атак для преступников, и тенденция не показывает никаких признаков ослабления; злоумышленники все чаще избегают сетевых атак благодаря межсайтовому скриптингу, SQL-инъекциям и многим другим методам проникновения, направленным на прикладной уровень. К уязвимостям веб-приложений можно отнести многие вещи, включая плохую проверку ввода, небезопасное управление сеансом, неправильно настроенную систему настройки и недостатки операционных систем и программного обеспечения веб-сервера.

Взлом веб-приложений является одним из наиболее часто используемых методов кибератак как на организации, так и на частных лиц. Взломанные сайты используются в различных целях – для распространения вредоносного ПО, кражи информации, размещения несанкционированной рекламы или запрещенной информации, мошенничества, проникновения во внутреннюю сеть компании.

Перечень наиболее распространенных атак со временем практически не меняется: на верхних строчках рейтинга традиционно SQL Injection, Path Traversal и XSS. Суммарно они составляют более половины всех выявляемых кибератак на веб-ресурсы компаний.

Основными протоколами обеспечения безопасности процесса взаимодействия информационных систем являются SSH, IPsec и SSL/TLS. Сравнение данных протоколов приведено в таблице 1.

Таблица 1.3.1 - OWASP топ 3 наиболее критических рисков безопасности для веб-приложений

	Название угрозы	Описание
A1	Сломанный контроль доступа	Управление доступом применяет политику таким образом, что пользователи не могут действовать за пределами своих предполагаемых разрешений. Сбои обычно приводят к несанкционированному раскрытию информации, модификации или уничтожению всех данных или выполнению бизнес-функций за пределами возможностей пользователя.
A2	Криптографические сбои	Основное внимание уделяется сбоям, связанным с криптографией (или ее отсутствием)
A3	Инъекция	Некоторые из наиболее распространенных инъекций – SQL, NoSQL, команда ОС, реляционное сопоставление объектов (ORM), LDAP, язык выражений (EL) или библиотека навигации по графу объектов (OGNL).

Наиболее критичными являются уязвимости в сфере финансовых организаций. В первую очередь стоит отметить банковские сервисы, которые предоставляют пользователям возможность распоряжаться их деньгами – оплачивать услуги, открывать вклады и брать кредиты, переводить средства другим пользователям. Именно атаки на клиентов располагаются на первой строчке по

распространенности среди атак на веб-приложения финансовых организаций, в частности «Межсайтовое выполнение сценариев» (Cross-Site Scripting).

Таким образом, веб-приложения финансовых компаний с точки зрения рисков выделяются на фоне сайтов организаций из других отраслей.

Список использованных источников:

1. OWASP Top 10 – 2021 [Электронный ресурс]. – Режим доступа : https://owasp.org/Top10/

2. Исследование актуальных киберугроз 2019 – [Электронный ресурс]. – Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2019/

3. Classification of Web Application Vulnerabilities – [Электронный ресурс]. – Режим доступа : http://www.ijesit.com/Volume%202/Issue%202/IJESIT201302_35.pdf

УДК 537.531

ПРОГРАММНОЕ СРЕДСТВО РАСПОЗНАВАНИЯ ДИКТОРА ПО РЕЧИ

Куницкий Ю.О., Лунь Н.С., Зайковский В.С.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Зельманский О. Б. – канд. техн. наук

Обоснована целесообразность применения уникальных особенностей речи при решении задачи верификации пользователя. Предложены программные модули распознавания речевого сигнала и верификации диктора по голосу.

Стремительное развитие и повсеместное распространение информационных систем и технических средств обуславливает необходимость компьютерной обработки речевой информации, поскольку голосовой интерфейс взаимодействия представляется наиболее удобным и востребованным. Таким образом, целесообразно использовать голосовые технологии для биометрики, а именно верификацию говорящего по его голосу. Верификация по голосу представляет собой процедуру подтверждения личности с помощью индивидуальных особенностей речи. Различают текстозависимые и текстонезависимые системы верификации. Текстозависимые требуют произнесения определенной фразы и сравнивают ее с эталоном для каждого пользователя. Верификация в текстонезависимых системах осуществляется на основании любого речевого фрагмента заданной длины.

Первоочередной задачей верификации говорящего является распознавание речевого сигнала. Для ее решения предлагается программный модуль осуществляющий анализ акустической обстановки и расчет следующих параметров сигнала: среднеквадратическое значение, среднее число перехода сигнала через нуль, период основного тона. Далее рассчитанные значения параметров сравниваются с устанавливаемыми пользователем пороговыми значениями. В случае если значения одновременно всех параметров удовлетворяют установленным требованиям, то анализируемый фрагмент сигнала считается речевым. Данный модуль реализован на языке программирования C++ в среде Visual Studio. Предусмотрена возможность вручную задавать пороговые значения параметров с целью адаптации настройки алгоритма и изучения особенностей распознавания речевых сигналов. Структурная схема модуля представлена на рисунке 1.

Рисунок 1 – Структурная схема модуля распознавания речи

Непосредственная верификация пользователя реализована в отдельном модуле, на вход которого подаются фрагменты сигнала, классифицированные как речевые. Модуль верификации также реализован на языке программирования C++ в среде Visual Studio. Работа модуля построена таким образом, что предварительно требуется тестовый ввод логина с целью идентификации пользователя, а следом произнесения пароля. Это позволяет избежать необходимости эмпирического поиска баланса между возможностью возникновения ошибок первого и второго рода, понижая при этом коэффициент когнитивного сопротивления конечного пользователя [1]. В модуле из частотной характеристики сигнала с помощью дискретного косинусного преобразования выполняется расчет вектора мел-кепстральных коэффициентов [2], который сравнивается с базой эталонных записей пользователей. В качестве эталонной записи для каждого пользователя используется усреднённое значение вектора мел-кепстральных коэффициентов трех вариантов

произнесения парольной фразы. Сравнение реализовано при помощи самоорганизующейся нейросети Кохонена.

Список использованных источников:

1. Куницкий, Ю.О. Верификация диктора по голосу на базе метода динамического искажения времени / Ю.О. Куницкий, О.Б. Зельманский // Технические средства защиты информации: материалы XIX Белорус.-российск. науч.-техн. конф., Минск, 8 июня 2021 г. / БГУИР ; редкол.: Т.В. Борботько [и др.]. – Минск, 2021. – С. 59.

2. Запрягаев С.А., Коновалов А.Ю. Распознавание речевых сигналов. Вестник ВГУ, 2009, №2, с. 39-48.

УДК 366.636.2

СОЦИАЛЬНАЯ ИНЖЕНИРИЯ В ВИДЕОСЕРВИСАХ И СОЦИАЛЬНЫХ СЕТЯХ

Мокеров В.С., студент гр.061402

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук

Аннотация. Автором статьи описан личный опыт обнаружения социальной инженерии при использовании социальных сетей и видеоресурсов. В статье представлены примеры попыток манипулирования социальным поведением пользователей с помощью рекламы запрещенных товаров, предоставления недостоверной прополитичной информации, блокировки государственных каналов средств массовой информации, описаны методы и приемы, которые используются журналистами и видеоблогерами с целью привлечения внимания пользователей и навязывания недостоверной информации, приведены меры по анализу достоверности информации и ограничения возникновения нежелательной рекламы при посещении видео ресурсов и социальных сетей.

Ключевые слова. Социальная инженерия, социальные сети, видео сервисы, недостоверная информация.

На фоне стремительного развития приложений, веб и видео ресурсов увеличилось число попыток воздействия на пользователей посредством социальной инженерии [1]. Социальная инженерия в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации [2].

Многие платформы видеосервисов и социальных сетей за последнее время неоднократно предоставляли рекламу запрещённых товаров, услуг, различных игорных сервисов и услуг мошенников Одним из таких примеров является видеохостинг YouTube, при просмотре которого возникает прополитическая реклама, целью демонстрации которой является дестабилизации ситуации в некоторых странах и увеличения энтропии общества, что является нарушением статьи 130 Уголовного Кодекса Республики Беларусь и Закона Республики Беларусь № 15-З «О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам рекламы» [3]. Необходимо отметить, что такая реклама относится к детскому контенту [4] и распространяется на детских каналах, что может сформировать неправильное представление у подрастающего поколения. При этом на YouTube блокируются некоторые официальные государственные каналы средств массовой информации, по причине нарушения правил пользования платформой. В то же время другие политические каналы с иными взглядами не подвержены такой блокировке [5]. Возникает проблема восприятия и анализа информации пользователями данного видеохостинга в виду отсутствия альтернативных источников, результатом чего является принятие заведомо ложной информации в качестве достоверной. Во многих социальных сетях, например, в Facebook появляются ложные официальные аккаунты, публикующие недостоверную информацию и продвигаемые данной платформой в виде рекламы и рекомендаций, что способствует намеренному формированию отрицательных отношений к русскоговорящему населению [6]. В распространение ложных сведений участвуют представители различных организаций, преследующих определенные цели и выгоду в дестабилизации социального настроения, нанося тем вред политическому и экономическому секторам государства, путем оплаты специальной провокационной рекламы на платформах видео сервисов и социальных сетей. Согласованность действий таких организаций увеличивает эффективность влияния на мнение пользователей и их настроения.

На основе обзора и изучения множества источников, придерживающихся различных взглядов, и выступлений журналистов и блогеров, можно выделить используемые ими приемы для убедительности представляемых ими недостоверных фактов:

– однополярность, представление одной точки зрения;

– синхронность – резкая одновременная подача одного и того же материала, зачастую даже без изменения текста;

– попытки избавиться от инакомыслия;

– использование минимального количество фактов и максимального количества эмоциональных высказываний.

Кроме того, многие журналисты и видеоблогеры используют в своей работе эффект доктора Фокса, психологический эффект, заключающийся в том, что выразительность диктора может полностью завуалировать для слушающих бесполезность и вымышленность всего материала. Точнее говоря, имеется корреляция между положительными оценками слушателей по части качества выступления и степенью импрессивности журналиста [7].

Таким образом, такое представление информации является спланированным действием, направленным не на информирование пользователей, а на дестабилизацию мнений.

Автором данной статьи разработаны меры для эффективного анализа и углубленного понимания новой информации, а именно:

– обращать внимание на эмоциональность подачи, количество фактов;

– оценить, не противоречит ли заявления, изложенные в сообщении, информации из других источников;

– оценить репутацию автора данных материалов, благодаря чему можно оценить его объективность;

– наличие ссылок на первоисточник;

– обратить внимание на детали, при возможности их в других источниках;

– проверить историю взаимодействия с данным объектом.

– правила использования цитат, которые зачастую используются без контекста и ссылок.

Использование ресурсов, специализирующихся на проверке информации, такие как «Проверено» и «Fakecheck», также могут помочь в анализе достоверности информации, но интернет-издания могут совершать ошибки, поэтому также необходимо анализировать логические ошибки.

Для борьбы с распространением недостоверной информации должна проводиться быстрая реакция на любые события и даваться подробная своевременная информация. Поддержка общественных организаций по информированию населения и организации государственных информационных источников во всех возможных ресурсах интернета так же способствует правильному информированию населения. В правовом регулировании вводиться ряд запретов на осуществление информационно-психологического воздействия, проводиться идеологическая информационная работа среди населения [8].

В качестве мер по ограничению возникновения нежелательной рекламы при посещении видео ресурсов и социальных сетей рекомендуется установить и правильно настроить системы антивирусной проверки веб ресурсов. Большинство веб-сайтов содержат привлекательные названия, рассчитанные на манипулирование любопытством или иными чувствами пользователей с целью переадресации пользователей на другие сайты и получения их личных данных. Система антивирусной проверки может блокировать вход на подозрительные сайты с нежелательным контентом или низкой репутацией. Также следует установить программы обеспечения безопасности, такие как SIEM-системы, системы учёта рабочего времени и др. При посещении различных веб-сайтов также может возникать всплывающая реклама, которая может нести положительный и отрицательный эффект воздействие, первый заключается в рекламе услуг, интересных пользователям и не нарушающих законы Республики Беларусь, второй – распространение недостоверной информации, призывы к насилию, и иные противоправные действия. Для блокировки всплывающей рекламы в браузере могут использоваться такие приложения как Adguard, AdBlock, Ad Muncher, При этом следует помнить, что использование такого рода программ может привести к некорректной работе некоторых веб-сайтов. В случае получения электронных сообщений от незнакомых лиц не рекомендуется открывать их содержимое и переходить по ссылкам, указанных в таких сообщениях.

Таким образом, на каждого пользователя социальных сетей и видео сервисов возлагается индивидуальная ответственность по анализу информации и определению степени ее достоверности, а также ограждение своих родственников от воздействия нежелательной рекламы. Представленные меры по ограничению возникновения нежелательной информации не являются максимально эффективными, но способствуют защите от социальной инженерии.

Список использованных источников:

1. Социальная инженерия в 2021 году / АО «Лаборатория Касперского». – Опубл. 20.08.2021. – Режим доступа: https://docs.cntd.ru/document/499074140 – Дата доступа: 01.04.2022.

2. Светлана Собалева. Социальная инженерия. [Электронный ресурс] – Опубл. 06.0.2019 – Режим доступа: https://stekspb.ru/blog/socialnaya-inzheneriya – Дата доступа: 30.03.2022.

3. Закон Республики Беларусь «О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам рекламы» от 03.01.2013 г. № 15-З.

YouTube рекламирует мошенников. [Электронный ресурс]. – Режим доступа: https://zen.yandex.ru/media/id/5d3c48671ee34f00aed7792c/youtube-reklamiruet-moshennikov-obescaiuscih-vyplatu-ot-gosudarstva-razlichnyh-summ-5ebe1ee28600f212158d078d – Дата доступа: 30.03.2022.

4. Реклама в контенте для детей и контролируемых аккаунтов. [Электронный ресурс] – Режим доступа: https://support.google.com/youtube/answer/9713557?hl=ru – Дата доступа: 30.03.2022.

Пример явного нарушения. [Электронный ресурс] – Режим доступа: https://www.youtube.com/channel/UC2ErIXePrCMUVGglpgg1SeQ – Дата доступа: 30.03.2022.

5. YouTube начал блокировку каналов российских медиа. [Электронный ресурс] – Режим доступа: https://www.rbc.ru/society/11/03/2022/622b865f9a794703dac56740 – Дата доступа: 30.03.2022.

6. Facebook использует свои платформы для распространения фейков и психологических атак. Новости первого канала. [Электронный ресурс] – Режим доступа: https://www.1tv.ru/news/2022-03-02/422433-facebook_ispolzuet_svoi_platformy_dlya_rasprostraneniya_feykov_i_psihologicheskih_atak – Дата доступа: 30.03.2022.

Разжигание межнациональной розни. [Электронный ресурс] – Режим доступа: https://zen.yandex.ru/media/riafan.ru/razjiganie-mejnacionalnoi-rozni-deputat-butina-o-licemernoi-politike-facebook-i-instagram-622b7ddab2c8b30490b3058e – Дата доступа: 30.03.2022.

7. Эффект доктора Фокса. [Электронный ресурс] – Режим доступа: https://lifemotivation.online/razvitie-lichnosti/samorazvitie/effekt-doktora-foksa – Дата доступа: 30.03.2022.

8. Защита населения от искаженных фактов. [Электронный ресурс] - Режим доступа https://www.sb.by/articles/u-istiny-ne-byvaet-dvoynikov.htm – Дата доступа: 30.03.2022.

UDC 366.636.2

SOCIAL ENGINEERING IN VIDEO SERVICES AND SOCIAL NETWORKS

Mokerov V.S., Student of the group 961402

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Belousova E.S. – PhD in technical sciences, associate professor

Annotation. The author of the article describes the personal experience of detecting social engineering when using social networks and video resources. The article presents examples of attempts to manipulate the social behavior of users by advertising prohibited goods, providing false pro-political information, blocking state media channels. The methods and techniques used by journalists and video bloggers in order to attract the attention of users and impose false information are described. The measures for analyzing the reliability of information and limiting the occurrence of unwanted advertising when visiting video resources and social networks are provided.

Keywords. Social engineering, social networks, video services, fakes, false information.

УДК 537.531

ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ В ФИНТЕХ КОМПАНИЯХ

Мотуз А. А., студент гр. 861402

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук, доцент

Аннотация. Представлены основные типы угроз кибербезопасности, оценены риски данных угроз.

Ключевые слова. Угрозы кибербезопасности, вредоносное ПО, оценка рисков.

Аудит информационной системы - это процесс сбора и оценки доказательств для определения того, была ли компьютерная система разработана для поддержания целостности данных, защиты активов, эффективного достижения целей организации и эффективного использования ресурсов.
Для защиты от киберугроз необходимы следующие компоненты:
– Надежный брандмауэр и прокси-сервер
– Антивирусное программное обеспечение
– Своевременное и частое сканирование сетевых уязвимостей
Финтех компаниям (организациям, которые при построении своих бизнес-моделей в сферах финансовых услуг используют современные технологии и IT-продукты) следует проводить внутреннюю/внешнюю оценку рисков, включая тестирование на проникновение, сканирование уязвимостей, социальную инженерию и анализ бизнес-процессов, связанных с безопасностью данных. Они также должны разработать дорожную карту облачных вычислений, основанную на подверженности бизнес-рискам (низкий-высокий), стоимости владения и возможности возврата инвестиций в переход на облако.
Необходимость количественной оценки рисков и возможное влияние нарушений безопасности на репутацию мотивируют к более строгим процедурам внутреннего аудита и оценки рисков.
Согласно ежегодного отчету агентства Европейского Союза по сетевой и информационной безопасности (ENISA) об инцидентах в сфере телекоммуникационной безопасности за 2018 год, сегодня организации должны учитывать четыре основных типа ИТ-рисков: риски безопасности, риски доступности, риски производительности и риски соответствия требованиям. Риски безопасности представляют собой несанкционированный доступ к информации: утечка данных, конфиденциальность данных, мошенничество и безопасность конечных точек. Риски безопасности включают также широкие внешние угрозы, такие как вирусы, а также более целенаправленные атаки на конкретные приложения, конкретных пользователей и конкретную информацию.
Для оценки величины угрозы необходимо оценить:
– вероятность её реализации;
– потенциал злоумышленника, реализующего угрозу.
Решение о степени критичности угрозы информационной безопасности принимается в соответствии с таблицей 1.

Таблица 1 – Матрица рисков

Потенциал злоумышленника	Вероятность выполнения			
	Низкая 0	Средняя 1	Высокая 2	Крайне высокая 3
Низкий 0	0	1	2	3
Средний 1	1	2	3	4
Высокий 2	2	3	4	5

Для каждой из выявленных угроз оценивается ее вероятность, потенциал реализующего угрозу нарушителя и, как следствие, степень критичности угрозы.
Из общего списка угроз формируется список критических угроз, которые следует блокировать в первую очередь (угрозы, находящиеся в красной зоне – имеющие 4-5 баллов). В таблицах 2, 3 представлены угрозы для клиентов (физических лиц) и сетевых объектов.
Угрозы хищения у клиентов [2-3] (физических лиц):

– заражение вредоносным ПО (клиент);
– халатность заказчика (социальная инженерия, разглашение или утеря аутентификационных данных);
– халатность сотрудников финтех компании (некомпетентность в обслуживании);
– умышленные действия сотрудника финтех компании;
– фишинг.
Угрозы обслуживанию, хищения у клиентов (юридических лиц):
– заражение вредоносным ПО (клиент);
– халатность сотрудника финтех компании (некомпетентность в обслуживании);
– умышленные действия сотрудника финтех компании;
– фишинг;
Угроза потери контроля над сетевыми объектами [4] :
– использование возможностей финтех компании для атаки на клиентов;
– использование возможностей финтех компании для получения доступа к информации внутри сети.
Угрозы полной/частичной утраты или недоступности активов:
– вредоносное ПО (инфраструктура, AWS);
– DoS/DDoS-атаки;
– APT-атака.
Угроза потери/недоступности банка данных при использовании облачных технологий:
– DoS/DDoS-атаки на провайдера.
Утечка конфиденциальной информации из-за некомпетентности сотрудников:
– отправка по открытым каналам связи;
– компрометация учетных записей администратора.

Таблица 2 – Угрозы хищения у клиентов (физических лиц)

№	Угроза	Потенциал нарушителя	Вероятность выполнения	Критическая область
1	Заражение вредоносным ПО (клиент)	2 (высокий)	3 (крайне высокая)	5
2	Заражение вредоносным ПО (финтех компания)	2 (высокий)	1 (средняя)	3
3	Умышленные действия третьих лиц	2 (высокий)	3 (крайне высокая)	3
4	Халатность заказчика (социальная инженерия, разглашение или утеря аутентификационных данных)	2 (высокий)	3 (крайне высокая)	5
5	Халатность сотрудников финтех компании (некомпетентность в обслуживании)	2 (высокий)	2 (высокая)	4
6	Умышленные действия сотрудника финтех компании	2 (высокий)	2 (высокая)	4
7	Фишинг	2 (высокий)	2 (высокая)	4
9	Скимминг	2 (высокий)	1 (средняя)	3
11	Подбор кодового слова у клиента	1 (средний)	2 (высокая)	3

Таблица 3 – Угроза потери контроля над сетевыми объектами

№	Угроза	Потенциал нарушителя	Вероятность выполнения	Критическая область
12	Возможность финтех компании участвовать в рассылке спама	2 (высокий)	1 (средняя)	3
13	Использование возможностей финтех компании для участия в DDoS-атаках	2 (высокий)	1 (средняя)	3
14	Использование возможностей финтех компании для атаки на клиентов	2 (высокий)	2 (высокая)	4
15	Использование возможностей финтех компании для получения доступа к информации внутри сети	2 (высокий)	2 (высокая)	4

Список использованных источников:

1. ISO/IEC 27001 Information technology. Security techniques. Information security management systems. [Электронный ресурс]. – Режим доступа: https://www.iso.org/ru/standard/54534.html.

2. Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri= CELEX:02016R0679-20160504
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [Электронный ресурс] – Режим доступа: https://eur-lex.europa.eu/eli/dir/1995/46/oj.
4. Risk analysis framework for a cloud specific environment [Электронный ресурс]. – Режим доступа: https://studylib.net/doc/8837952/risk-analysis-framework-for-a-cloud-specific-environment.

УДК 537.531

МОНИТОРИНГ ИНФОДЕМИЙ ДЛЯ АНАЛИЗА И ПРОГНОЗИРОВАНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ ПОСЛЕДСТВИЙ В УСЛОВИЯХ СОЦИАЛЬНЫХ КАТАСТРОФ НА ПРИМЕРЕ РАСПРОСТРАНЕНИЯ ГЛОБАЛЬНОЙ ПАНДЕМИИ COVID-19

Мурашка А.А.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Давыдовский А.Г. – канд. биол. наук, доцент

В данной работе исследована динамика изменений заболеваемости и смертности от COVID-19. Рассмотрена взаимосвязь между запросами в социальных сетях и мессенжерах с взаимосвязью динамики заболеваемости и смертности от COVID-19. Показано, что увеличение частоты запросов может выступать предиктором роста заболеваемости и смертности от COVID-19 в частности, а также увеличением вероятности социальных и социально-экономических катастроф.

В условиях социальных катастроф на примере распространения глобальной пандемии COVID-19, анализ поисковых запросов пользователей, включающих социальные сети и мессенджеры, по тематике, связанной коронавирусной инфекцией, является полезным источником для прогнозирования медико-биологических, социальных и социально-экономических последствий для различных групп пользователей интернет практически во всех странах мира.

Целью работы является возможности и перспективы мониторинга инфодемий для анализа и прогноза заболеваемости и смертности в условиях социальных катастроф на примере распространения глобальной пандемии COVID-19.

Результаты исследования, выполненного на основе статистической обработки поисковых запросов по тематике COVID-19 интернет-пользователей в социальных сетях, а также данных университета имени Джонса Хопкинса о заболеваемости и смертности от коронавирусной инфекции, свидетельствуют о существовании зависимости между частотой поисковых запросов, с одной стороны, и частотой случаев заболеваемости и смертности от COVID-19, с другой стороны. Частота поисковых запросов с упоминанием коронавируса, заболеваемости, госпитализации, лечения, смертности, вакцинации и последствий COVID-19 коррелируют с частотой запросов, отражающих депрессивные и тревожные настроения, распространенные среди значительной части интернет-пользователей, отражающих, в частности, рост тревожности и страха перед заражением. Наиболее популярными запросами интернет-пользователей в Республике Беларусь по «коронавирусной» тематике являются: «COVID-19», «коронавирус», «ковид» и др. Подобные поисковые запросы можно рассматривать в качестве прогностического предиктора развития заболеваемости и смертности при COVID-19. Анализ частоты поисковых запросов по терминам-предикторам позволяет прогнозировать динамику заболеваемости, социальные и социально-экономические последствия коронавирусной инфекции, включая распространение новых штаммов COVID-19 и наступление очередной волны пандемии. Вместе с тем, возрастание частоты подобных поисковых запросов может свидетельствовать о заражении медиааудитории интернет-пользователей медиавирусом «глобальная пандемия COVID-19». Медиавирусы распространяются в медиапространстве точно так же, как биологические в организме хозяина или в популяции организмов. Возникшие в результате пандемии COVID-19 и определяющиеся основными ключевыми словами по данной теме запросы могут быть использованы как медиавирусы-«тягачи» для распространения различных манипулятивных воздействий на все аспекты жизнедеятельности медиааудитории в условиях глобальной пандемии [1].

На основе полученных результатов сформулирована гипотеза о медиапространстве интернет как активной социотехнической среде с диффузионными и квазиупругими свойствами, в которой медиавирусные сообщения могут распространять гармонические, резонирующие или затухающие колебания. Предложена модель волнового распространения медиавирусных сообщений в медиапространстве:

$$D\frac{d^2n}{dz^2} - \alpha(f-g)\frac{dt}{dz} - \beta\left(\frac{df}{dz} - \frac{dg}{dz}\right)n = 0, \quad z = \gamma\Delta\tau N\sum_{i=1}^{N} C_i \sum_{j=1}^{M} M_j,$$

где n – количество медиапользователей, подверженных влиянию факторов инфодемии, обусловленной распространением медиавирусов; z – функция, описывающая связь между количеством всех медиапользователей (N), количеством связей, образуемых каждым из них, по которым осуществляется передача множества сообщений (M_j) в течение периода времени $\Delta\tau$, γ – средний показатель пропускной способности каждого медиаканала; D – коэффициент диффузии медиасообщений, зависящий от социотехнических свойств медиапространства; f – функция распространения медиазаражения, g – функция ограничения медиазаражения; α и β – постоянные [2].

Таким образом, анализ и прогнозирование динамики поисковых запросов населения предоставляет определенные возможности для управления медико-биологическими, социальными и социально-экономическими последствиями распространения коронавирусной инфекции, а также для формирования информационной повестки для организации профилактики роста заболеваемости, подготовки и организации превентивных мер, ликвидации последствий социальной катастрофы вызванной глобальной пандемией COVID-19.

Список литературных источников:

1. *Левчук, Н. Н. Принцип медиавируса в процессе коммуникативного взаимодействия. Веснік Беларускага дзяржаўнага універсітэта. Серыя 4, Філалогія. Журналістыка. Педагогіка. - 2009. - N 3. - С. 96-100.*
2. *Петросян А. Э. В паутине Фамы (природа слухов, их распространение и социальный резонанс) // Вестник ОмГУ. 2008. №3. С. 114-126.*

УДК 004.056.5

ВОЗМОЖНЫЕ УЯЗВИМОСТИ КОМБИНИРОВАННОГО МЕТОДА ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА С ПОМОЩЬЮ СИНЗРОНИЗИРУЕМЫХ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Радюкевич М.Л.[1], аспирант

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Голиков В.Ф. – доктор тех. наук

Аннотация. В статье рассматриваются возможные уязвимости комбинированного метода формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей. Рассмотрена атака «отложенный перебор» и атака, основанная на знании четностей пар. Полученные результаты показали, что благодаря использованию функции свертки на первом этапе экспоненциально увеличивается объем отложенного перебора, а при атаке на втором этапе криптоаналитик не может однозначно различить значения оставшихся битов. Таким образом комбинированный метод позволяет повысить конфиденциальность формируемого общего секрета и существенно сократить количество обменов информацией по сравнению с технологией Neural key generation.

Ключевые слова. синхронизируемые искусственные нейронные сети, общий секрет, криптографический ключ, комбинированный метод, атака.

Введение. Одной из задач современной криптографии является формирование общего криптографического ключа у абонентов, обменивающихся информацией через открытый для прослушивания канал связи.

В работе [1] предлагается комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей (СИНС). Использование СИНС для формирования общего криптографического ключа предложено В. Кантером, И. Кинцелем и описано в [2-6]. Предлагаемое комбинированное формирование состоит из двух этапов: формирование частично совпадающих бинарных последовательностей с использованием функции свертки результатов нескольких независимых синхронизаций [7, 8] и устранение несовпадающих битов путем открытого сравнения четностей пар битов [9]. Рассмотрим возможные уязвимости комбинированного метода.

На мой взгляд, предлагаемый метод может быть атакован как на первом, так и на втором этапах. На первом этапе, т.е. при синхронизации сетей A и B, криптоаналитик E создает свою сеть, идентичную сетям A и B за исключением начальных значений весовых коэффициентов (ВК), синхронизирует (методом отложенного перебора [10]) свою сеть с сетью, например, A в надежде, что его сеть успеет полностью синхронизоваться за отведенное число тактов, обозначим их как $d_{\text{ус}}$. В этом случае окажется, что ключ абонента E и ключ абонента A за отведенное число тактов равны, обозначим это как $K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})$, и сформированный ключ будет полностью дискредитирован.

На втором этапе знание E объявленных четностей пар битов и тот факт, что за счет синхронизации возникает корреляция между $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$, может позволить ему использовать данную информацию для вычисления некоторых битов в итоговой бинарной последовательности (БП).

Любая из этих атак не может быть успешной без наличия критерия, по которому можно удостовериться, что $K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})$. Однако в данной технологии прямая проверка невозможна, но возможна косвенная.

Атака «отложенный перебор». Атака «отложенный перебор» проводится криптоаналитиком E с помощью его искусственной нейронной сети (ИНС), идентичной ИНС A, в течении $d_{\text{ус}}$ тактов.

Так как, первый этап заканчивается только объявлением четностей пар битов бинарных последовательностей A и B, то это не позволяет E сделать однозначный вывод о совпадении $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$ и это усложняет атаку тем, что каждую синхронизацию нужно проводить до завершения второго этапа. И только, если на всех итерациях наблюдается полная идентичность эволюции четностей БП A с B и A с E, то можно считать, что этому предшествовало $K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})$.

Следовательно, вероятность успеха атаки зависит только от вероятности совпадения $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$, т.е. если E удалось синхронизировать свою сеть за $d_{\text{ус}}$ тактов с сетью A, так как все последующие операции не разрушают совпадения ВК сетей E и A.

В таблице 1 приведены результаты анализа вероятностей синхронизации сетей A и E и корреляции ВК сетей E и A, а также их динамика с увеличением числа тактов синхронизации (d). Корреляция ВК рассматривается как относительное среднее число совпадающих битов, обозначим их как $\overline{n_{AB}^{cb}}/b$ и $\overline{n_{EA}^{cb}}/b$, в БП сетей A и B и E и A соответственно. Приведенные данные рассчитывались имитационным моделированием с количеством экспериментов 10^4, при следующих параметрах сетей $n = 1000, K = 3, L_1 = -7, L_2 = 8$, $r = 5$, где n – количество входов каждого персептрона; K – количество персептронов; $\pm L$ – интервал возможных значений весовых коэффициентов персептронов; r – количество строк для функции свертки. Вероятность синхронизации сетей A и B, обозначим как P_{AB}, а сетей E и A - P_{EA}. Вероятности синхронизации сетей при усилении секретности $P_{AB,r}$, $P_{EA,r}$ рассчитывались аналитически по следующим формулам:

$$P_{AB,r} = (P_{AB})^r, \tag{1}$$

$$P_{EA,r} = (P_{EA})^r. \tag{2}$$

Таблица 1. – Вероятность синхронизации сетей A и E и корреляция ВК

d	1000	1200	1500	1800	2000	2500	3000
P_{AB}	0	0	0,005	0,111	0,273	0,736	0,8117
P_{EA}	0	0	0	0,003	0,006	0,032	0,048
$P_{AB,r}$	0	0	$3{,}1*10^{-4}$	$1{,}6*10^{-5}$	0,0015	0,2469	0,352
$P_{EA,r}$	0	0	0	$3*10^{-15}$	$6*10^{-15}$	$2{,}5*10^{-7}$	$3{,}7*10^{-7}$
$\overline{n_{AB}^{cb}}/b$	0,5175	0,5731	0,6756	0,8063	0,8867	0,976	0,9967
$\overline{n_{EA}^{cb}}/b$	0,507	0,509	0,51	0,5072	0,506	0,5033	0,503

Из таблицы 1 видно, что уже при $d > 2000$ относительное среднее число совпадающих битов $\overline{n_{AB}^{cb}}/b$ приближается к 1, в то время как $P_{AB,r}$ остается относительно небольшой. Это объясняется тем, что многие синхронизации получаются не завершенными из-за того, что в них содержится небольшое количество несовпадающих битов.

Оценим вероятность успеха атаки «отложенный перебор». Вероятность этого события равна $P\left(K^E(d_{\text{ус}}) = K^A(d_{\text{ус}})\right) = P_{EA,r}(d_{\text{ус}})$ и зависит от выбора r и $d_{\text{ус}}$. Выбор $d_{\text{ус}}$ обоснован выше. Влияние r рассматривалось в [8], отметим лишь то, что в комбинированном методе за счет увеличения r ослабляется корреляция между $K^E(d_{\text{ус}})$ и $K^A(d_{\text{ус}})$, а это очень важно для второго этапа. При этом корреляция между $K^A(d_{\text{ус}})$ и $K^B(d_{\text{ус}})$тоже ослабляется, но гораздо в меньшей степени (таблица 1). Таким образом, выбрав, например, $r = 5, d_{\text{ус}} = 2000$ для обоснованных ранее значений параметров сетей: $n = 1000, K = 3, L_1 = -7, L_2 = 8$, получим $P_{EA,r} = 6 * 10^{-15}$, $\overline{n_{AB}^{cb}}/b = 0{,}8867$, $\overline{n_{EA}^{cb}}/b = 0{,}506$. Полученные результаты свидетельствуют о значительном сокращении числа необходимых тактов обмена информацией (с 3000 до 2000), снижения за счет этого вероятности дискредитации ФОС на несколько порядков (с 10^{-7} до 10^{-15}).

Атака, основанная на знании четностей пар. На втором этапе метода, когда абоненты A и B оглашают четности пар БП (обозначим их C), сформированных с помощью СИНС, у криптоаналитика E появляется возможность сравнения этих четностей с четностями своей БП и сделать определенные выводы относительно формируемого общего секрета. Оценим эффективность атаки, описанной в [9].

Для этого проведем анализ влияния параметров сетей на процесс устранения несовпадающих битов на втором этапе.

Поскольку процедура устранения несовпадающих битов оперирует с парами битов, то целесообразно проводить анализ на уровне пар, а не отдельных битов. Анализ может быть выполнен аналитически с использованием результатов, полученных в [9] или методом статистического моделирования.

Если длина БП, сформированных путем синхронизации сетей A и B это b. Тогда число пар равно $D = b/2$, если b окажется нечетным, то его следует привести к четному, отбросив последний бит. Тогда согласно [9], среднее число совпадающих пар битов в анализируемых БП равно

$$m_{c,c} = \overline{(n_{AB}^{cb}/b)}^2 * D \text{ ,} \tag{3}$$

где $\overline{n_{AB}^{cb}}$ – среднее количество совпадающих битов в БП A и B.

Среднее число пар битов, содержащих один совпадающий бит, равно

$$m_{c,\text{н}} = \frac{\overline{n_{AB}^{cb}}}{b} \frac{\left(b-\overline{n_{AB}^{cb}}\right)}{b} * 2D\text{,} \tag{4}$$

Среднее число пар битов, содержащих два несовпадающих бита, равно

$$m_{\text{н,н}} = \frac{\left(b-\overline{n_{AB}^{cb}}\right)^2}{b^2} * D\text{.} \tag{5}$$

Пары, содержащие один совпадающий бит, в дальнейшем согласовании не участвуют, т.к. подлежат удалению. Поэтому представляет интерес только величины $m_{c,c}$ и $m_{\text{н,н}}$. В таблице 2 приведены значения этих величин в зависимости от среднего количества совпадающих битов для бинарных последовательностей длиной $b = 12000$.

Таблица 2. – Значения величины $m_{c,c}$ и $m_{\text{н,н}}$ в зависимости от количества совпадающих битов

$\overline{n_{AB}^{cb}}/b$	0,500	0,583	0,666	0,750	0,833	0,9166	1,000
$m_{c,c}$	1500	2041	2666	3375	4166	5401	6000
$m_{\text{н,н}}$	1500	1041	666	375	166	41	0
$m_{c,c} + m_{\text{н,н}}$	3000	3082	3332	3750	5832	5442	6000

Четность пар бит обозначим через $C_i^{A/B/E} = k_j \oplus k_{j+1}$, где i – номер пары, k_j – j-й бит БП. После остановки синхронизации и оглашения четностей пар битов E знает, что A и B оставят для дальнейшего рассмотрения только пары, у которых четности совпадают $C_i^A = C_i^B$. Поэтому E будет рассматривать только те свои пары битов, для которых выполняется $C_i^E = C_i^A = C_i^B$. Для битов каждой из этих пар E может выдвинуть следующие гипотезы:

$$H_0\text{: } k_j^E = k_j^A = k_j^B, k_{j+1}^E = k_{j+1}^A = k_{j+1}^B;$$

$$H_1: k_j^E = \overline{k_j^A} = \overline{k_j^B},\ k_{j+1}^E = \overline{k_{j+1}^A} = \overline{k_{j+1}^B};$$

$$H_2: k_j^E = k_j^A = \overline{k_j^B},\ k_{j+1}^E = k_{j+1}^A = \overline{k_{j+1}^B};$$

$$H_3: k_j^E = \overline{k_j^A} = k_j^B,\ k_{j+1}^E = \overline{k_{j+1}^A} = k_{j+1}^B.$$

Гипотеза H_0 означает, что биты пар E равны битам пар A, которые равны битам пар B. Гипотеза H_1 означает, что биты пар E противоположны битам пар A, которые равны битам пар B. Гипотеза H_2 означает, что биты пар E равны битам пар A, которые противоположны битам пар B. Гипотеза H_3 означает, что биты пар E противоположны битам пар A, которые противоположны битам пар B. Например,

$$H_0: C_i^E = 1 \oplus 1; C_i^A = 1 \oplus 1; C_i^B = 1 \oplus 1;$$

$$H_1: C_i^E = 1 \oplus 1; C_i^A = 0 \oplus 0; C_i^B = 0 \oplus 0;$$

$$H_2: C_i^E = 1 \oplus 1; C_i^A = 1 \oplus 1; C_i^B = 0 \oplus 0;$$

$$H_3: C_i^E = 1 \oplus 1; C_i^A = 0 \oplus 0; C_i^B = 1 \oplus 1.$$

Зная параметры сетей и $d_{\text{ус}}$, E может априорно оценить вероятности этих гипотез путем моделирования, многократно повторяя первый этап метода и подсчитывая количество исходов в которых имело место событие, соответствующее той или иной гипотезе

$$P(\vartheta) \approx \frac{n(\vartheta)}{n_\Sigma}, \quad (6)$$

где ϑ – номер гипотезы, $\vartheta = 0,1,2,3$; $n(\vartheta)$ - число пар, соответствующее гипотезе H_ϑ ,n_Σ – общее число пар, у которых $C_i^E = C_i^A = C_i^B$.

В таблице 3 приведены результаты моделирования для $\text{К} = 3, n = 1000, L_1 = -7,\ L_2 = 8, r = 5$.

Таблица 3 – Результаты моделирования при $r = 5$

$P(\vartheta)$	$d_{\text{ус}}$					
	500	1000	2000	2500	3000	10000
$P(0)$	0,257	0,302	0,483	0,501	0,505	0,506
$P(1)$	0,267	0,363	0,457	0,490	0,495	0,493
$P(2)$	0,245	0,214	0,029	0,003	0,001	0,000
$P(3)$	0,245	0,215	0,029	0,003	0,001	0,000

В таблице 4 приведены результаты моделирования для $\text{К} = 3, n = 1000, L_1 = -7,\ L_2 = 8, r = 10$.

Таблица 4 – Результаты моделирования при $r = 10$

$P(\vartheta)$	$d_{\text{ус}}$					
	500	1000	2000	2500	3000	10000
$P(0)$	0,2494	0,2584	0,4433	0,4887	0,4991	0,5011
$P(1)$	0,2495	0,2558	0,4404	0,4883	0,4964	0,4988
$P(2)$	0,2496	0,2426	0,0584	0,0147	0,0018	0,000

$P(3)$	0,2451	0,2430	0,0578	0,0153	0,0020	0,000

Для наглядности структуры БП на рисунке 1 представлены диаграммы, поясняющие распределения пар битов с различными свойствами.

Рисунок 1. – Диаграммы распределения пар битов с различными свойствами

Из всех пар битов, для которых $C_i^A = C_i^B$, в итоговую БП $K^{AB}(d_{\text{ус}})$ пройдут только биты пар, соответствующие гипотезам H_0, H_1. Поэтому E предполагает, что те биты его БП, для которых выполнялось $C_i^E = C_i^A = C_i^B$ и которые у A и B прошли в итоговую БП, с вероятностью $P(0)$ равны битам последовательностей A и B, а с вероятностью $P(1)$ противоположны им. Однако из таблицы 4 видно, что значения вероятностей $P(0)$ и $P(1)$ в диапазоне предлагаемых значений d и при $r \geq 5$ одинаковы между собой и близки к 0,5, следовательно, для E значения отслеженных битов равновероятны. Данное свойство объясняется, тем, что корреляция БП $K^A(d_{\text{ус}})$, $K^B(d_{\text{ус}})$ и $K^E(d_{\text{ус}})$ очень слабая и с ростом d $K^E(d_{\text{ус}})$ остается практически статистически независимой от $K^A(d_{\text{ус}})$, $K^B(d_{\text{ус}})$ и, следовательно, в ней число пар, соответствующих гипотезам H_0, H_1, остается одинаковым. Следовательно, атака, использующая знание четностей БП, сформированных A и B комбинированным методом, при правильно выбранных параметрах сетей не позволяет дискредитировать ФОС.

Заключение. Рассмотрев возможные уязвимости комбинированного метода формирования криптографического ключа с помощью СИНС можно сделать следующий вывод. На первом этапе при формировании частично совпадающих бинарных последовательностей благодаря использованию функции свертки экспоненциально увеличивается объем отложенного перебора, что позволяет обеспечить требуемую конфиденциальность формируемого общего секрета, а также делает данный способ устойчивым к атаке, основанной на знании четностей пар, на втором этапе. Таким образом комбинированный метод позволяет существенно сократить количество обменов информацией и повысить криптостойкость по отношению к атаке «отложенный перебор» по сравнению с технологией Neural key generation.

Список использованных источников:

1. Радюкевич М.Л., Голиков В.Ф. Комбинированный метод формирования криптографического ключа с помощью синхронизируемых искусственных нейронных сетей. Доклады БГУИР. 2021; 19(1): 79-87.

2. Kinzel, W. Neural Cryptography / W.Kinzel, / I. Kanter // 9th International Conference on Neural Information Processing, Singapore, 2002.

3. Kanter, I. Secure exchange of information by synchronization of neural networks / I. Kanter, W. Kinzel, E. Kanter//arxiv: cond/0202112v1, [cond-mat.stat-mech], 2002.

4. Kanter, I. The Theory of Neural Networks and Cryptography, Quantum Computers and Computing / I. Kanter, W.Kinzel.−2005. Vol. 5, n.1. – P. 130−140.

5. Ruttor, A. Dynamics of neural cryptography / A. Ruttor, I. Kanter, and W. Kinzel // Phys. Rev. E, 75(5):056104, 2007.

6. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологии / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика; под ред. И. М. Жарского. – Минск: БГТУ, 2005.

7. Голиков, В. Ф. Формирование общего секрета с помощью искусственных нейронных сетей / В. Ф. Голиков, М. Л. Радюкевич // Системный анализ и прикладная информатика. – 2019. – № 2. – С. 49–56.

8. Радюкевич, М. Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей / М. Л. Радюкевич, В. Ф. Голиков // Информатика. – 2020. − Т. 17, № 1. – С. 75–81. https://doi.org/10.37661/1816-0301-2020-17-1-75-81.

9. Пивоваров В.Л., Голиков В.Ф. Способ формирования криптографического ключа для слабо совпадающих бинарных последовательностей. Информатика, № 3(51), 2016.Стр. 31-37.

10. Голиков В.Ф. Атака на синхронизируемые исскуственные нейронные сети, формирующие общий секрет, методом отложенного перебора /В.Ф. Голиков, А.Ю. Ксеневич //Доклады БГУИР, №8, 2017. С48-53.

UDC 004.056.5

POSSIBLE VULNERABILITIES OF THE COMBINED METHOD FOR FORMING A CRYPTOGRAPHIC KEY USING SYNCHRONIZED ARTIFICIAL NEURAL NETWORKS

Radziukevich M.L.[1], аспирант

Belarusian State University of Informatics and Radioelectronics[1]

Minsk, Republic of Belarus

Golikov V.F. – doctor of tech. sciences

Annotation. The article discusses possible vulnerabilities of the combined method of generating a cryptographic key using synchronized artificial neural networks. The «delayed enumeration» attack and the attack based on the knowledge of the parity of pairs are considered. The results obtained showed that due to the use of the convolution function at the first stage, the amount of deferred enumeration increases exponentially, and during the attack at the second stage, the cryptanalyst cannot unambiguously distinguish the values of the remaining bits. Thus, the combined method makes it possible to increase the confidentiality of the generated shared secret and significantly reduce the number of information exchanges compared to the Neural key generation technology.

Keywords. synchronized artificial neural networks, shared secret, cryptographic key, combined method, attack.

УДК 004.056.5

МЕТОДИКА ПОВЕРКИ ИЗМЕРИТЕЛЬНОГО ГЕНЕРАТОРА Г4-МВМ-37

Савицкий К. А.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белошицкий А. П.. – кандидат технических наук, доцент

Доклад посвящён разработке методики поверки измерительного генератора Г4-МВМ-37.

С освоением новых частотных диапазонов и быстрым ростом числа и видов различного телекоммуникационного и радиоэлектронного оборудования сверхвысокочастотного (СВЧ) диапазона возрастает роль метрологического обеспечения (МО) его разработки и эксплуатации. Одной из важных задач МО является контроль метрологических характеристик (МХ) используемых измерительных приборов. На разных стадиях жизненного цикла приборов этот контроль осуществляется при проведении государственных испытаний, поверки, калибровки и метрологической экспертизы. При проведении этих работ по метрологической оценке используются специальные, научно-обоснованные методики.

В докладе рассматривается методика поверки (МП) измерительного генератора Г4-МВМ-37, разработанного в центре 1.9 НИИ БГУИР. Генератор предназначен для генерирования электрических синусоидальных колебаний СВЧ в двух основных режимах: непрерывной генерации на одной частоте и перестройки частоты в диапазоне от 25,95 до 37,5 ГГц.

При поверке генератора определяются его следующие основные МХ: нестабильность частоты выходного сигнала - $\pm 2 \times 10^{-8}$; пределы допускаемой относительной погрешности установки частоты - $\pm 2 \times 10^{-7}$; пределы допускаемой погрешности установки уровня выходной мощности - ± 1 дБ; КСВН выхода генератора – не более 1,4.

Для определения этих МХ при поверке генератора были выбраны следующие эталонные средства поверки: электронно-счётный частотомер Ч3-82; ваттметр поглощаемой мощности М3-53; измеритель КСВН панорамный Р2-65.

На рисунках 1, 2 и 3 приведены схемы поверки для контроля выше указанных МХ.

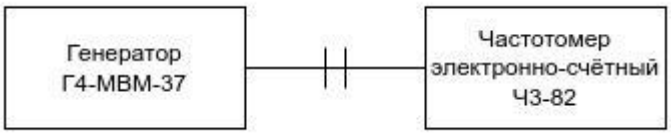


Рисунок 1 – Схема соединения приборов при определении погрешности установки и нестабильности частоты.

Рисунок 2 – Схема соединения приборов при определении погрешности установки уровня мощности выходного сигнала.

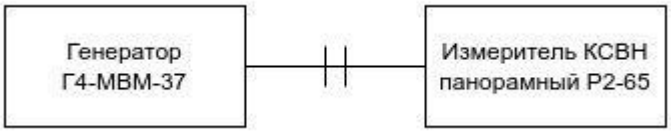


Рисунок 3 – Схема соединения приборов при измерении КСВН выхода генератора.

Определение погрешности установки частоты выходного сигнала проводят в режимах непрерывной генерации на частотах: 25,95; 28,00; 30,00; 32,00; 34,00; 37,50 ГГЦ.

Определение кратковременной нестабильности частоты проводят на частоте *f*н = 30,00 ГГц. Частоту измеряют в течение 15 минут с интервалом 1 минута. Нестабильность частоты определяют из выражения (1):

$$\delta_{\text{н}} = \frac{f_{max} - f_{min}}{f_{\text{н}}} \quad (1),$$

Где f_{max} и f_{min} – максимальное и минимальное значение измеренной частоты соответственно.

Определение основной погрешности установки уровня выходной мощности проводят путём измерения уровней мощности: 0 дБм; - 15 дБм; - 30 дБм на частотах 25,95; 28,00; 30,00; 32,00; 34,00; 37,50 ГГЦ. Определение КСВН выхода генератора проводят на этих же частотах.

Результаты поверки генератора считаются положительными, если полученные при поверке значения МХ соответствуют установленным МХ.

УДК 004.056

ДЕСТРУКТИВНОЕ ИНФОРМАЦИОННОЕ ВОЗДЕЙСТВИЕ НА ГРАЖДАН РЕСПУБЛИКИ БЕЛАРУСЬ

Челядинский В.С.[1], студент гр.061402

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В статье представлены результаты анализа распространения недостоверной информации в мировых средствах массовой информации с целью деструктивного информационного воздействия на граждан Республики Беларусь и Российской Федерации.

Ключевые слова. Информационная безопасность, национальная безопасность, информационная война, деструктивное информационное воздействие, средства массовой информации.

Актуальность информационной безопасности растёт с каждым годом, тем самым требуя подготовки новых кадров, протоколов и методов защиты информации, таким образом государство сможет защитить своих граждан от деструктивного информационного воздействия. Концепция информационной безопасности Республики Беларусь базируется на национальных интересах в информационной сфере, понимании основных тенденций современного мира, потенциальных либо реально существующих угроз национальной безопасности. В концепции информационной безопасности Республики Беларусь утвержден термин «деструктивное информационное воздействие», который обозначает информационного влияния на политические и социально-экономические процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности и др. [1].

Термин «информационная война» утвержден в соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности [2] и обозначает противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и др. для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Известно, что средства массовой информации (СМИ) являются одним из важнейших институтов общества, конкурентной площадкой для быстрого распространения информации среди населения. Как правило, некоторые СМИ становятсясубъектамииобъектами информационных войн. СМИ играют важную роль в формировании и эволюции общественного сознания, тем самым оказывая влияние практически на все сферы и институты общества, включая политику, образование, религию. Восприятие и интерпретация важнейших событий в стране и мире осуществляется посредством СМИ. В работе [3] отражена идея подчинения современного мира правилу «реальное событие только тогда существенно, когда о нем широкой публике рассказали средства массовой информации».

В настоящее время в мировых СМИ можно наблюдать выполнения этого правила, так как ведется полноценная информационная война между Россией и странами западной Европы, США. Особое внимание уделяется событиям, происходящим на территории Украины, однако еще раньше страны западной Европы и США вели антироссийскую пропаганду в основном внутри своих стран. Со времён холодной войны между США и СССР были натянутые отношения, в СМИ обсуждали уклад жизни в СССР при коммунизме, ссылки в Сибирь или Гулаг, уголовное преследование невинных людей [4]. Многие писатели отражали в своих произведениях ужас и страх многих событий в СССР, пропагандировали демократический уклад жизни в США [5].

На данный момент Западная пропаганда заключается в том, чтобы настроить население России и Беларуси против действующего правительства. Целью такой пропаганды является распространение недостоверной (фейковой) информации, в которой упоминаются смерти российских солдат и победа военных сил Украины (ВСУ) [6]. Массово распространяются видео ракетного обстрела российскими военными школ, жилых домов, больниц, стрельбы по мирному населению, оккупации городов, террора мирных жителей. Целью данных видео являются призывы

русских военнослужащих сдаться в плен, совершить военное преступление, призывы к гражданам России идти против действующего правительства, выступать на митингах, совершить государственный переворот, однако все эти призывы можно интерпретировать в призывы к совершению преступлений гражданами России, за которые они будут нести административную или уголовную ответственность.

Российское правительство опровергает недостоверную информацию, указывая на аналогию Западной пропагандой с событиями, произошедшими в прошлом. Так, например, оказалось, что видео с кадрами ракетных обстрелов жилых домов в Киеве аналогично военным событиям в Югославии. Новости, распространенные украинскими СМИ, о происшествии на острове Змеином и гибели военнослужащих пограничных войск Украины оказались недостоверными [7].

Примером призыва к восстанию народа против власти могут выступать события августа 2020 года в РБ во время выборов президента РБ. Однако у провокаторов не получилось реализовать задуманные планы в виду недостаточной поддержки населения. Необходимо отметить, что подобная пропаганда в РБ продолжается и сейчас. Распространяются призывы к борьбе с действующим правительством, не только в Беларуси, но и в России [8].

Исходя из вышеизложенного можно сделать вывод, что роль информационной безопасности в информационных войнах стоит на первом месте. Специальные подразделения должны проверять все источники информации, ее подлинность, защищать среды передачи и распространения информации, предоставлять проверенные источники информации обычному населению, предоставлять актуальную информацию. Пренебрежение информационной безопасности может привести к угрозе различным сферам жизни граждан, ухудшению общественного настроения и гражданской войне. Перехват информации, относящейся к государственной тайне, распространение ее неверной интерпретации в СМИ пропагандистами может привести к угрозе национальной безопасности.

Для защиты от деструктивного информационного воздействия в ходе информационных войн следует придерживаться следующих правил:

– рассудительно изучать актуальную информацию из разных источников;

– анализировать получаемую информацию, не поддаваясь внешним или внутренним провокациям.

Надо помнить, что каждый гражданин своей страны самостоятельно выбирает, чему верить, и несет ответственность за свою информационную безопасность. СМИ, социальные сети и интернет ресурсы могут только предоставить актуальную и достоверную информацию, исходя из анализа которой каждый гражданин совершает свой выбор.

Список использованных источников:

1. Концепция информационной безопасности Республики Беларусь / Беларусь Сегодня [Электронный ресурс]. – Опубл. 19.03.2019. – Режим доступа: https://www.sb.by/articles/kontseptsiya-informatsionn – Дата доступа: 30.03.2022.

2. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности / АО «Кодекс» [Электронный ресурс]. – Опубл. 25.12.2013. – Режим доступа: https://docs.cntd.ru/document/499074140 – Дата доступа: 30.03.2022.

3. Почепцов, Г.В. Имиджмейкер / Г.В. Почепцов. – Киев, 2005. – 74 с.

4. Erickson, J Road to Stalingrad: Stalin’s War with Germany. – 1975. – 614 p.

5. Агеносов, В. В. Литература русского зарубежья (1918–1996). – М.: Высш. шк., 1998.

6. Stop Russia 's war against Ukraine [Электронный ресурс]. – Режим доступа: https://www.youtube.com/channel/UCM-nimmmkTsADPgCBqWb5mA/videos – Дата доступа: 30.03.2022.

7. Разоблачение самых популярных фейков о спецоперации в Донбассе / Сетевое издание «Смотрим» [Электронный ресурс]. – Режим доступа: https://smotrim.ru/article/2692688 – Дата доступа: 30.03.2022.

8. Революция несбывшихся надежд. Как Беларусь за год прошла путь от массовых демонстраций к репрессиям / BBC [Электронный ресурс]. – Опубл. 09.06.2021 –Ркжим доступа: https://www.bbc.com/russian/features-58016427 – Дата доступа: 30.03.2022.

UDC 004.056

DESTRUCTIVE INFORMATION IMPACT FOR CITIZENS OF THE REPUBLIC OF BELARUS

Chelyadinsky V.S. student gr.061402

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Belousova E.S. – PhD in technical sciences, associate professor

Annotation. The article presents the results of the analysis of the dissemination of unreliable information in the world mass media with the aim of destructive information impact on the citizens of the Republic of Belarus and the Russian Federation.

Keywords. Information security, national security, information war, destructive information impact, mass media.

УДК 003.26

СТЕГАНОГРАФИЧЕСКОЕ ПРОГРАММНОЕ СРЕДСТВО

Чкоидзе О. Д., студент группы 861401

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Зельманский О. Б. – канд. техн. наук

Аннотация. Проанализированы методы сокрытия данных в цифровых изображениях, а именно метод наименьшего значащего бита и метода двумерного косинусного преобразования, разработано специализированное программное средство, реализующее данные методы.

Ключевые слова. Стеганография, дискретное косинусное преобразование, наименее значимый бит, гаммирование.

На сегодняшний день существует множество способов сокрытия информации в цифровых изображениях, однако многие из них не являются эффективными в части сокрытия самого факта передачи информации, так, например, склеивание цифрового изображения с архивом или запись важной информации в метаданные являются легко обнаружимыми способами передачи информации посредством цифровых изображений, поскольку анализ структуры файла в шестнадцатеричном редакторе позволяет обнаружить скрываемую информацию.

Эффективными методами сокрытия информации в цифровых изображениях являются те методы, которые работают непосредственно с цветовыми информационными каналами изображения. Каналы являются изображениями в градациях серого, которые содержат информацию различного типа. Цветовые информационные каналы создаются автоматически при открытии нового изображения. Например, в изображении RGB есть канал для каждого цвета (красный, зелёный и синий). Также существует альфа-канал, который несёт в себе информацию о прозрачности пикселя. Стоит отметить, что в зависимости от формата изображения, количество каналов может быть разным, так в изображениях формата “Bitmap” существует только 3 цветовых канала, а в изображениях формата “Portable Network Graphics” существует 4 цветовых канала.

К эффективным методам сокрытия информации можно причислить такие методы, как метод наименьшего значащего бита (НЗБ) и множество вариаций метода двумерного косинусного преобразования (ДКП).

В рамках настоящего проекта, был разработан программный модуль, который позволяет работать с различными стеганографическими методами и анализировать их влияние на исходное изображение. Во время разработки была использована библиотека, позволяющая получить из картинки любого формата информацию о цветовых каналах. Сам модуль написан на C++ с помощью Visual Studio 2022.

Метод, который позволяет скрыть наиболее большой объём двоичных данных в пределах одной картинки, является НЗБ (LSB – Least Significant Bit). Суть данного метода заключается в том, что произвольно выбирается один или несколько цветных каналов в которых будет производится скрытие информации, далее определяется первое значение цветового сигнала, одного из выбранных каналов, в формате целого неподписанного числа, то есть числа имеющего значение от 0 до 255, в некоторых случаях это может быть число с плавающей запятой, которое будет варьироваться от 0.0 до 1.0, после чего это число конвертируется в двоичный формат и на него накладывается маска с помощью побитового логического оператора И (AND), которая обнуляет последние два бита данного числа, далее, посредством логического оператора ИЛИ (OR), в освобождённое место, записывается два бита двоичных данных, которые необходимо скрыть в исходном изображении. Этот процесс повторяется до тех пор, пока не будут записаны все входные данные. Стоит учитывать, что, если в одном канале не хватает места для записи двоичных данных в полном объёме, то они записываются в следующий канал, однако в разработанном программном модуле изначально производится фрагментация входных данных с учётом количества выбранных цветовых каналов для записи, это позволило значительно уменьшить последствия изменения цветовых сигналов в одном цветовом канале. Таким образом, исходные данные равномерно распределяются по всем выбранным каналам, сохраняя исходное состояние некоторых пикселей, тем самым уменьшая шанс возможных визуальных дефектов.

Для наглядности рассмотрим изображение, преобразованное данным методом (рис.1, 2). Входными данными в этом случае выступала строчка с цифрами от нуля до тридцати (81 байт двоичной информации), а запись производилась равномерно по всем цветовым каналам. Исходное изображение имело формат PNG (Portable Network Graphics) и размеры 512 на 512 пикселей.

Рисунок 1 – Исходное изображение

Рисунок 2 – Преобразованное изображение

Как можно видеть, визуальных дефектов не наблюдается, а следовательно факт передачи информации остался в тайне.

Размер двоичных данных (I), которые потенциально можно скрыть в данном изображении рассчитывается по следующей формуле:

$$I = \frac{((W \times H) \times 8) \times N}{2},$$

где W – ширина исходного изображения;

H – высота исходного изображения;

N – количество цветовых каналов.

После произведения расчётов, получаем размер в 3145728 бит или 384 килобайт, не учитывая канал прозрачности. Необходимо понимать, что цена за большой объём двоичной информации, которую позволяет скрыть этот метод, является его неустойчивость к повреждениям или изменениям преобразованного изображения.

Метод ДКП (DCT – Discrete Cosine Transform), вариация Коха-Жао. Преимущество данного метода заключается в его стойкости к повреждениям или изменениям преобразованного изображения, однако, как и с предыдущим методом у этого преимущества есть своя цена, заключается она в малом потенциальном объёме данных, которые может быть скрыто в изображении.

Суть метода заключается в том, чтобы фрагментировать выбранные цветовые каналы на блоки 8 на 8 сигнальных коэффициентов каждый и применить к ним формулу ДКП. После этого получаются матрицы размером 8 на 8, в которых будут хранится коэффициенты ДКП. Далее пользователь должен произвольно выбрать случайное число и два индекса среднечастотных коэффициентов ДКП с помощью которых будет выполнятся интеграция скрываемых данных в исходное изображение. Следующим шагом будет циклический проход по каждой из матриц ДКП, учитывая размер входных данных, во время которого будут произведены изменения над выбранными пользователем двумя коэффициентами ДКП по следующим правилам:

1) Находится модуль каждого из двух коэффициентов, и вычисляется их разность.
2) При записи бита равного единице эта разность должна быть больше заданного пользователем случайного числа. В противном случае эти коэффициенты изменяются так, чтобы это правило выполнялось. В разработанном программном модуле эти коэффициенты обмениваются значениями.
3) При записи бита равного нулю эта разность должна быть меньше, заданного пользователем, случайного числа. В противном случае выполняется то, что было оговорено ранее.

После завершения цикла к каждой из изменённых матриц применяется формула обратного двумерного косинусного преобразования (ОДКП). Значения коэффициентов результирующей матрицы ОДКП будут представлять новые значения цветовых сигналов, которые в дальнейшем будут записаны в соответствующий цветовой канал (рис. 3). Необходимо учитывать, что выходные коэффициенты ОДКП могут выходить за пределы значений цветового сигнала, в связи с этим, каждый коэффициент должен пройти через функцию нормирования, при этом может произойти потеря или искажение входных данных, исходя из этого, можно сделать вывод, что, чем больше случайное значение, выбранное пользователем, тем вероятнее то, что после прохождения через функцию нормирования данные останутся без искажений.

Для чтения данных цветовые каналы фрагментируются на блоки 8 на 8 сигнальных коэффициентов, на их основе вычисляются матрицы с коэффициентами ДКП, после чего сравниваются значения коэффициентов с учётом выбранных ранее индексов в матрице. Если первый коэффициент больше второго, то в буфер данных записывается бит со значением 1, в противном случае записывается бит со значением 0.

Рисунок 3 – Преобразованное изображение

Для расчёта ДКП используется следующая формула [1]:

$$\mathrm{DCT}(u, v) = \frac{1}{\sqrt{2N}} C(u) C(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \mathrm{signal}[i][j] \cos\frac{(2i+1)u\pi}{2N} \cos\frac{(2j+1)v\pi}{2N}$$

$$C(x) = \frac{1}{\sqrt{2}} \text{ if } x \text{ is } 0, \text{else } 1 \text{ if } x > 0,$$

где u – индекс смещения по ширине в матрице ДКП;

v – индекс смещения по высоте в матрице ДКП;

N – размерность матрицы ДКП;

signal – матрица цветовых сигналов;

i – индекс смещения по ширине в матрице цветовых сигналов;

j – индекс смещения по высоте в матрице цветовых сигналов.

Для расчёта ОДКП используется следующая формула [3]:

$$\mathrm{IDCT(i,j)} = \frac{1}{\sqrt{2\mathrm{N}}}\sum_{\mathrm{u=0}}^{\mathrm{N-1}}\sum_{\mathrm{v=0}}^{\mathrm{N-1}} \mathrm{C(u)C(v)DCT[u][v]}\cos\frac{(2\mathrm{i}+1)\mathrm{u}\pi}{2\mathrm{N}}\cos\frac{(2\mathrm{j}+1)\mathrm{v}\pi}{2\mathrm{N}}$$

$$C(\mathrm{x}) = \frac{1}{\sqrt{2}} \text{ if x is } 0, \text{else } 1 \text{ if x} > 0,$$

Для расчёта размера двоичных данных (I), которые потенциально возможно записать в коэффициенты ДКП используется следующая формула:

$$\mathrm{I} = ((\frac{\mathrm{W}}{\mathrm{L}} \times \frac{\mathrm{H}}{\mathrm{L}})) \times \mathrm{N},$$

где L – размерность матрицы.

После произведения расчёта размера получается число в 12288 бит или 1,536 килобайт (на 3 канала). Таким образом, при устойчивости данного алгоритма к повреждениям преобразованного изображения, он имеет малый объём информации на один цветной канал.

Предварительное использование алгоритма шифрования на блоке входных данных является важной составляющей сокрытия факта передачи информации по стегоканалу, так как представленные стеганографические алгоритмы являются публичными и довольно известными. Однако, возникает очевидная проблема, связанная с возможным повреждением или изменением преобразованного изображения при передаче через физический канал или сжатию, поэтому ассиметричные шифры могут привести к полной потере скрытой информации. Для решения данной проблемы применяется симметричный шифр, а именно – гаммирование, смысл которого заключается в наложении последовательности случайных чисел на буфер с входными данными. Данная последовательность называется гамма-последовательностью и используется для шифрования и дешифрования данных. Клод Шеннон доказал, что при определённых свойствах гаммы этот метод шифрования является абсолютно стойким. Следующие требования к гамма-последовательности обязательно должны быть соблюдены [2]:

1) Для шифрования каждого нового сообщение нужно использовать новую гамму.
2) Для формирования гаммы нужно использовать аппаратные генераторы случайных чисел, основанные на физических процессах.
3) Длина гаммы должна быть не меньше длины защищаемого сообщения.

Рассмотрим результаты дешифрования данных с наложением искусственных повреждений при использовании ранее рассмотренного стеганографического метода ДКП в вариации Коха-Жао (рис. 4).

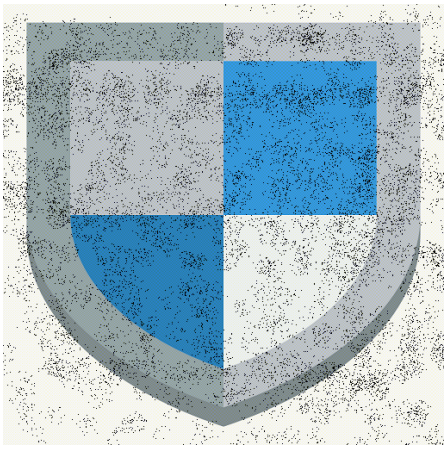


Рисунок 4 – Преобразованное изображение с наложением искусственного шума

Исходные данные: “1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30”

Результат дешифрования данных: “1 2 3 4 5 6 7 8 9 10 11 12 11 14 15 16 17 18 19 20 21 22 23 24дг5 26 27 28 29 3р”.

Исходя из результатов, можно сделать вывод, что при повреждении преобразованного изображения, из стегоканала возможно частичное извлечение данных, хоть и с определённым количеством ошибок.

В рамках данной работы было разработано программное средство, позволяющее анализировать и работать со стеганографическими методами. На сегодняшний день передача данных с помощью стегоканалов остаётся довольно актуальной и может быть использована как для доставки вредоносного кода, так и для передачи засекреченных сообщений. Предложенное программное средство может быть усовершенствовано путем добавления дополнительных стеганографических методов с целью увеличения объема передаваемой информации и стойкости шифрования, а также с целью изучения и сравнительного анализа различных методов сокрытия и шифрования информации, так как базовый код полностью основан на структурах и классах, предназначенных для работы с пикселями изображений и с информацией, разбивая её на битовые буферы.

Список использованных источников:

1. Lossy Data Compression: JPEG / Standford University [Электронный ресурс]. – Режим доступа: https://cs.stanford.edu/people/eroberts/courses/soco/projects/data-compression/lossy/jpeg/dct.htm - Дата доступа: 04.04.2022
2. Гаммирование / Wikipedia [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Гаммирование - Дата доступа: 04.04.2022
3. Computer graphics / Stanford University [Электронный ресурс] – Режим доступа: http://nifty.stanford.edu/2003/pests/2002/lectures/08.2_graphics/TwoDimensions.html?CurrentSlide=13 Дата доступа: 05.04.2022

UDC 003.26

STEGANOGRAPHY SOFTWARE TOOL

Chkoidze O. D., student of the group 861401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Zelmansky O.B. - PhD

Annotation. The methods of hiding data in digital images, namely the method of the least significant bit and the method of two-dimensional cosine transform, have been analyzed, a specialized software tool has been developed that implements these methods.

Keywords. Steganography, discrete cosine transform, least significant bit, additive cipher.

УДК 003.26

МОДУЛЬ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Шакин К.П., Мухыев Н. А, Сокаше И.Л.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Предложен модуль синтеза речеподобных сигналов путем формирования псевдотекста на основании особенностей различных языков и его последующее озвучивание методом компиляции заранее выделенных из речи аллофонов. Данный модуль предназначен для защиты речевой информации от утечки по техническим каналам.

Развитие цифровизации неразрывно связано с защитой информации, которая является одним из наиболее важных активов любой организации. В связи с этим одной из проблем информационной безопасности является утечка информации по акустическому каналу. Защита речевой информации является важным направлением по обеспечению информационной безопасности и реализуется при помощи пассивных и активных методов защиты информации. Активные методы защиты речевой информации предполагают применение генераторов белого, розового и речеподобного шума, для создания маскирующих шумовых помех. Доказано, что для эффективного маскирования помеха по своему спектральному составу должна быть близка к речевому сигналу.

Для генерации речеподобного сигнала предлагается применить компиляционный метод синтеза речи, заключающийся в соединении сформированных минимальных акустических единиц – аллофонов. При этом формирование базы данных звуковых фрагментов для русского языка осуществляется на основании артикуляционных слоговых и словесных таблиц, соответствующих ГОСТ 16600-72 [1].

Разработанный модуль защиты речевой информации [2] выполняет следующие функции: формирование фонемного псевдотекста, компиляцию речеподобного сигнала и его воспроизведение. Структурная схема предлагаемого модуля представлена на рисунке 1.

Рисунок 1 – Структурная схема модуля защиты речевой информации

В свою очередь формирование фонемного псевдотекста осуществляется в соответствии с предложенными в [3, 4] правилами и алгоритмом на основании особенностей языка, на котором ведется конфиденциальный разговор. Были исследованы особенности русского, арабского, казахского и туркменского языков с целью достижение наибольшего подобия генерируемого речеподобного сигнала речи на соответствующем языке.

В результате на выходе модуля формируется речеподобная помеха, которая в дальнейшем поступает на вход акустической системы.

Список использованных источников:

1. Авдеев В.Б., Трушин В.А., Кунгуров М.А. Унифицированная речеподобная помеха для средств активной защиты речевой информации. // Информатика и автоматизация. 2020. Том 19 № 5.

2. Шакин, К.П. Разработка системы синтеза речеподобного сигнала / К.П. Шакин, О.Б. Зельманский // Технические средства защиты информации: материалы XIX Белорус.-российск. науч.-техн. конф., Минск, 8 июня 2021 г. / БГУИР ; редкол.: Т.В. Борботько [и др.]. – Минск, 2021. – С. 99.

3. Воробьев В.И., Давыдов А.Г., Лобанов Б.М. // XIII сессия Российского акустического общества: Сб. тр. Н. Новгород, 25–29 августа 2003 г. / М., 2003. Т. 3.

4. Лобанов Б.М. Синтез речи по тексту. Сборник научных трудов 4-й Международной школы-семинара по искусственному интеллекту. Мн.: БГУИР, 2000.

УДК 537.531

УМЕНЬШЕНИЕ ВЕРОЯТНОСТИ ОШИБКИ ПРИ ПЕРЕДАЧЕ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ ПО РАДИОКАНАЛУ

Шилко К.Н.

Белорусский государственный университет информатики и радиоэлектроники,

г. Минск, Республика Беларусь

Белошицкий А. П. – кандидат технических наук, доцент

Доклад посвящен проблеме уменьшения вероятности ошибки при передаче телеметрической. Приводится оценка погрешности телеизмерений из-за наличия помех и рекомендаций по их уменьшению.

В буквальном смысле телеметрия - означает измерение на расстоянии. Содержание современной телеметрии составляет широкий круг задач, связанных с получением, преобразованием, передачей и обработкой измерительной информации, используемой при управлении удаленными объектами, определении их состояния, изучении физических процессов в местах, где непосредственное присутствие наблюдателя затруднено или невозможно. Основные части телеметрической системы — передающая часть и приемно-регистрирующая часть.

В современных информационных телеметрических системах в состав их передающей части входит аппаратура предварительной обработки информации, обеспечивающая сокращение избыточности передаваемых сообщений, получение обобщённых данных, согласование производительности системы с пропускной способностью канала связи и решение других задач.

Приемно-регистрирующая аппаратура обеспечивает прием, селекцию, декодирование, регистрацию и отображение телеметрической информации. Принятый сигнал с выхода приемника поступает в устройство селекции и декодирования. Здесь осуществляется выделение части телеметрических сигналов, которые поступают в устройство визуального отображения данных. Этим достигается возможность оперативного контроля наиболее важных параметров в темпе приема информации. Одновременно весь поток принимаемых данных после необходимых преобразований поступает на вход регистрирующего устройства.

Основными операциями первичной обработки телеметрической информации являются дешифровка данных, отбраковка ошибок, усреднение отсчетов, выделение экстремальных значений параметров, контроль за отклонением от номинальных значений и некоторые другие операции.

Основным видом информации, принимаемым от передающей части, является телеметрическое сообщение. Телеметрическое сообщение – это сообщение, передаваемое телеметрической системой, несущее информацию о контролируемых событиях и процессах. Значащая часть сообщения представлена в виде *k*-значных двоичных чисел с повышенной точностью.

Шумы и помехи в канале связи искажают кодовые комбинации, что приводит к ошибкам при декодировании. Для повышения качества передачи используются специальные корректирующие коды, обнаруживающие и исправляющие часть ошибок [1].

Однако ни один код не может исправить все ошибки. Это означает, что после декодирования принятые *k*-значные двоичные числа регистрируются с вероятными ошибками в одном или нескольких разрядах. В настоящее время при традиционном использовании блочных кодов показателем эффективности является вероятность ошибки декодирования. При этом вопрос о величине той или иной ошибки (о «цене» ошибки), т.е. об ущербе, возникающем при ее возникновении, остается вне внимания теории корректирующих кодов. Оценим погрешности телеизмерений из-за наличия помех.

Если передается числовое сообщение m_i , записанное в виде k-значной кодовой комбинации, а приемник регистрирует сообщение m_j, то разность между ними можно записать в виде вектора ошибки Δ_{ij} (в виде k-значного числа):

$$\Delta_{ij} = m_i - m_j, (1)$$

где единицами отмечены разряды, принятые с ошибкой. Рассмотрим ситуации, когда наиболее вероятными являются одиночные ошибки. Модуль ошибки в s-разряде (s = 1, 2, …, k) однозначно зависит от номера ошибочного разряда:

$$|\Delta_s| = 2^{s-1}, (2)$$

Рассмотрим совокупность ошибок, вызванных поражением помехами каждого из k разрядов. Используем сделанное выше допущение о статистической независимости таких событий, как композицию случайных потоков ошибок с индивидуальными статистиками. Воспользуемся выражением для суммарной интенсивности потока ошибок при приеме [2]:

$$\Delta_c^{-2} = \sum_{s=1}^{n} \Delta_s^{-2} P_s = \sum_{s=1}^{k} 2^{2(s-1)} P_s, (3)$$

где s – разряд с ошибкой, k – разряд, n – кол-во ошибок, P_s -поток ошибок. Среднеквадратичная величина из формулы выше находится в виде:

$$\Delta_c = \sqrt{\sum_{s=1}^{k} 2^{2(s-1)} P_s} = \frac{M}{2} \sqrt{\sum_{s=1}^{k} 2^{2(s-k)} P_s}, (4)$$

Из выражения (4) следует, что если при приеме сигнала происходит ошибка в том или ином разряде исходной кодовой комбинации, то цена ошибки, т.е. погрешность измерения, будет существенно зависеть от номера пораженного разряда – чем старше разряд, тем выше погрешность.

Проведенный анализ позволяет сделать вывод о целесообразности построения канала передачи цифровой телеметрической информации таким образом, чтобы при заданных ограничениях на скорость передачи и мощность передатчика в максимальной степени обеспечить защиту от помех старших по иерархии разрядов принимаемого кода и за счет этого минимизировать погрешность телеизмерений.

Список использованных источников:

1. Питерсон, У. Коды, исправляющие ошибки /У. Питерсон, Э. Уэлдон- М.: Мир, 1976. – 595 с.
2. Вентцель, Е.С. Теория вероятностей /Е.С. Вентцель - М.: Наука, 1964. – 575 с.

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

УДК 628.336.42

АЛГОРИТМЫ ОБРАБОТКИ МУЛЬТИСПЕКТРАЛЬНЫХ ИЗОБРАЖЕНИЙ СО СПУТНИКОВ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Манулик П.В.1, студент гр.962991

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – канд. физ.-мат. наук

Аннотация. В работе описаны основные алгоритмы обработки мультиспектральных снимков со спутников дистанционного зондирования Земли, основанные на вегетационных индексах и способности растительного покрова земли поглощать и отражать различные спектральные составляющие светового потока.

Ключевые слова. Мультиспектральные изображения, вегетационные индексы, картография, спутники дистанционного зондирования, количественная оценка зелёности.

Дистанционное зондирование – процесс, посредством которого собирается информация об объекте, территории или явлении без непосредственного контакта с ним. [1] Для осуществления зондирования земной поверхности используются летательные воздушные и космические аппараты. Наибольший объём данных предоставляется мультиспектральными изображениями со специализированных спутников дистанционного зондирования. Снимок определяется как изображение конкретных объектов, получаемое целенаправленно в результате дистанционной регистрации или измерения собственного и отражённого излучения.

Для обработки мультиспектральных снимков используют различные алгоритмы, целью которых является определение состояния земной поверхности на момент съёмки. Результатом обработки являются количественные и качественные оценки состояния поверхности. Наиболее распространёнными алгоритмами являются алгоритмы на основе вегетационных индексов, позволяющие определить состояние растительного покрова на изображении.

Основными вегетационными индексами являются относительный вегетационный индекс (Ratio VI, RVI) и нормализованный разностный вегетационный индекс (Normalized Difference VI, NDVI). Данные индексы базируются на двух наиболее стабильных участках спектральной кривой отражения света растениями: инфракрасном и красном. На красную область спектра (0,6-0,7 мкм.) приходится максимум поглощения солнечной радиации хлорофиллом высших сосудистых растений, а в инфракрасной области (0,7-1,0 мкм) находится область максимального отражения клеточных структур листа (рисунок 1). [2]

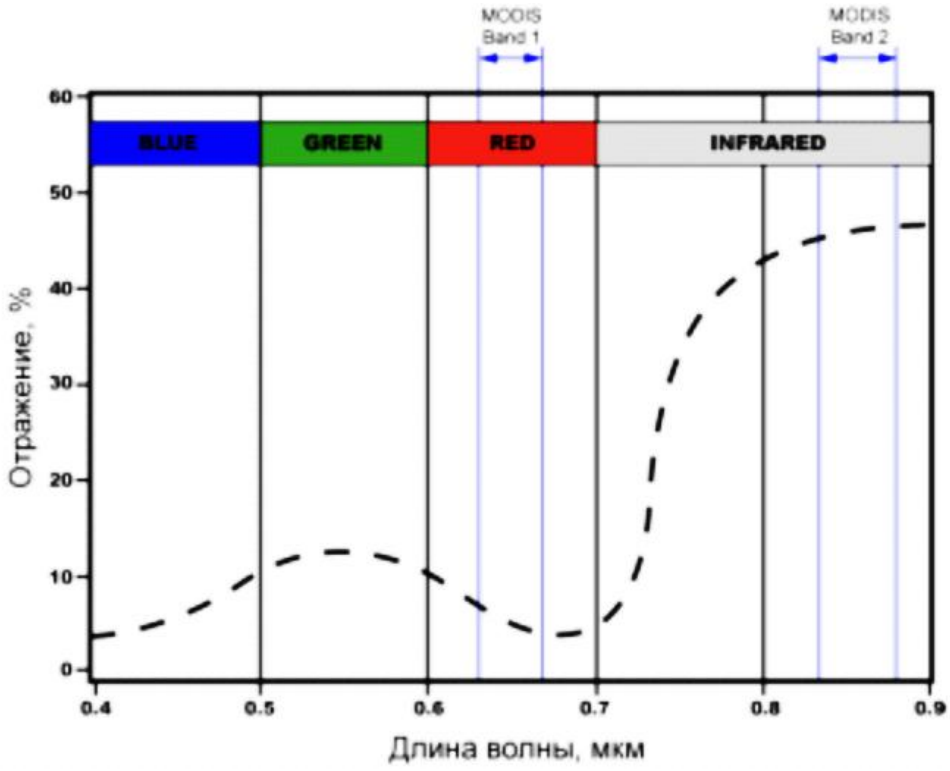


Рисунок 1 – спектральная кривая поглощения солнечной радиации хлорофиллом

Расчёт индексов производится на основе изображений, имеющих спектральные каналы в красном и инфракрасном диапазоне. Для отображения количественной оценки на изображении используются дискретные цветовые шкалы, на которых значению индекса соответствует цвет от чёрного (полное отсутствие растительности), до тёмно-зелёного (выское содержание растительности в рассматриваемой области). Пример шкалы для индекса NDVI представлен на рисунке 2.

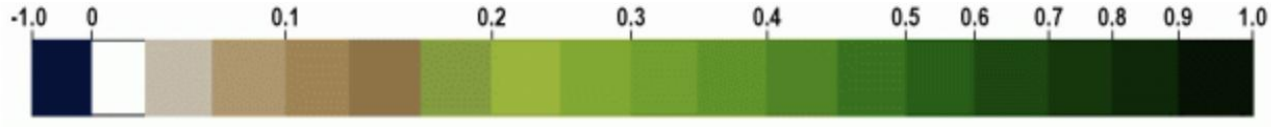


Рисунок 2 – дискретная шкала показателей индекса NDVI.

Относительный вегетационный индекс основан отношении ближней инфракрасной и красной составляющей спектра:

$$RVI = \frac{NIR}{RED}, \quad (1)$$

где NIR – ближняя инфракрасная составляющая спектра.

RED – красная составляющая спектра.

Нормализованный разностный вегетационный индекс основан на отношении разности ближнего инфракрасного диапазона и красного диапазона к сумме инфракрасного и красного диапазонов:

$$NDVI = \frac{(NIR-RED)}{(NIR+RED)}, \quad (2)$$

где NIR – ближняя инфракрасная составляющая спектра.

RED – красная составляющая спектра.

Индексы между собой функционально равнозначны и связаны отношением:

$$NDVI = \frac{(RVI-1)}{(RVI+1)}, \quad (3)$$

где RVI – относительный вегетационный индекс.

Данные два индекса являются основными, фундаментальными индексами оценки, продолжением которых являются модифицированные вегетационные индексы, осуществляющие коррекцию данных с учётом атмосферы, погодных условий и данных о составе растительности на исследуемой территории. [3]

Таким образом, индексы вегетации растительности позволяют количественно и качественно оценить состояние растительного покрова. Однако, для каждого случая требуется применять индекс, подходящий под текущие условия. В большинстве случаев, для анализа данных достаточно использовать NDVI индекс, однако, при ухудшении погодных условий или уменьшения количества растительности на исследуемой территории, требуется применение помехоустойчивых индексов, работающих с изображениями с разреженной растительностью.

Список использованных источников:

1. Сутырина, Е.Н. Дистанционное зондирование Земли : учеб. пособие /Е.Н. Сутырина. – М. : Изд-во Иркутск ИГУ, 2013. – 166 с.
2. Kriegler, F. J., Malila, W. A., Nalepka, R. F., and Richardson, W. (1969) "Preprocessing transformations and their effects on multispectral recognition, in _Proceedings of the Sixth International Symposium on Remote Sensing of Environment, University of Michigan, Ann Arbor, MI, pp.97-131.
3. Deering, D.W. Rangeland reflectance characteristics measured by aircraft and spacecraft sensors / D.W. Deerind. – Ph.D. Diss Texas A&M Univ., College Station, 1978 – 388 p.

УДК 628.336.42

СПОСОБ РАСЧЕТА СПЕКТРА МОЩНОСТИ СИГНАЛОВ МЕТОДОМ ТЬЮКИ

Горбачева Д.Н., студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель каф. ИКТ

Аннотация. Этот метод позволяет получать оценку спектральной плотности мощности через преобразование Фурье оценки корреляционной функции.

Ключевые слова. спектральной плотности, преобразование Фурье, корреляционная функцию, оценок спектральной плотности мощности, временной сдвиг, математическое ожидание, дисперсия оценки Тьюки.

Этот метод позволяет получать оценку спектральной плотности мощности через преобразование Фурье оценки корреляционной функции. Следует отметить, что метод Блэкмана-Тьюки (коррелограммный метод) был разработан в 1958 г., тогда как алгоритм БПФ для эффективного вычисления ДПФ не был опубликован до 1965 г. Кроме того, этот метод имеет некоторые преимущества по сравнению с методом периодограмм. Например, метод Блэкмана-Тьюки характеризуется большей добротностью. К тому же, корреляционную функцию теперь можно вычислять с помощью ДПФ посредством быстрой корреляции.

Одна из возможных оценок спектральной плотности мощности, получаемая на основе несмещённой оценки корреляционной функции $\hat{K}_x(m)$, которая вычисляется при временном сдвиге с максимальными значениями в интервале $\pm L$, определяется выражением

$$\hat{P}_{\text{вт}}(f) = \Delta t \sum_{m=-L}^{L} \hat{K}_x(m) \exp(-j2\pi f m \Delta t).$$

Данная оценка определяется для интервала частот $-\frac{1}{2\Delta t} \le f \le \frac{1}{2\Delta t}$. Максимальное значение временного сдвига *L*, как правило, меньше числа отсчетов *N* выборки исходных данных. Использовать максимальное значение $L \simeq N/10$ было предложено Блэкманом и Тьюки. Выбор такого максимального значения основывался на стремлении исключить большие значения дисперсии, связанные с оценками корреляционной функции при больших временных сдвигах, поскольку такие значения дисперсии давали менее устойчивую оценку СПМ.

Математическое ожидание оценки (1.246) можно вычислить обычным образом:

$$M[\hat{P}_x(f)] = \Delta t \sum_{m=-L}^{L} M[\hat{K}_x(m)] \exp(-j2\pi f m \Delta t) = \Delta t \sum_{m=-L}^{L} K_x(m) \exp(-j2\pi f m \Delta t) = P_x(f) * W_L(f),$$

(1.247)

где $W_L(f)$ – преобразование Фурье прямоугольного окна (ядро Дирихле).

Несмотря на то, что оценка СПМ вычисляется с использованием несмещенных оценок корреляционной функции, она будет смещенной оценкой истинной спектральной плотности мощности. Неявное присутствие прямоугольного окна при конечной корреляционной последовательности приводит к оценке, которая, по сути, является сверткой истинной спектральной плотности мощности с преобразованием Фурье дискретно-временного прямоугольного окна.

Для уменьшения эффекта просачивания из-за неявного присутствующего прямоугольного окна, а следовательно, и для уменьшения смещения оценки необходимо использовать (2*L* + 1)-точечное корреляционное окно *w*(*n*) нечетной длины на интервале $-L \le m \le L$, симметричное относительно начала отсчета. Наиболее общая форма корреляционного метода оценивания СПМ в этом случае принимает следующей вид:

$$\hat{P}_{\text{вт}}(f) = \Delta t \sum_{m=-L}^{L} \hat{K}_x(m) w(n) \exp(-j 2\pi f m \Delta t)$$

где должна использоваться несмещенная оценка корреляционной функции.

Выражение (1.248) и определяет оценку, которая была предложена Блэкманом и Тьюки, о чем свидетельствует подсрочный индекс *BT*. Окно здесь нормируется так, чтобы *w*(0) = 1, поэтому оценка $\hat{K}_x(0)$ будет несмещенной, мощность отсчетов сохраняется, а следовательно, оценка $\hat{P}_{\text{вт}}(f)$ будет правильно промасштабирована как оценка СПМ. Если необходимо, чтобы не площадь под кривой оценки Блэкмана и Тьюки была пропорциональна мощности истнной СПМ, а пики этой оценки были пропорциональны мощности импульсов в спектре, то выражение (1.248) следует промасштабировать величиной $1/N\Delta t$. Не следует применять корреляционные окна, Фурье-образ которых меньше нуля, поскольку это приводит к получению отрицательных значений СПМ, что противоречит ее физическому смыслу. Не все весовые функции удовлетворяют данным критериям. Например, им не удовлетворяют функции Хемминга и Ханна, Кайзера и прямоугольное окно. С увеличением числа значений оценки $\hat{K}_x(m)$ коррелограммный метод дает асимптотически несмещенные оценки СПМ. Блэкман и Тьюки рекомендовали использовать число оцениваемых значений корреляционной последовательности примерно равному 10 % числа имеющихся отсчетов данных.

Дисперсия оценки Блэкмана и Тьюки определяется выражением:

$$D[\hat{P}_{\text{вт}}(f)] \approx \left[\frac{1}{N} \sum_{m=-L}^{L} w^2(m) \right] \cdot P_x^2(f).$$

Очевидно, что при $N/L \to \infty$ $D[\hat{P}_{\text{вт}}(f)] \to 0,$ так что при данных условиях оценка Блэкмана и Тьюки является состоятельной.

Для вычисления оценки СПМ, определяемой выражением (1.248), на сетке из (*N* + 1) частот $f_k = k/N\Delta t,$ где используют алгоритмы БПФ. Значение *N* здесь может быть произвольным, но обычно $N \gg L,$ а это значит, что полученная оценка будет сохранять тонкие детали спектра. При использовании значений временного сдвига от *L* + 1 до *N* отсчеты имеющихся данных необходимо дополнить нулями.

+Сравнивая процедуру Блэкмана и Тьюки с периодограммным методом, нетрудно заметить, что в этом случае сглаживание достигается не за счет усреднения нескольких периодограмм, а за счет усредняющего эффекта процесса корреляции.

UDC 628.336.42

METHOD FOR CALCULATION OF THE POWER SPECTRUM OF SIGNALS BY THE TUKEY METHOD

Gorbacheva D.N. st.933701

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Daneyko T.M. - scientific director

Annotation. This method allows to obtain an estimate of the power spectral density through the Fourier transform of the correlation function estimate.
Keywords. spectral density, Fourier transform, correlation function, power spectral density estimates, time shift, mathematical expectation, Tukey estimate variance.

УДК 628.336.42

АЛГОРИТМ ДОСТИЖЕНИЯ КОНСЕНСУСА ПОСРЕДСТВОМ БЛОКЧЕЙНА ETHEREUM

Жовнерик А.В., студентка группы 863102

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Саломатин С.Б. – к.т.н.,доцент

Аннотация. Актуальность данной работы связана с большим количеством взломов приложений, которые имеют централизованную структуру и непрозрачность в обработке и сбора данных посредниками. Цель работы - продемонстрировать феномен децентрализации через смарт-контракт Voting, развернутый в сеть Rinkeby.

Ключевые слова. Блокчейн Ethereum, смарт-контракт, криптография, распределенные системы.

Информационно-коммуникационные технологии (ИКТ) традиционно основываются на централизованной парадигме, в которой база данных или серверы приложений находятся под чьим-то единоличным управлением.

Децентрализация является основным преимуществом, предоставляемым технологией блокчейн, ее ключевым сервисом. Консенсус – основание блокчейна, которое обеспечивает децентрализацию и контроль при помощи майнинга.

В качестве платформы для построения приложения были проанализированы возможности Ethereum, TON и Hyperledger.

Ethereum – проект, в роли ключевой идеи которого выступает разработка тьюринг-полного языка, который позволяет создавать программное обеспечение произвольной сложности (smart contracts) для блокчейна и децентрализованных приложений [1]. Новшество Ethereum заключается в том, что любая выполняемая внутри него операция одновременно выполняется каждым отдельным узлом во всей сети. Состояние Ethereum включает в себя огромное количество транзакций. Эти транзакции группируются в «блоки».

Блок содержит группы транзакций, а каждый блок связан с предыдущим, тем самым образуя цепочку.

EVM (Ethereum Virtual Machine) – стековая, полностью изолированная среда выполнения, которая изменяет состояние системы с помощью инструкций в виде байт-кода [2]. Память не ограничена по размеру, но требует уплаты комиссии в виде газа. Хранилище виртуальной машины позволяет обращаться к данным по ключу и является частью состояния системы. Ключи и значения занимают по 32 байта. Программный код находится в виртуальной памяти, доступной только для чтения(анг. Virtual read-only memory, или VROM). VROM хранит код программы, который копируется в основную память. Затем EVM считывает основную память, ссылаясь на счетчик программы, и последовательно выполняет лексемы кода. Счетчик и стек виртуальной машины обновляются соответствующим образом после выполнения каждой инструкции(см. рисунок 1).

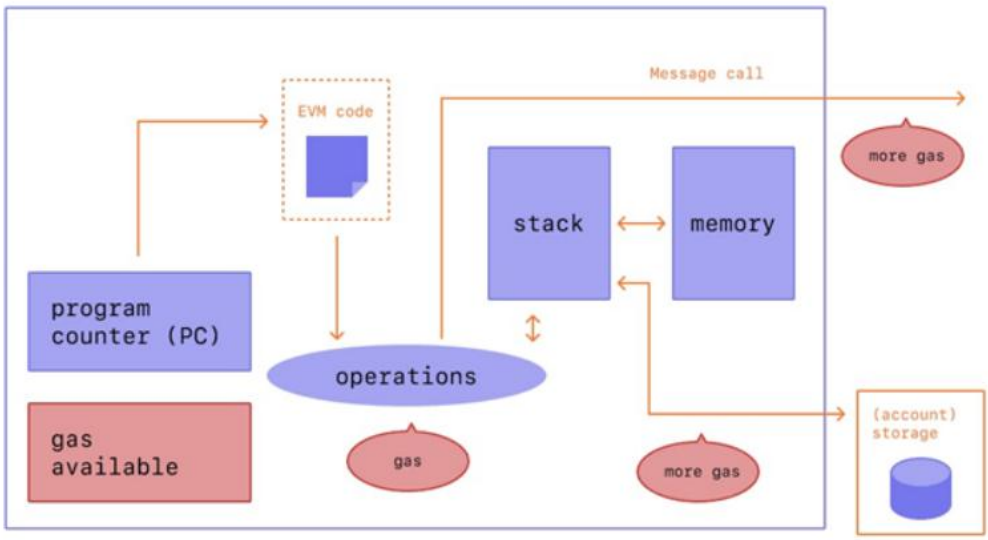


Рисунок 1 – Схема работы EVM

Учетная запись состоит из криптографической пары ключей: public и private. Public key генерируется из private key с помощью алгоритма ECDSA.

Смарт-контракт – это компьютерный алгоритм, который контролирует выполнение обязательств сторон в процессе обмена активами в технологии блокчейн [3]. Когда смарт-контракт работает на блокчейне, он автоматически запускается, когда выполняются все необходимые условия. Вся структура основана и проверена множеством подключенных компьютеров(см. рисунок 2) Это гарантирует, что смарт-контракты: безопасные, открытые, заслуживают доверия, почти лишены любых возможных ошибок.

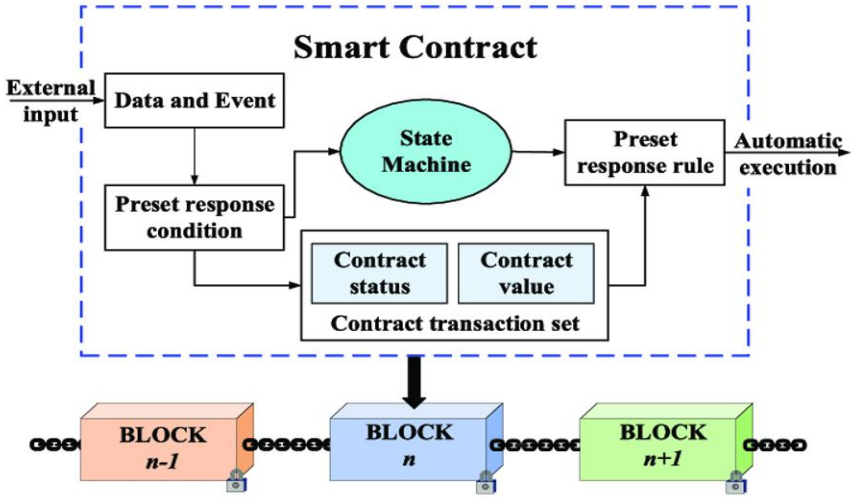


Рисунок 2 – Функционирование смарт-контракта в Ethereum

В рамках дипломной работы был разработан смарт-контракт(см. рисунок 3) на платформе Ethereum, предназначенный для голосований с возможностью других пользователей выбрать победителя и развернутый в тестовой сети Rinkeby.

Rinkeby — тестовая сеть Ethereum, которая позволяет проводить тестирование разработки блокчейна перед развертыванием в Mainnet, основной сети Ethereum [4].

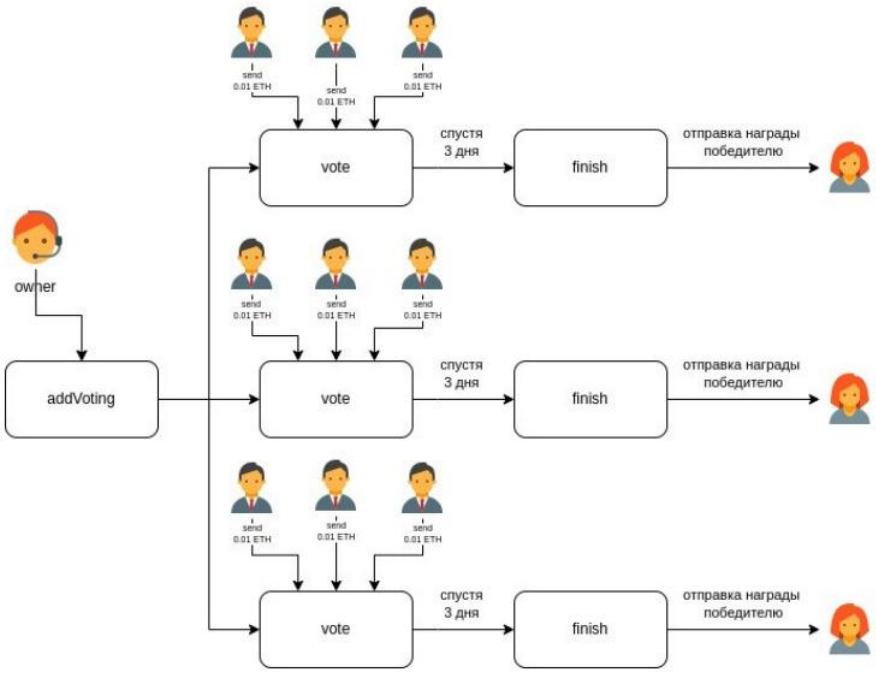


Рисунок 3 – Смарт-контракт Voting

Работа представляет интерес с практической точки зрения. Смарт-контракт, созданный в рамках данной дипломной работы, может быть использован для организации онлайн-голосования пользователей в сети Интернет.

Список использованных источников:

1. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты/пер. с анг.М.А. Райтмана. – М.:ДМК Пресс, 2019. – 538 с.: ил.
2. Yellow Paper Ethereum [Электронный ресурс]. – Режим доступа: Ethereum Yellow Paper: a formal specification of Ethereum, a programmable blockchain
3. Смарт-контракт, Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Смарт-контракт
4. Ethereum: работа с сетью, смарт-контракты и распределенные приложения / А. Бурков — «ЛитРес: Самиздат», 2020

UDC 628.336.42

Consensus algorithm through the ethereum blockchain

Zhauneryk A.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Salomatin S.B. – candidate of technical sciences

Annotation. The relevance of this work is due to the large number of hacks of applications that have a centralized structure and lack of transparency in the processing and collection of data by intermediaries. The goal is to demonstrate the phenomenon of decentralization through a smart contract voting based on the Ethereum blockchain, deployed in the Rinkeby network.

Keywords. Blockchain Ethereum, smart contract, cryptography, distributed systems.

УДК 628.336.42

РАСЧЕТ ЦИФРОВЫХ РЕКУРСИВНЫХ ФИЛЬТРОВ ПО ДАННЫМ АНАЛОГОВЫХ

Кирилюк Н.Н., студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – магистр технических наук

Аннотация. Данная работа рассматривает вопрос расчета цифровых фильтров с помощью аналоговых характеристик. В работе указан метод расчета билинейного преобразования.

Ключевые слова. Рекурсивный фильтр, частотная характеристика, частотное преобразование, прямой метод, косвенный метод, норма, передаточная функция.

При расчете рекурсивных фильтров применяются прямые и косвенные методы.

Косвенный метод предполагает в качестве промежуточного этапа расчета аналогового фильтра (АФ). Затем по передаточной функции АФ получают схему цифрового фильтра (ЦФ).

Рассмотрим метод билинейного преобразования:

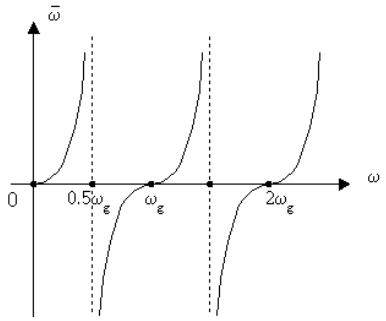
Основой этого метода является такое преобразование частоты, при котором частотная характеристика АФ сжимается до конечных размеров. В результате ошибок наложения, которые всегда существуют при переходе от АФ к ЦФ, частотные преобразования осуществляются с помощью выражения:

$$\frac{\bar{\omega}T}{2} = \operatorname{tg}\frac{\omega T}{2} \quad \text{где} \quad \bar{\omega} \to \bar{p} = \bar{\sigma} + j\bar{\omega} \quad ; \quad \omega \to p = \sigma + j\omega$$

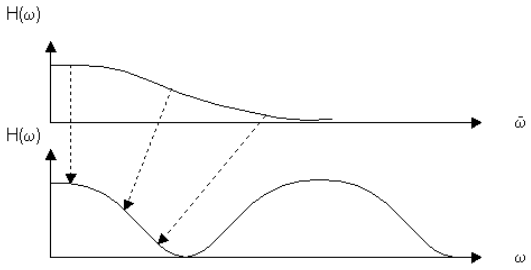
ω – реальная частота (частота ЦФ). Тогда:

$$\frac{\bar{p}T}{2} = \operatorname{th}\frac{pT}{2}$$

Соотношение между реальной и расчетной частотой удобно изобразить на графике.



Рассмотрим графически, как преобразуется частотная характеристика АФ в частотную характеристику ЦФ.



Рассмотрим соотношение частот $\bar{p}$ по отношению к Z-плоскости.

Соотношение между P и Z:

$$e^{pT} = Z$$

Соотношение между $\bar{P}$ и Z-плоскостью:

$$\frac{\bar{p}T}{2} = \text{th}\frac{pT}{2}, \text{ тогда } \bar{P} = \frac{2}{T}\text{th}\frac{PT}{2} = \frac{2}{T}\cdot\frac{e^{\frac{PT}{2}} - e^{-\frac{PT}{2}}}{e^{\frac{PT}{2}} + e^{-\frac{PT}{2}}} = \frac{2}{T}\cdot\frac{1-e^{-PT}}{1+e^{-PT}} =$$

$$= \frac{2}{T}\cdot\frac{1-Z^{-1}}{1+Z^{-1}} = \bar{P}$$

Последовательность расчета по методу билинейного преобразования.

1. Задано: норма на АФ переходит на ЦФ. $\frac{\bar{\omega}T}{2} = tg\frac{\omega T}{2}$
2. Рассчитать АФ в соответсвии в полученными нормами. В результате расчетов становится известной передаточная характеристика H($\bar{p}$).
3. Определить H(Z) по H($\bar{p}$) применяя формулу: $\bar{p} = \frac{2}{T} * \frac{1-z^{-1}}{1+z^{-1}}$
4. По передаточной функции H(Z) построить схему ЦФ.
5. Выполнить нужные расчеты по учету эффекта конечных разрядностей.

Недостаток метода в том, что преобразование частот носит нелинейный характер. Метод применяется, в основном, при проектировании частотно-селективных фильтров.

Список использованных источников:

1. https://studfile.net/preview/7519662/page:27/
2. https://siblec.ru/telekommunikatsii/tsifrovaya-obrabotka-signalov/23-raschet-rekursivnykh filtrov
3. http://ru.dsplib.org/forum/viewtopic.php?t=6706
4. https://dic.academic.ru/dic.nsf/eng_rus/208738/паразитная
5. https://www.ngpedia.ru/id161223p1.html

УДК 628.336.42

СПОСОБ РАСЧЁТА СПЕКТРА МОЩНОСТИ СИГНАЛОВ МЕТОДОМ БЛЭКМАНА

Бабич П.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

В докладе рассказывается про один из способов расчёта спектра мощности сигналов, о преимуществах пользования данным методом Блэкмана, и его актуальность на сегодняшний день.

Этот метод позволяет получать оценку спектральной плотности мощности через преобразование Фурье оценки корреляционной функции. Следует отметить, что метод Блэкмана-Тьюки (коррелограммный метод) был разработан в 1958 г., тогда как алгоритм БПФ для эффективного вычисления ДПФ не был опубликован до 1965 г. Кроме того, этот метод имеет некоторые преимущества по сравнению с методом периодограмм. Например, метод Блэкмана-Тьюки характеризуется большей добротностью. К тому же, корреляционную функцию теперь можно вычислять с помощью ДПФ посредством быстрой корреляции.
Одна из возможных оценок спектральной плотности мощности, получаемая на основе несмещённой оценки корреляционной функции $\hat{K}_x(m),$ которая вычисляется при временном сдвиге с максимальными значениями в интервале $\pm L,$ определяется выражением

$$\hat{P}_{\text{вт}}(f) = \Delta t \sum_{m=-L}^{L} \hat{K}_x(m) \exp(-j2\pi f m \Delta t).$$

Данная оценка определяется для интервала частот $-\frac{1}{2\Delta t} \le f \le \frac{1}{2\Delta t}.$ Максимальное значение временного сдвига *L*, как правило, меньше числа отсчетов *N* выборки исходных данных. Использовать максимальное значение $L \simeq N/10$ было предложено Блэкманом и Тьюки . Выбор такого максимального значения основывался на стремлении исключить большие значения дисперсии , связанные с оценками корреляционной функции при больших временных сдвигах, поскольку такие значения дисперсии давали менее устойчивую оценку СПМ.

Математическое ожидание оценки можно вычислить обычным образом:

$$M[\hat{P}_x(f)] = \Delta t \sum_{m=-L}^{L} M[\hat{K}_x(m)] \exp(-j2\pi f m \Delta t) = \Delta t \sum_{m=-L}^{L} K_x(m) \exp(-j2\pi f m \Delta t) = P_x(f) * W_L(f),$$

где $W_L(f)$ – преобразование Фурье прямоугольного окна (ядро Дирихле).

Несмотря на то, что оценка СПМ вычисляется с использованием несмещенных оценок корреляционной функции, она будет смещенной оценкой истинной спектральной плотности мощности. Неявное присутствие прямоугольного окна при конечной корреляционной последовательности приводит к оценке, которая, по сути, является сверткой истинной спектральной плотности мощности с преобразованием Фурье дискретно-временного прямоугольного окна.

Для уменьшения эффекта просачивания из-за неявного присутствующего прямоугольного окна, а следовательно, и для уменьшения смещения оценки необходимо использовать (2*L* + 1) - точечное корреляционное окно *w*(*n*) нечетной длины на интервале $-L \le m \le L,$ симметричное относительно начала отсчета. Наиболее общая форма корреляционного метода оценивания СПМ в этом случае принимает следующей вид:

$$\hat{P}_{\text{вт}}(f) = \Delta t \sum_{m=-L}^{L} \hat{K}_x(m) w(n) \exp(-j2\pi f m \Delta t)$$

где должна использоваться несмещенная оценка корреляционной функции.

Выражение и определяет оценку, которая была предложена Блэкманом и Тьюки, о чем свидетельствует подсрочный индекс *BT*. Окно здесь нормируется так, чтобы *w*(0) = 1, поэтому оценка $\hat{K}_x(0)$ будет несмещенной, мощность отсчетов сохраняется, а следовательно, оценка $\hat{P}_{\text{вт}}(f)$ будет правильно промасштабирована как оценка СПМ. Если необходимо, чтобы не площадь под кривой оценки Блэкмана и Тьюки была пропорциональна мощности истнной СПМ, а пики этой оценки были пропорциональны мощности импульсов в спектре, то выражение следует промасштабировать величиной $1/N\Delta t$. Не следует применять корреляционные окна, Фурье-образ которых меньше нуля, поскольку это приводит к получению отрицательных значений СПМ, что противоречит ее физическому смыслу. Не все весовые функции удовлетворяют данным критериям. Например, им не удовлетворяют функции Хемминга и Ханна, Кайзера и прямоугольное окно. С увеличением числа значений оценки $\hat{K}_x(m)$ коррелограммный метод дает асимптотически несмещенные оценки СПМ. Блэкман и Тьюки рекомендовали использовать число оцениваемых значений корреляционной последовательности примерно равному 10 % числа имеющихся отсчетов данных.

Дисперсия оценки Блэкмана и Тьюки определяется выражением:

$$D[\hat{P}_{\text{вт}}(f)] \approx \left[\frac{1}{N}\sum_{m=-L}^{L} w^2(m)\right] \cdot P_x^2(f).$$

Очевидно, что при $N/L \to \infty$ $D[\hat{P}_{\text{вт}}(f)] \to 0,$ так что при данных условиях оценка Блэкмана и Тьюки является состоятельной.

Для вычисления оценки СПМ, определяемой выражением, на сетке из (*N* + 1) частот $f_k = k/N\Delta t,$ где используют алгоритмы БПФ. Значение *N* здесь может быть произвольным, но обычно $N \gg L,$ а это значит, что полученная оценка будет сохранять тонкие детали спектра. При использовании значений временного сдвига от *L* + 1 до *N* отсчеты имеющихся данных необходимо дополнить нулями.

Сравнивая процедуру Блэкмана и Тьюки с периодограммным методом, нетрудно заметить, что в этом случае сглаживание достигается не за счет усреднения нескольких периодограмм, а за счет усредняющего эффекта процесса корреляции.

УДК 628.336.42

ВЫЧИСЛИТЕЛЬНО ЭФФЕКТИВНЫЕ КИХ-ФИЛЬТРЫ

Пиляк Г.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Существует два основных типа цифровых фильтров: фильтры с конечной импульсной характеристикой (КИХ) и фильтры с бесконечной импульсной характеристикой (БИХ). Как следует из терминологии, эта классификация относится к импульсным характеристикам фильтров. Изменяя веса коэффициентов и число звеньев КИХ фильтра, можно реализовать практически любую частотную характеристику. КИХ фильтры могут иметь такие свойства, которые невозможно достичь методами аналоговой фильтрации (в частности, совершенную линейную фазовую характеристику). Но высокоэффективные КИХ фильтры строятся с большим числом операций умножения с накоплением и поэтому требуют использования быстрых и эффективных процессоров DSP. С другой стороны, БИХ фильтры имеют тенденцию имитировать принцип действия традиционных аналоговых фильтров с обратной связь. Поэтому их импульсная характеристика имеет бесконечную длительность. Благодаря использованию обратной связи, БИХ фильтры могут быть реализованы с меньшим количеством коэффициентов, чем КИХ фильтры. Другим способом реализации КИХ или БИХ фильтрации являются решетчатые фильтры, которые часто используются в задачах обработки речи. Цифровые фильтры применяются в приложениях адаптивной фильтрации, благодаря своему быстродействию и простоте изменения характеристик воздействием на его коэффициенты.

Типы цифровых фильтров:

1. Фильтр скользящего среднего
2. Фильтр с конечной импульсной характеристикой (КИХ)
   a. Линейная фаза
   b. Легкость проектирования
   c. Значительные вычислительные затраты
3. Фильтр с бесконечной импульсной характеристикой
   a. Основаны на классических аналоговых фильтрах
   b. Высокая вычислительная эффективность
4. Решетчатые фильтры (могут быть КИХ или БИХ)
5. Адаптивные фильтры

Элементарной формой КИХ фильтра является фильтр скользящего среднего (moving average), показанный на рисунке 1.3. Фильтры скользящего среднего популярны для сглаживания данных, например, для анализа стоимости акций и т.д. Входные отсчеты x(n) пропускаются через ряд регистров памяти (помеченных z^{-1} в соответствии с представлением элемента задержки при z-преобразовании). В приведенном примере имеется четыре каскада, соответствующих 4-точечному фильтру скользящего среднего. Каждый отсчет умножается на 0,25, и результаты умножения суммируются для получения значения скользящего среднего, которое подается на выход y(n). На рисунке также представлено общее уравнение фильтра скользящего среднего на N точек. N относится к числу точек при вычислении фильтра, а не к разрешающей способности АЦП или ЦАП.

С учетом равенства коэффициентов, наиболее простой путь исполнения фильтра скользящего среднего представлен на рисунке 1.4. Обратите внимание, что первым шагом является запоминание первых четырех отсчетов x(0), x(1), x(2), x(3) в регистрах. Эти величины суммируются и затем умножаются на 0,25 для получения первого выхода y(3). Обратите внимание, что начальные значения выходов y(0), y(1) и y(2) некорректны, потому что, пока отсчет x(3) не получен, не все регистры заполнены.

Когда получен отсчет x(4), он суммируется с результатом, а отсчет x(0) вычитается из результата. Затем новый результат должен быть умножен на 0,25. Поэтому вычисления, требуемые для

получения нового значения на выходе, состоят из одного суммирования, одного вычитания и одного умножения, независимо от длины фильтра скользящего среднего.

Реакция 4-точечного фильтра скользящего среднего на ступенчатое воздействие представлена на рисунке 1.5. Скользящего среднего не имеет выброса по фронту входного сигнала. Это делает его полезным в приложениях обработки сигналов, где требуется фильтрация случайного белого шума при сохранении характера входного импульса. Из всех возможных линейных фильтров, фильтр скользящего среднего дает самый низкий уровень шума при заданной крутизне фронта импульса. Это показано на рисунке 1.6, где уровень шума понижается по мере увеличения числа точек. Существенно, что время реакции фильтра на ступенчатое воздействие от 0 % до 100 % равно произведению общего количества точек фильтра на период дискретизации.

Частотная характеристика простого фильтра скользящего среднего выражается функцией sin(x)/x. Она представлена в линейном масштабе на рисунке 1.6. Увеличение числа точек при реализации фильтра сужает основной лепесток, но существенно не уменьшает амплитуду боковых лепестков частотной характеристики, которая равна приблизительно -14 дБ для фильтра с 11 и с 31 отводами (длиной буфера). Естественно, эти фильтры не подходят в том случае, где требуется большое ослабление в полосе задержания.

Можно существенно улучшить эффективность простого КИХ фильтра скользящего среднего, выбирая разные веса или значения коэффициентов вместо равных значений. Крутизна спада может быть увеличена добавлением большего количества звеньев в фильтр, а характеристики полосы затухания улучшаются выбором надлежащих коэффициентов фильтра. Обратите внимание, что, в отличие от фильтра скользящего среднего, для реализации каждой ступени обобщенного КИХ фильтра требуется цикл умножения с накоплением. Сущность проектирования КИХ фильтра сводится к выбору соответствующих коэффициентов и необходимого числа звеньев при формировании желаемой частотной характеристики фильтра H(f). Для включения необходимой частотной характеристики H(f) в набор КИХ коэффициентов имеются различные алгоритмы и программные пакеты. Большинство этого программного обеспечения разработано для персональных компьютеров и доступно на рынке. Ключевой теоремой проектирования КИХ фильтра является утверждение, что коэффициенты h(n) КИХ фильтра являются просто квантованными значениями импульсной характеристики этого фильтра. Соответственно, импульсная характеристика является дискретным преобразованием Фурье от H(f).

Обобщенная форма КИХ фильтра с числом звеньев N представлена на рисунке 1.7. Как было сказано, КИХ фильтр должен работать в соответствии с уравнением, задающим свертку:

$$\mathrm{Y\ (n) = h\ (k)\ *x\ (n) = \sum_{k=0}^{N-1} h(k)x(n-k)\ ,}$$

где h(k) – массив коэффициентов фильтра и x(n-k) – входной массив данных фильтра. Число N в уравнении представляет собой число звеньев и определяет эффективность фильтра, как было сказано выше. КИХ фильтр с числом звеньев N требует N циклов (операций) умножения с накоплением.

Согласно рисунке 1.8, диаграммы КИХ-фильтров часто изображаются в упрощенном виде. Операции суммирования представляются стрелками, указывающими в точки, а операции умножения обозначают, помещая коэффициенты h(k) рядом со стрелками на линиях. Элемент задержки z^{-1} показывают, помещая его обозначение выше или рядом с соответствующей линией.

УДК 628.336.42

МОДИФИЦИРОВАННЫЕ ОДНОРОДНЫЕ ФИЛЬТРЫ

Кухта Н.В.[1], студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Модифицированные однородные фильтры отличаются от обычных более чёткой частотной локализацией и поэтому могут более эффективно использоваться в подавлении шума. Во-первых, модифицированные однородные фильтры позволяют достичь большего подавления в зоне непрозрачности, чем обычные однородные фильтры. Во-вторых, их импульсная характеристика на краях плавно сходится к нулю. Это означает, что отсчёты, близкие к центру такой группы, оказывают более сильное влияние на формирование выходного отсчёта. В-третьих, переходные процессы модифицированных фильтров оказываются более плавными и не имеют резких изгибов.

Ключевые слова. Модифицированный фильтр, однородный фильтр, передача сигнала, цифровой фильтр, реализация

Наиболее просто в цифровом виде однородный фильтр, так как для его реализации не требуются умножители. Для однородного фильтра четвертого порядка эта формула выглядит следующим образом:

$$y(n) = x(n) + x(n-1) + x(n-2) + x(n-3) + x(n-4) + x(n-5) + x(n-6) \quad (1)$$

Структурная схема фильтра, реализующего формулу (1), приведена на рисунке 1.

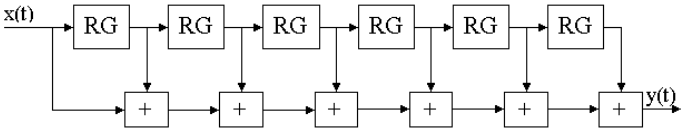


Рисунок 1. Структурная схема однородного фильтра седьмого порядка

При реализации такого фильтра потребуется 6 сумматоров. Во столько же раз уменьшится быстродействии цифрового фильтра. Можно несколько видоизменить структуру данного фильтра. Для сокращения количества выполняемых операций формула 1 может быть переписана в следующем виде:

$$y(n) = x(n) + y(n-1) - x(n-6) \quad (2)$$

Эта формула может быть реализована за два действия:

$$y(n) = x(n) + y(n-1) \quad (3)$$
$$y(n) = x(n) - x(n-6)$$

В таком случае для реализации фильтра потребуется два каскада. Первый каскад будет выполнять интегрирование, а второй — фильтр с конечной импульсной характеристикой всего с двумя ненулевыми коэффициентами, равными единице. Структурная схема нового фильтра приведена на рисунке 2.

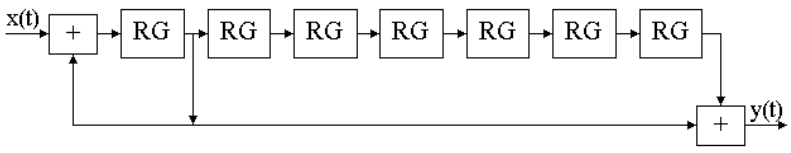


Рисунок 2. Структурная схема двухкаскадного фильтра, эквивалентного фильтру, приведенному на рисунке 1

В этой схеме максимальное время задержки сигнала определяется быстродействием сумматора и временем записи в регистр. Мы увеличили быстродействие почти в семь раз.

Список использованных источников:

1. Микушин А.В., Сажнев А.М., Сединин В.И. Цифровые устройства и микропроцессоры. СПб, БХВ-Петербург, 2010. URL: https://digteh.ru/digteh/sinc.php?

UDC 628.336.42

MODIFIED UNIFORM FILTERS

Kukhta N.V.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Daneyko T.M. – senior lector of department of ICT

Annotation. Modified homogeneous filters differ from conventional ones in a clearer frequency localization and therefore can be more effectively used in noise suppression. First, modified uniform filters achieve greater suppression in the opacity zone than conventional uniform filters. Secondly, their impulse response smoothly converges to zero at the edges. This means that samples close to the center of such a group have a stronger influence on the formation of the output sample. Thirdly, the transient processes of the modified filters turn out to be smoother and do not have sharp bends.

Keywords. Modified filter, uniform filter, signal transmission, digital filter, implementation.

УДК 628.336.42

АНАЛИЗ ВЛИЯНИЯ КОНЕЧНОЙ РАЗРЯДНОСТИ ЧИСЕЛ НА ПАРАМЕТРЫ ФИЛЬТРА

Рымчёнок В.О., курсант гр.933701

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – магистр технических наук

Аннотация. Этапы аппроксимации и реализации предполагают работу с бесконечной или очень высокой точностью. Влияние конечного числа битов проявляется в снижении производительности фильтра, и фильтр может стать неустойчивым. Для анализа влияния разрядности чисел на параметры фильтра перечислим основные источники ухудшения его производительности.

Ключевые слова. Квантование, ошибки, размерность, аппроксимация, фильтр

Этапы аппроксимации и реализации предполагают работу с бесконечной или очень высокой точностью. В то же время, в настоящих реализациях часто требуется представить коэффициенты фильтра конечным числом битов (обычно от 8 до 16 бит), кроме того, арифметические операции, указанные в разностных уравнениях, выполняются с использованием арифметики конечной точности.

Влияние конечного числа битов проявляется в снижении производительности фильтра, и в некоторых случаях фильтр может стать неустойчивым. Разработчик должен проанализировать данные эффекты и выбрать подходящую длину слова (т.е. число битов) для представления коэффициентов фильтра, переменных фильтра (т.е. входных и выходных выборок) и выполнения арифметических операций в фильтре.

Перечислим основные источники ухудшения производительности фильтра.

- Квантование сигнала на входе-выходе. В частности, шум АЦП вследствие квантования входных выборок сигнала — это существенная величина

- Квантование коэффициентов. Данный фактор приводит к искажению частотных характеристик КИХ- и БИХ-фильтров и возможной неустойчивости БИХ-фильтров.

- Ошибки округления. Использование для фильтрации арифметики конечной точности дает результаты, представление которых требует дополнительных битов. Если результаты квантуются до допустимой длины слова (часто для этого используется округление), возникает шум округления. В результате возможны такие нежелательные следствия, как неустойчивость БИХ-фильтров.

- Переполнение. Этот эффект проявляется, когда результат сложения превышает разрешенную длину слова. Это приводит к неверным выходным выборкам и возможной неустойчивости БИХ-фильтров.

Степень ухудшения фильтра зависит от

1) Длины слова и типа арифметики, исполь¬зуемой для фильтрации,
2) Метода квантования коэффициентов фильтра и переменных до выбранных размеров,
3) Структуры фильтра.

Зная эти факторы, разработчик может оценить влияние конечной разрядности на производительность фильтра и при необходимости принять меры.

Список использованных источников:

1. https://studopedia.info/2-82333.html
2. https://cyberleninka.ru/article/n/effekty-konechnoy-razryadnosti-dvoichnyh-chisel-pri-realizatsii-tsifrovyh-filtrov
3. https://scienceforum.ru/2017/article/2017035730
4. https://scask.ru/c_book_r_cos.php?id=90
5. https://studref.com/667485/tehnika/effekty_konechnoy_razryadnosti_tsifrovyh_filtrah

UDC 628.336.42

ANALYSIS OF THE EFFECT OF FINITE-BIT NUMBERS ON FILTER PARAMETERS

Rymchenok V.O.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Daneiko. T.M. – Master of Technical Sciences

Annotation. The stages of approximation and implementation involve working with infinite or very high accuracy. The effect of a finite number of bits is manifested in a decrease in filter performance, and the filter may become unstable. To analyze the effect of the number of digits on the filter parameters, we list the main sources of deterioration in its performance.

Keywords. Quantization, errors, dimensionality, approximation, filter

УДК 628.336.42

МЕТОД БИЛИНЕЙНОГО Z-ПРЕОБРАЗОВАНИЯ

Готин Н.А.[1], студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Исследована сущность билинейного z-преобразования. Установлена его схожесть с отображением z=exp(s*T). Определено, что билинейное преобразование позволяет осуществить переход из s плоскости в z-плоскость при помощи дробно-рациональной подстановки, что упрощает переход от аналогового фильтра к цифровому.

Ключевые слова. Цифровой фильтр, передаточная характеристика, ряд Тейлора, плоскость z.

Билинейное преобразование осуществляется подстановкой вида:

$$s = \frac{2}{T} * \frac{1-z^{-1}}{1+z^{-1}} \quad (1)$$

Также данную подстановку можно инвертировать:

$$z^{-1} = \frac{2-s*T}{2+s*T} \text{ или } z = \frac{2+s*T}{2-s*T} \quad (2)$$

При билинейном преобразовании мнимая ось плоскости s переходит в единичную окружность на плоскости z, причем левая полуплоскость плоскости s отображается внутрь единичной окружности плоскости z, а правая полуплоскость плоскости s отображается вне единичной окружности. Отображение плоскости s в плоскость z при билинейном преобразовании показано на рисунке 1.

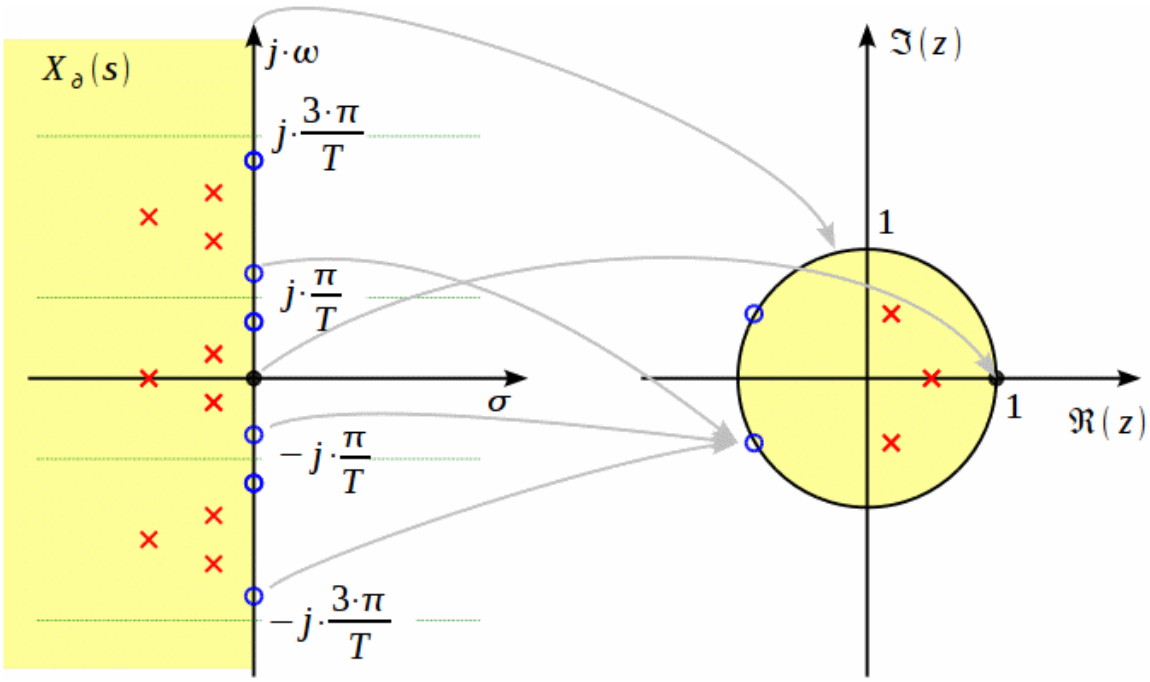


Рисунок 1 – Отображение плоскости s в плоскость z

Данное отображение очень похоже на отображение z=exp(s*T). Такая схожесть обуславливается тем, что выражение (2) представляет собой разложение в ряд Тейлора z=exp(s*T) при

ограничении степени ряда равной единицы. Действительно, разложение в ряд Тейлора экспоненты равно:

$$\exp(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad (3)$$

Тогда можно представить:

$$exp(x) = \frac{\exp(s*T/2)}{\exp(-s*T/2)} \approx \frac{1+s*T/2}{1-s*T/2} = \frac{2+s*T}{2-s*T} \quad (4)$$

Таким образом, билинейное преобразование позволяет осуществить переход из s плоскости в z-плоскость при помощи дробно-рациональной подстановки. Поскольку в числителе и знаменателе этой подстановки полиномы только первой степени, то при переходе от передаточной характеристики аналогового фильтра H(s) к цифровому фильтру с передаточной характеристикой H(z), максимальная степень полиномов числителя и знаменателя не изменится, а значит не измениться и порядок фильтра.

Список использованных источников:

1. Бахурин С. Расчет передаточной характеристики БИХ фильтра на основе аналогового фильтра прототипа. Билинейное преобразование. URL: http://www.dsplib.ru/content/filters/bilinear/bilinear.html

UDC 628.336.42

BILIARY Z-TRANSFORMATION METHOD

Gotin N.A.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Daneiko T.M. – Senior Lecturer of department of ICT

Annotation. The essence of the bilinear z-transform is investigated. Its similarity with the form z=exp(s*T) has been established. It is determined that the bilinear transformation allows the transition from the original filter to the digital one.

Keywords. Digital filter, transfer characteristic, Taylor series, z-plane.

УДК 628.336.42

МЕТОД СОГЛАСОВАННОГО Z-ПРЕОБРАЗОВАНИЯ

Гец П.А.[1], студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Метод согласованного z-преобразования, амплитудная характеристика цифрового фильтра

Ключевые слова. Цифровой фильтр, передаточная характеристика, дискретизация, эффект наложения, плоскость z.

Метод согласованного z-преобразования довольно прост в использовании, однако во многих случаях он неприменим. Так, если центральные частоты аналогового фильтра, соответствующие его нулям, превышают половину частоты дискретизации, то положение нулей цифрового фильтра будет существенно искажено эффектом наложения. Покажем это на примере передаточной функции

$$H(s) = \frac{s^2 + 2s + 5626}{s^2 + 2s + 2}$$

с нулями в точках $s = -1 \pm j75$ и полюсами в точках $s = -1 \pm j1$. Пусть T=1/2. Используя согласованное z -преобразование, получим следующее выражение для передаточной функции цифрового фильтра:

$$H(s) = \frac{1 - 2e^{-1/12}\cos(\frac{75}{12})z^{-1} + e^{-1/6}z^{-2}}{1 - 2e^{-1/12}\cos(\frac{1}{12})z^{-1} + e^{-1/6}z^{-2}}$$

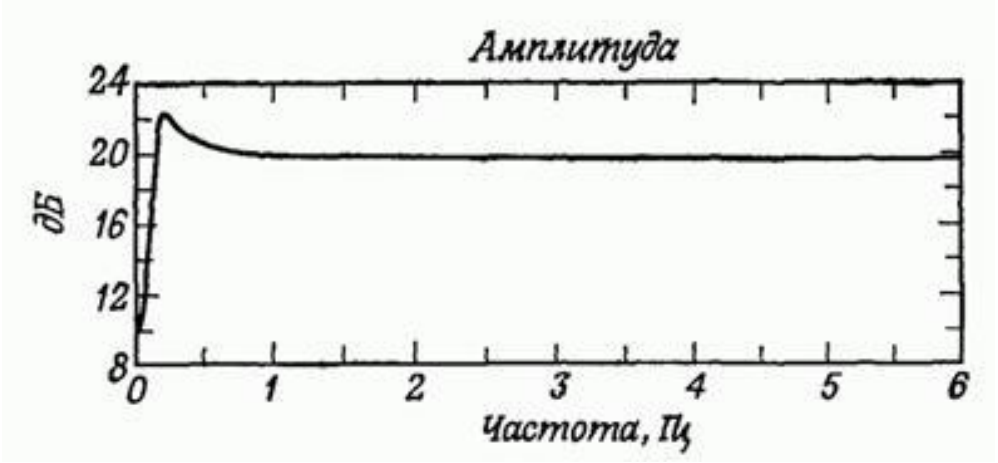


Рисунок 1 – Амплитудная характеристика цифрового фильтра, рассчитанного методом согласованного z-преобразования полюсов и нулей аналогового фильтра

Полюсы этой функции расположены в точках с полярными координатами $z = e^{-1/12}e^{\pm j(\frac{1}{12})}$ нули — в точках с координатами $z = e^{-1/12}e^{\pm 75/12}$. Видно, что при использовании согласованного z -преобразования из-за эффекта наложения нули аналогового фильтра из области верхних смещаются в область нижних частот для цифрового фильтра.

Список использованных источников:

1. Марпл, С. Л. Цифровой спектральный анализ и его применения: Пер. с англ. / С. Л. Марпл. – М.: Мир, 1990. – 584 с

2. Шахтарин, Б. И. Методы спектрального оценивания случайных процессов / Б. И. Шахтарин, В. А. Ковригин. – М.: Гелиос АРВ, 2005. – 248 с

UDC 628.336.42

CONSISTENT Z-TRANSFORMATION METHOD

Hets P.A.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Daneyko T.M. – senior lector of department of ICT

Annotation. Z–transform matching method. Estimated characteristic of the observer filter

Keywords. Digital filter, transfer characteristic, sampling, aliasing, z-plane.

УДК 628.336.42

ПАРАЗИТНАЯ АМПЛИТУДНАЯ МОДУЛЯЦИЯ СПЕКТРА ПРИ ДПФ И СПОСОБЫ ЕЕ МИНИМИЗАЦИИ

Пинголь А.И., студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – магистр технических наук

Аннотация. Данная работа рассматривает вопрос паразитной модуляции при ДПФ. Называет особенности по которым можно определить её наличие, а также наиболее действенный метод её решения..

Ключевые слова. Фурье, дискретное преобразование, полосовал фильтры, паразитная модуляция, гармоника, круговая частота дискретизации, гребешковое искажение, комплексная интерполяция.

Дискретное преобразование Фурье это ничто иное, как обработка сигналов набором полосовых фильтров, центральные частоты которых в точности соответствуют дискретным отсчетам X(k), где k – целое число из интервала [0; N –1]

При идеальных обстоятельствах каждому коэффициенту ДПФ соответствует фильтр с прямоугольной частотной характеристикой, но есть одно но, из-за умножения входной последовательности на взвешивающую (оконную) функцию, фактическая частотная характеристика образует вид функции sinc(x), имеющей боковые и основной лепестки. Это мы можем наблюдать на рисунке 1.

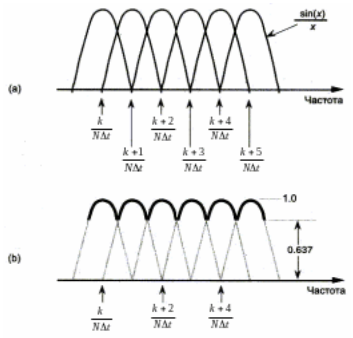


Рисунок 1 – Амплитудно-частотная характеристика ДПФ: (а) отдельные кривые вида sin(x)/хдля каждого коэффициента ДПФ; (б) общая амплитудно-частотная характеристика

Главные лепестки формируют собой N независимых фильтров. Значит, что входной сигнал $ej_{\omega\Delta}t$ с частотой кратной 1/T, будет проходить через фильтр, настроенный соответственно на частоту сигнала, без каких-либо изменений и будет полностью подавлен остальными фильтрами.

Эффект паразитной модуляции спектра отображается, когда частота анализируемого сигнала не совпадает ни с одной из наших дискретных ортогональных частот. Вот такой пример приведу, у нас есть некий сигнал, частота которого находится между первым и вторым гармониками, проходя через первый, так и второй фильтр, но важным моментом является то, что его уровень на выходе двух фильтров будет меньше единицы. В наихудших случаях, при попадании в середину между гармониками, падает довольно значительно, а при возведении этого значения в квадрат уменьшается ещё более значительно. Всё это представляет собой паразитную модуляцию. Это явление схоже с анализом истинного спектра через частокол («гребешковое искажение») (1)

$$\text{ГИ} = \frac{W(\omega_s / 2N)}{W(0)} = \frac{\left| \sum_{n=0}^{N-1} w(n\Delta t) \cdot \exp(-j\pi n / N) \right|}{\sum_{n=0}^{N-1} w(n\Delta t)},$$

где W – ДПФ весовой функции, $\omega_s = 2\pi f_s$ – круговая частота дискретизации, N – число элементов выборки n – номер элемента выборки, $w(n\Delta t)$ – весовая функция, дискретизированная во временной области.

Уменьшить гребешковое искажение можно при помощи комплексной интерполяции коэффициентов ДПФ или путем введения в реальные данные дополнительных нулей.

Если дополнить исходную выборку нулями, то в результате получается избыточный алгоритм ДПФ, который даст дополнительные отстчеты спектра на частотах, лежащих между частотами первоначальных гармоник. При этом частотные характеристики фильтров, ассоциируемых с новым набором коэффициентов ДПФ, перекрывают друг друга в большей степени.

Дополнительные коэффициенты ДПФ, возникающие в результате данной операции, размещаются в промежутках первоначального набора коэффициентов Фурье. При этом паразитная амплитудная модуляция спектра уменьшается с 60 % до 20 %. Она может быть меньше или больше 20 % в зависимости от того, большее или меньшее число дополнительных отсчетов используется при расчете ДПФ.

Следует отметить, что на практике гребешковое искажение не столь вносит коррективы или существенно мешает, так как во многих случаях обрабатываемый сигнал не является сугубо гармоническим или полигармоническим, а достаточно широкополосен для заполнения нескольких фильтров.

Список использованных источников:

1. https://forkalor.livejournal.com/80764.html?
2. http://rateli.ru/books/item/f00/s00/z0000017/st020.shtml
3. http://ru.dsplib.org/forum/viewtopic.php?t=6706
4. https://dic.academic.ru/dic.nsf/eng_rus/208738/паразитная
5. https://www.ngpedia.ru/id161223p1.html

UDC 628.336.42

TI PARASITIC AMPLITUDE MODULATION OF THE SPECTRUM IN THE DFT AND WAYS TO MINIMIZE IT

Pingol A.I.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Daneyko T.M.– master of technical sciences

Annotation. This paper considers the issue of parasitic modulation in the DFT. Names the features by which its presence can be determined, as well as the most effective method for solving it.

Keywords. Fourier, discrete transform, bandpass filters, spurious modulation, harmonics, circular sampling rate, comb distortion, complex interpolation.

УДК 628.336.42

МЕТОД ИНВАРИАНТНОГО ПРЕОБРАЗОВАНИЯ ИМПУЛЬСНОЙ ХАРАКТЕРИСТИКИ

Прохоренко А.В.[1], студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Рассмотрен метод инвариантного преобразования импульсной характеристики. Продемонстрирован метод дискретизации аналогового фильтра с использованием инвариантного преобразования импульсной характеристики.

Ключевые слова. Импульсная характеристика, z-преобразование, Аналоговый фильтр.

Импульсная характеристика аналогового фильтра с передаточной функцией вида описывается соотношением:

$$h(t) = \sum_{i=1}^{N} c_i e^{-d_i t} u_{-1}(t) \quad (1)$$

На рисунке 1 показано соответствующее инвариантному преобразованию импульсной характеристики отображение из s-плоскости в z-плоскость. Каждая горизонтальная полоса шириной $2\pi / T$ из s-плоскости отображается па z-плоскость. Поэтому все смежные полосы из s-плоскости будут при отображении накладываться друг па друга в z-плоскости. Отсюда следует, что для того, чтобы частотные характеристики исходного аналогового фильтра и рассчитываемого методом инвариантного преобразования импульсной характеристики цифрового фильтра соответствовали друг другу, необходимо, чтобы полоса пропускания аналогового фильтра находилась в пределах диапазона $-\pi / T \le \Omega \le \pi / T$.

Для выполнения этого условия необходимо до начала преобразования вводить дополнительный фильтр нижних частот, гарантирующий соответствующее ограничение полосы пропускания аналогового фильтра.

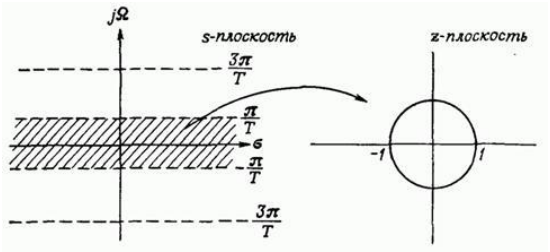


Рисунок 1 – Отображение плоскости s в плоскость z

Список использованных источников:

1. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. М: Мир, 1978. URL: https://scask.ru/c_book_r_cos.php?id=78

UDC 628.336.42

METHOD OF INVARIANT TRANSFORMATION OF THE IMPULSE RESPONSE

Prohorenko A.V.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Daneiko T.M. – senior lector of department of ICT

Annotation. The method of invariant transformation of the impulse response is considered. A method for sampling an analog filter using an invariant transformation of the impulse response is demonstrated.

Keywords. Impulse response, z-transform, Analog filter.

УДК 628.336.42

АНАЛИЗ ЭФФЕКТИВНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Скороходов Р.В., студент гр.067001/магистрант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Тарченко Н.В. – канд. технических наук

Аннотация. Тематика работы обусловлена повсеместным использованием волоконно-оптических систем передачи, в том числе и со спектральным уплотнением. При постоянном увеличении пропускной способности волоконно-оптических систем передачи (ВОСП) совершенствуются способы обработки оптического сигнала как в передающем и приемном оборудовании, так и в процессе передачи по оптическому волокну. Совершенствование оптических технологий расширяет возможности алгоритмов обработки сигналов на приемной стороне и требует оценки их эффективности.

Ключевые слова. Спектральная эффективность, энергетическая эффективность, методы модуляций.

1 Введение

Многоуровневые форматы модуляции сочетают в себе высокую спектральную эффективность и устойчивость к воздействию дисперсии в оптическом волоке [1, 2]. Эти достоинства многоуровневых форматов модуляции делают их перспективными при необходимости увеличения скорости передачи в действующих системах связи со спектральным уплотнением. Сочетание когерентного детектирования с цифровой обработкой сигналов позволяет достигнуть более высоких значений количества передаваемой информации на один символ [3]. Когерентные оптические системы связи были предложены в 1970-е гг. [4] и в 1980-е начали интенсивно исследоваться, поскольку обеспечивают достижение квантового предела чувствительности приемников [5, 6]. Однако с появлением систем связи со спектральным уплотнением и оптическими усилителями научно-исследовательские работы в этом направлении были прерваны примерно на 20 лет.

Развитие оптических технологий привело к возрождению интереса к когерентным системам. Он обусловлен возможностями реализации в этих системах множества разнообразных многоуровневых форматов модуляции. Кроме того, цифровая обработка сигналов в электронной форме позволяет компенсировать искажения, связанные, например, с хроматической и поляризационно-модовой дисперсией. Существенным недостатком первых когерентных систем связи была их высокая поляризационная чувствительность. Однако проблема была решена благодаря изобретению поляризационной диверсификации (*polarization diversity*) [7]. Более того, современные цифровые когерентные приемники позволяют удвоить скорость передачи информации за счет поляризационного уплотнения информации.

В настоящей работе проведена оценка эффективности когерентных систем связи с многоуровневой модуляцией.

2 Критерии эффективности инфокоммуникационных систем

Основными критериями эффективности инфокоммуникационных систем являются критерии спектральной и энергетической эффективности. Энергетическая эффективность характеризует энергию, которую необходимо затратить для передачи информации с заданной достоверностью (вероятностью ошибки).

Спектральная эффективность характеризует полосу частот, необходимую для того, чтобы передавать информацию с определенной скоростью. Кроме данных критериев, виды модуляции сравниваются по устойчивости к различным типам помех и искажений и сложности аппаратной реализации. Существуют также специфические критерии, существенные для отдельных систем связи, отражающие особенности канала связи [8].

Спектральная (частотная) эффективность цифровой системы определяется, как

$$\gamma = \frac{R_b}{B_w}, \quad (1)$$

где R_b – скорость передачи информации, бит/с;

B_W – полная полоса частот канала, Гц.

Измеряется спектральная эффективность числом битов в секунду, приходящихся на 1 Гц полосы канала, т.е. бит/(с·Гц).

В реальных условиях доступная полоса частот канала B_W по тем или иным причинам может использоваться не полностью, поэтому даже достаточно эффективная система передачи в ее конкретном применении по данному критерию оценки будет выглядеть неэффективной. Кроме того, необходимо уточнить критерий спектральной эффективности, связав его с полосой Найквиста B_N и коэффициентом скругления спектра α, значение которого характеризует расширение практически занимаемой спектром сигнала полосы частот канала B_L сверх полосы Найквиста B_N:

$$B_L = B_N(1 + \alpha). \quad (2)$$

Соответственно реальная спектральная эффективность η различных схем модуляции, предназначенных для цифровой передачи, выражается формулой:

$$\eta = \frac{R_b}{B_L} = \frac{R_b}{B_N(1+\alpha)}. \quad (3)$$

В идеальном случае при полном использовании всей полосы частот канала, когда $B_W = B_L$, показатели эффективности η и γ совпадают, т.е. $\gamma = \eta$.

Целесообразно ввести также критерий потенциальной спектральной эффективности конкретного метода модуляции, который соответствует коэффициенту η или γ при $B_W = B_L$ и $\alpha = 0$.

Определим потенциальную эффективность как:

$$\gamma_0 = \frac{R_b}{B_N}. \quad (4)$$

Отсюда следует, что

$$\eta = \frac{\gamma_0}{(1+\alpha)} \text{ или } \gamma_0 = \eta(1 + \alpha). \quad (5)$$

При использовании многопозиционной цифровой модуляции

$$R_b = \log_2(M)R_S, \quad (6)$$

где M – число элементов пространства сигналов при цифровой модуляции;

R_s – скорость передачи символов цифрового потока.

Согласно критерию Найквиста максимальная скорость передачи символов в полосовой системе численно равна

$$R_S = \frac{B_W}{(1+\alpha)}. \quad (7)$$

Следовательно, при $B_W = B_L$

$$\eta = \frac{\log_2(M)}{(1+\alpha)}. \quad (8)$$

Отсюда следует, что для повышения спектральной эффективности h необходимо увеличивать кратность модуляции $\log_2 M$ и одновременно снижать значение коэффициента скругления спектра α, тем самым увеличивая крутизну среза спектра модулирующего сигнала [8].

Способ модуляции играет основную роль в достижении максимально возможной скорости передачи информации при заданной вероятности ошибочного приема. Пропускная способность

канала связи с аддитивным белым гауссовым шумом (АБГШ) является функцией средней мощности принятого сигнала, средней мощности шума и ширины полосы пропускания. Предельные возможности системы передачи можно оценить с помощью теоремы Шеннона - Хартли, определяющей верхнюю границу пропускной способности канала связи:

$$C = W \log_2 \left(1 + \frac{S}{N}\right), \tag{9}$$

где C – пропускная способность канала связи, бит/сек;

W – ширина полосы пропускания системы, Гц;

S – средняя мощность принятого сигнала, Вт;

N – средняя мощность шума, Вт.

Теоретически информация по каналу связи может быть передана со сколь угодно малой ошибкой при любой скорости передачи данных R, удовлетворяющей условию $R \leq C$, что достигается при помощи использования сложных методов кодирования. В случае, если $R > C$, передача данных со сколь угодно малой вероятностью ошибки невозможна.

При сравнении различных видов модуляции обычно оперируют не соотношением сигнал/шум, а отношением энергии бита к плотности мощности шума, которое определяется следующим образом:

$$\frac{E_b}{N_0} = \frac{S}{N}\left(\frac{W}{R}\right), \tag{10}$$

где E_b – энергия бита, Вт/бит/сек;

N_0 – плотность мощности шума, Вт/Гц.

Таким образом, выражение верхней границы пропускной способности канала связи может быть модифицировано:

$$\frac{E_b}{N_0} = \frac{W}{R}\left(2^{C/W} - 1\right). \tag{11}$$

На рисунке 1. показан график зависимости отношения нормированной полосы пропускания сигнала W/C от отношения энергии бита к плотности мощности шума E_B/N_0. Как видно из рисунка, существует нижнее предельное значение E_B/N_0, при котором ни при какой скорости передачи нельзя осуществить безошибочную передачу информации. Это значение E_B/N_0 называется пределом Шеннона:

$$\frac{E_b}{N_0} = \ln(2) = -1{,}59 \text{ дБ}. \tag{12}$$

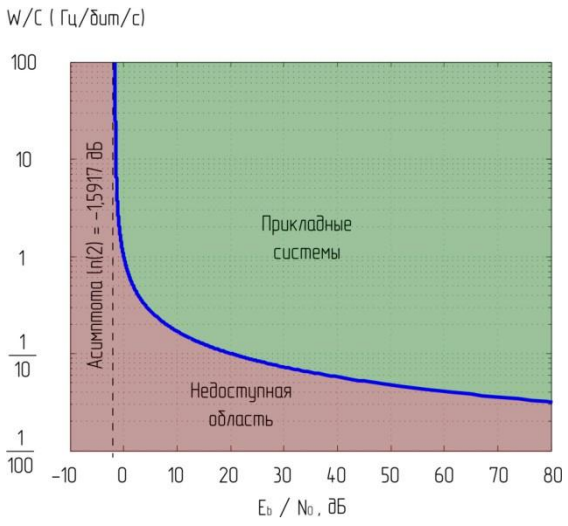


Рисунок 1 – Зависимость нормированной полосы пропускания канала от отношения энергии бита к плотности мощности шума

Шеннон теоретически доказал существование кодов, которые могут понизить вероятность битовой ошибки или снизить требуемое значение E_B/N_0 от уровней не кодированных двоичных систем модуляции до уровней, приближающихся к предельной кривой. Одной из основных задач разработчика современных систем цифровой связи является повышение спектральной эффективности модуляции, т. е. уменьшение отношения W/R до теоретического предела, что возможно при использовании современных методов канального кодирования [8].

Показатель энергетической эффективности оценивается формулой

$$\beta = \frac{R_b N_0}{P_c}, \tag{13}$$

где P_C – средняя мощность модулированного сигнала;

$N_0 = kT$ – односторонняя спектральная плотность мощности аддитивного белого гауссовского шума (АБГШ) на входе приемного фильтра.

С учетом того, что

$$P_C = E_b R_b, \tag{14}$$

где E_b – энергия сигнала на бит информации на входе приемного фильтра, получаем

$$\beta = \frac{N_0}{R_b}. \tag{15}$$

Таким образом, коэффициент *b* – величина обратная отношению энергии на бит в передаваемом сигнале к плотности шума на входе приемника [9].

При использовании в модеме согласованной фильтрации и формировании спектров, согласно критериям Найквиста, энергетическая эффективность *b* может быть выражена следующим образом:

$$\beta = \frac{N_0 R_b B_N}{P_C B_N} = \frac{P_m R_b}{P_C B_N} = \frac{\gamma_0}{q} = \frac{h(1+\alpha)}{q}. \tag{16}$$

Так как при согласованной найквистовской фильтрации шумовая полоса приемника совпадает с полосой Найквиста, то мощность шума на входе решающего устройства равна $P_m = N_0 B_N$, при этом отношение сигнал/шум $q = P_c/P_m$, $\gamma_0 = R_B/B_N$.

Коэффициенты *η* и *β* взаимосвязаны. Подставляя в формулу (16) для *β* отношение $R_b/B_N = \gamma_0 = \eta(1+\alpha)$, получаем:

$$\beta = \frac{\eta(1+\alpha)}{q}, \tag{17}$$

$$q = \frac{\eta(1+\alpha)}{\beta}. \tag{18}$$

Как известно, пропускная способность (максимально возможная скорость передачи информации) частотно-ограниченного канала с аддитивным белым гауссовским шумом определяется формулой Шеннона:

$$C = \Delta F \log_2\left(1 + \frac{P_C}{N_0 \Delta F}\right). \tag{19}$$

Здесь под полосой пропускания системы *ΔF* следует понимать шумовую полосу, равную полосе Найквиста B_N. В пределе, при выполнении условий теоремы, $R_b = C$, и тогда можно получить соотношение для верхней границы эффективности передачи информации:

$$\frac{R_b}{B_N} = \log_2(1+q) = \log_w\left(1 + \frac{\eta(1+\alpha)}{\beta}\right), \tag{20}$$

$$\eta(1+\alpha) = \log_2\left(1+\frac{\eta(1+\alpha)}{\beta}\right). \quad (21)$$

Найдем отсюда формулу для энергетической эффективности β как функции реальной спектральной эффективности η и коэффициента скругления спектра α:

$$\beta = \frac{\eta(1+\alpha)}{2^{\eta(1+\alpha)}-1}. \quad (22)$$

Для сравнения видов модуляций по критерию энергетической эффективности необходимо оценить для каждого вида модуляции требуемую энергию для передачи информации с одинаковой вероятностью ошибки на бит. В [4], определены соотношения, связывающие вероятность битовой ошибки с величиной E_b/N_0 для различных видов модуляции:

$$BER = f\left(\frac{E_b}{N_0}\right), \quad (23)$$

где *BER* – вероятность ошибки;

E_b – энергия, необходимая для передачи одного бита информации;

N_0 – спектральная плотность мощности белого шума в канале.

Если мощность передатчика равна P, то величина энергии, приходящаяся на один бит информации, равна:

$$E_b = PT_b, \quad (24)$$

где T_b – длительность бита.

3 Сравнительный анализ эффективности методов модуляции

Сравнение и выбор метода модуляции производят по показателям спектральной и энергетической эффективности, в качестве которых будем использовать удельную скорость передачи (бит/с/Гц) и отношение сигнал/шум:

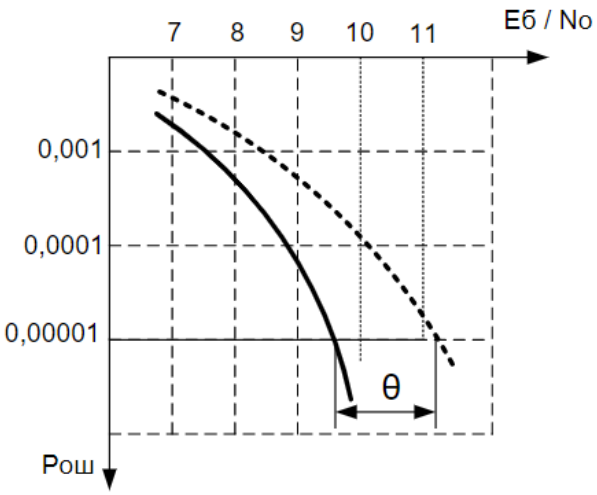
$$h^2 = {E_b}/{N_0} \quad (25)$$

Сравнение методов модуляции удобно производить по диаграмме спектрально-энергетической эффективности (рисунок 3). На этой диаграмме построена предельная кривая, определяемая выражением [9]:

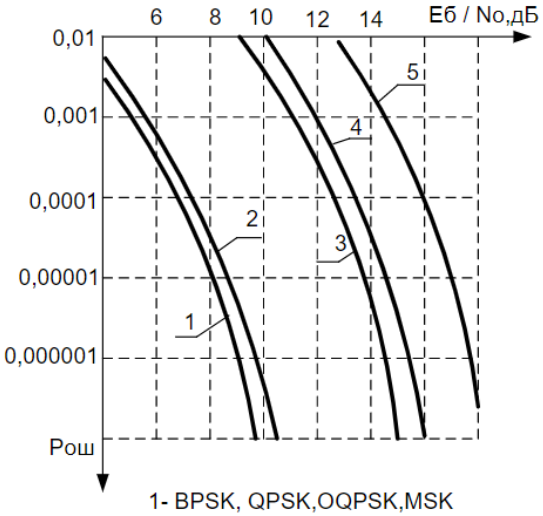
$${E_b}/{N_0} = \left(2^{{R_b}/{W}}-1\right)\Big/\left({R_b}/{W}\right) \quad (26)$$

Это выражение следует из формулы Шеннона. Тогда для некоторого «идеального» метода модуляции рост энергетических затрат при увеличении спектральной эффективности происходит по экспоненциальному закону (рисунок 3). Минимально возможное значение удельных энергетических затрат определяется путем вычисления предела:

$$\left({E_b}/{N_0}\right)_{min} = \lim_{{R_b}/{W}\to 0}\left(\left(2^{{R_b}/{W}}-1\right)\Big/\left({R_b}/{W}\right)\right) = \ln 2(-1{,}6\text{дБ}) \quad (27)$$



а) к оценке энергетических потерь



1- BPSK, QPSK,OQPSK,MSK

2 - DPSK

3 – PSK - 8

4 – QAM - 16

5 – PSK -16

б) кривые помехоустойчивые

Рисунок 2 –Кривые помехоустойчивости различных видов модуляции

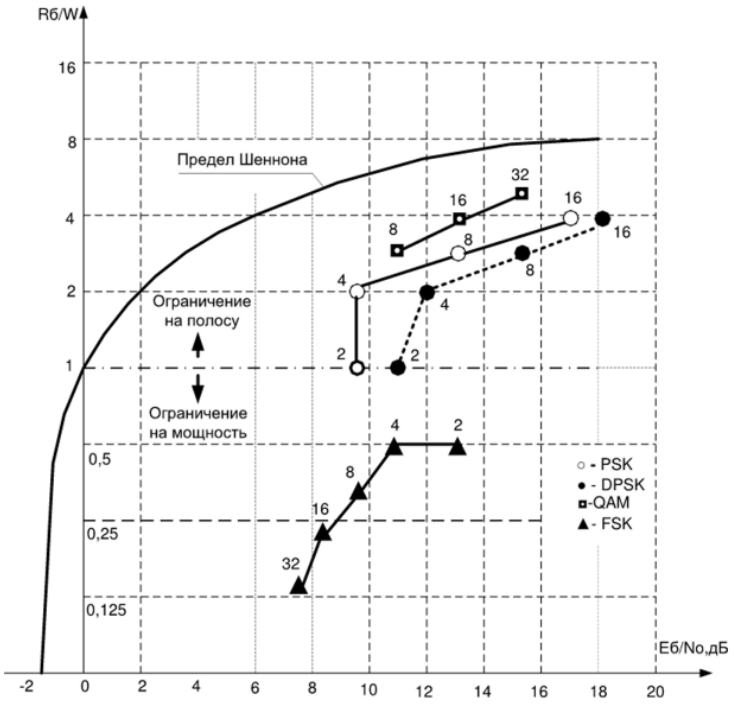


Рисунок 3 –Диаграммы спектрально-энергетической эффективности методов модуляции $(\mathrm{P}_{\text{ош}} = 10^{-5})$

Выводы

1. Методы фазовой и амплитудно-фазовой модуляции являются спектрально-эффективными, так как соответствующие точки располагаются выше разграничительной линии $R_b/_W = 1$. Часть диаграммы, расположенная выше этой линии, соответствует ситуации, когда имеется ограничение на имеющуюся полосу частот. Поэтому увеличение спектральной эффективности может быть достигнуто за счет увеличения позиционности модуляции. При заданном значении вероятности ошибки расплачиваться за это приходится увеличением энергетических затрат.

2. При *FSK* неэффективно используется имеющуюся полоса частот, поскольку соответствующие ей точки располагаются ниже разграничительной линии. Для этого вида модуляции характерны повышенные значения энергетической эффективности. Следует отметить различный характер размена показателей спектральной и энергетической эффективности, лежащих выше и ниже разграничительной линии. В соответствии с формой предельной кривой Шеннона в области, лежащей выше разграничительной линии, этот размен имеет плавный характер. Поэтому за увеличение спектральной эффективности приходится расплачиваться существенным снижением энергетической эффективности. Напротив, в области, лежащей ниже разграничительной линии, небольшие потери энергетической эффективности приводят к заметному увеличению спектральной эффективности. Двухуровневая *FSK* занимает вдвое большую полосу частот, чем *DQPSK*, и по этой причине применяется лишь в системах малой емкости

3. Достаточно высокая эффективность использования спектра может быть достигнута при 16-уровневой квадратурной модуляции. При одном и том же числе позиций при *QAM*-16 требуется меньшее отношение сигнал/шум на входе приемника для достижения одного и того же коэффициента ошибок, чем при 16-PSK.

4. Одним из преимуществ *QAM* является более простая аппаратурная реализация модемов, чем при многопозиционных *PSK*.

5. Существенным недостатком, свойственным всем системам с АМ, в том числе и *QAM*-n, является высокое требование к линейности трактов передачи, что не позволяет эффективно использовать мощность передатчика. Кроме того, эти системы более чувствительны к

межсимвольной интерференции. Тем не менее, данный вид манипуляции активно применяется в высокоскоростных цифровых волоконно-оптических системах связи.

Список использованных источников:

1. Winzer, P.J. Advanced optical modulation formats / R.J. Essiambre – Rimini: Proc. ECOC 2003, 2003. – Vol. 4 – 1002 p.
2. Величко, М.А. Новые форматы модуляции в оптических системах связи / О.Е. Наний, А.А. Сусьян – М.: Lightwave Russian Edition, 2005. – № 4 – 21 с.
3. Kikuchi, K. Coherent transmission system / K. Kikuchi. – ECOC, 2008. – Paper Th2A1.
4. De Lange, O.E. Wideband optical communication systems: Part II'fre' quency division multiplexing / O.E. De Lange – Proc. IEEE, 1970. – Vol. 58. – no. 10 – 1683 p.
5. Okoshi, T. Frequency stabilization of semiconductor lasers for heterodyne'type optical communi' cations systems / K. Kikuchi. – Electron. Lett., 1980. – Vol. 16. – no. 5. – 179 p.
6. Favre, F. High fre' quency stability of laser diode for heterodyne communications systems / D. Le Guen. – Electron. Lett., 1980. – Vol. 16. – no. 18. – 709 p.
7. Derr, F. et al. / F. Derr. – Electron. Lett., 1991. – Vol. 27 – no. 23 – 2177 p.
8. Kikuchi, K. Coherent transmission system / K. Kikuchi. – ECOC, 2008. – Paper Th2A1.
9. 9 В.М.Вишневкий, А.И.Ляхов, С.Л.Портной, И.В.Шахнович. Широкополосные беспроводные сети передачи информации.-М.: Техносфера, 2005.-592 с.

УДК 628.336.42

ТЕХНИЧЕСКИЕ АСПЕКТЫ ВИДЕОСЪЕМКИ В ПОМЕЩЕНИИ

Скорняков Ф.А., студент гр.163001

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. В работе описаны особенности съемки в условиях закрытого помещения, возможности и инструменты обработки исходного видеоматериала, средства для обеспечения лучшего качества видеоматериала.

Ключевые слова. Качественный видеоконтент, закрытое помещение, обработка исходного видеоконтента.

Для того чтобы добиться видеоконтента без технических и визуальных дефектов нужно решить следующие задачи: 1) Проанализировать особенности закрытого помещения. 2) выбрать необходимые технические средства. 3) обработать снятый видеоконтент. 4) оценить обработанный видеоконтент.

К особенностям закрытого помещения относится наличие или отсутствие внешнего (солнечный или лунный свет через окно) и внутреннего (света огонь камина или свет от лампы), а также STC (Sound transmission class) - рейтинг звукоизоляции стен здания, чем он выше – тем лучше. Пример этих особенностей можно увидеть на рисунке 1.

Рисунок 1 – пример закрытого помещения с внутренним и внешним светом

Если имеющегося света в помещении для получения желаемого изображения не хватает, применяют дополнительный свет. Его обеспечивают video lightning kit и light reflector. Благодаря им можно показать объект съемки с такими типами освещения как: общее, отраженное, рассеянное и направленное.

Для непосредственной съемки видео требуется видеокамера с высокими показателями разрешения (количество пикселей на 1 дюйм) и динамического диапазона (диапазон яркости видеокамеры). Пример важности динамического диапазона можно увидеть на рисунке 2.

Рисунок 2 – а) пример влияния динамического диапазона; б) на отображаемое изображение

Для наличия звука в видеоролике используют микрофоны с высоким показателем частотного диапазона. Это позволяет получить наиболее естественный звук. Для большинства случаев подойдут микрофоны с частотным диапазоном от 40–50 Гц до 15 кГц.

После съемок материал отправляется на post-production -- процесс обработки в видеоредакторах (например DaVinci Resolve или Adobe Premiere Pro). В них производят операции выравнивания цветов (цветокоррекция) и звука, а также удаление визуальных и звуковых дефектов.

Выводы

Установлено, что на качество видеоконтента влияют факторы:

1. Исходные условия закрытого помещения: наличие дополнительного, внешнего, внутреннего света и качество звукоизоляции.
2. Технические средства и оборудование: видеокамеры с высокими показателями разрешения и динамического диапазона, микрофон с широким частотным диапазоном.

Так же для улучшения качества видеоконтента рекомендуются следующие операции обработки:

1. Цветокоррекция.
2. Выравнивание звука.

UDC 628.336.42

TECHNICAL ASPECTS OF INDOOR VIDEO

Skarniakou F.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Daneyko T.M. - Senior Lecturer of the Department of ICT

Annotation. The work describes the features of shooting in an enclosed space, the possibilities and tools for processing the original video material, and the means to ensure the best quality of video material.

Keywords. High-quality video content, closed room, processing of original video content.

УДК 628.336.42

ОШИБКИ ПЕРЕПОЛНЕНИЯ И МАСШТАБИРОВАНИЯ БПФ

Копыл М.И., студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь (

Данейко Т.М. – старший преподаватель каф. ИКТ

Аннотация. Данная статья посвящена вопросу предотвращения переполнений разрядной сетки в высокопроизводительных реконфигурируемых вычислительных системах (РВС) на основе ПЛИС, приводящих к фатальным ошибкам обработки данных в процессе получения радиолокационного дальностно-скоростного портрета (ДСП) цели. Кратко рассмотрены существующие способы решения данной проблемы, и предложена методика априорного определения количества точек масштабирования в конвейерно-параллельных вычислительных структурах.

Ключевые слова. Масштабирование, переполнение, корреляционная функция, быстрое преобразование Фурье, временной сдвиг, математическое ожидание.

Данная методика позволяет заранее определить необходимое количество масштабирований на всех этапах обработки целочисленных данных и предотвратить переполнения при вычислении БПФ (ОБПФ) во всех возможных ситуациях. Рассмотрен алгоритм получения ДСП из исходной сигнальной матрицы (ИСМ) на примере радиолокационной системы (РЛС) непрерывного излучения с линейной частотной модуляцией (ЛЧМ). Приведены формулы, позволяющие рассчитать максимально допустимое значение (в используемой разрядной сетке) амплитуды преобразумых сигналов на всех этапах получения ДСП и количество итераций с масштабированием в процедурах БПФ (ОБПФ). Представлен численный пример расчета количества масштабирований для всех этапов алгоритма формирования ДСП, в котором определено необходимое число итераций с масштабированием при вычислении быстрой свертки и доплеровской скорости (с учетом умножения на оконную функцию), позволяющее предотвратить возможный выход значений сигнала за пределы разрядной сетки. В результате установлено, что предлагаемый способ расчета количества масштабирований позволяет избежать чрезмерного падения уровня сигнала на выходе обработки и снизить отношение ошибок цифровой обработки к уровню сигнала дальностно-скоростной матрицы. Масштабирование; дальностно-скоростной портрет; быстрое преобразование Фурье; реконфигурируемые вычислительные системы; цифровая обработка сигналов; линейная частотная модуляция.

Высокопроизводительные реконфигурируемые вычислительные системы (РВС) на основе ПЛИС все чаще находят применение в радиолокации, где требуется обрабатывать большие объемы данных с высоким темпом оцифровки в реальном масштабе времени. Одним из примеров такого применения являются РЛС непрерывного излучения с линейной частотной модуляцией (ЛЧМ), широко используемые в современной радиолокации для обнаружения движущихся объектов. В таких системах в качестве излучаемого сигнала используется периодическая последовательность непрерывно излучаемых ЛЧМ-импульсов с периодом. Соответственно эхо-сигнал, принимаемый от объекта, также будет представлять собой периодическую последовательность ЛЧМ-импульсов, каждый из которых имеет сдвиг несущей частоты на величину доплеровского смещения частоты и временную задержку т относительно излученного импульса. Закон изменения частоты, излучаемого и принимаемого сигналов представлен на рис 1.

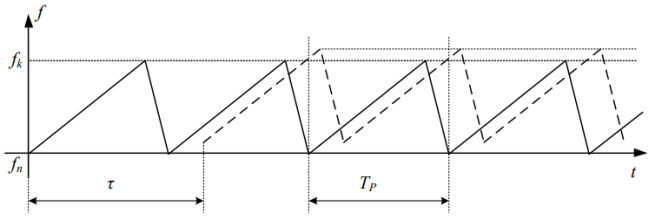


Рис. 1. Закон изменения частоты излучаемого (сплошная линия) и принимаемого (пунктир) сигналов

Основными задачами обработки данных в таких РЛС являются обнаружение и оценка параметров движущихся объектов в координатах дальность-скорость. Для решения задачи оценки дальности и скорости объекта формируется исходная сигнальная матрица (ИСМ), каждая строка которой представляет собой отсчеты отраженного сигнала на интервале приема, равном, а количество строк матрицы рассчитывается из условия обеспечения требуемых характеристик обнаружения. В процессе когерентной обработки принимаемых сигналов с использованием алгоритмов БПФ и ОБПФ происходит преобразование ИСМ в дальностно-скоростной портрет (ДСП), анализируя который можно обнаруживать объекты и оценивать их дальности и скорости. Поскольку формирование дальностно-скоростного портрета происходит в режиме реального времени и с высокой частотой дискретизации сигналов, то для ускорения расчетов цифровая обработка сигналов производится в целочисленной арифметике. В то же время, согласно теореме Парсеваля, при вычислении дискретного быстрого преобразования Фурье происходит увеличение энергии сигнала. Поэтому в процессе получения ДСП возникает вопрос о предотвращении переполнений разрядной сетки, приводящих к фатальным ошибкам обработки. В общем случае проблема недопущения переполнения решается либо введением обязательного масштабирования на каждом этапе преобразования Фурье, либо с помощью приемов, сводящихся к гибридной плавающей точке. Первый способ решения проблемы приводит к возрастанию ошибок цифровой обработки сигналов и уменьшению отношения сигнал/шум на выходе системы обработки. Второй способ требует контроля переполнений на каждой арифметической операции, что снижает быстродействие и усложняет аппаратное обеспечение системы обработки. Более подробно с этими способами можно познакомиться в [20]. Оптимальным решением было бы определение заранее минимального количества масштабирований на всех этапах обработки данных, необходимого и достаточного для отсутствия переполнений. Решению данного вопроса в процессе получения ДСП посвящена эта статья.

Для решения вопроса о необходимом и достаточном количестве масштабирований при формировании ДСП рассмотрим алгоритм его получения из ИСМ. Суть алгоритма заключается в следующем. Сначала производится согласованная фильтрация сигналов в каждой строке ИСМ методом быстрой свертки с применением алгоритмов БПФ и ОБПФ. Затем для каждого канала дальности (каждого столбца преобразуемой матрицы) производится узкополосная доплеровская фильтрация с помощью БПФ, которому предшествует умножение столбца на оконную функцию. Таким образом, преобразование ИСМ в ДСП содержит следующие основные этапы обработки.

1. БПФ по всем строкам ИСМ.
2. Умножение на эталонную функцию всех строк матрицы после этапа 1.
3. ОБПФ по всем строкам матрицы после этапа 2.
4. Умножение всех столбцов матрицы на оконную функцию.
5. БПФ по всем столбцам. Ниже на рис. 2 показана блок-схема преобразования ИСМ в ДСП.

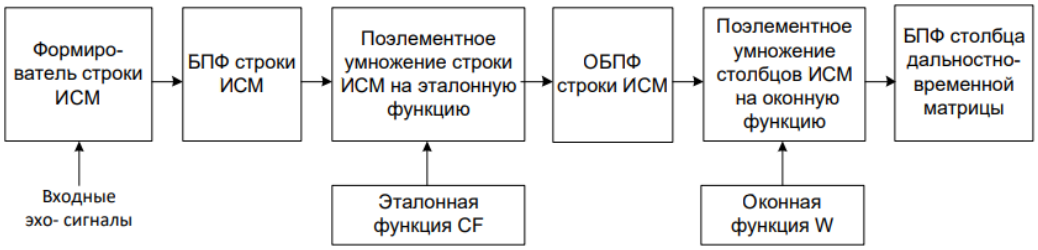


Рис. 2. Блок схема формирования ДСП

В данной статье при решении вопроса о количестве масштабирований на различных этапах формирования ДСП будем исходить из следующих допущений:

1. зондирующий сигнал является непрерывным периодическим сигналом с периодом повторения, в каждом периоде которого излучается импульс с линейной частотной модуляцией (ЛЧМ) в полосе частот; Известия ЮФУ. Технические науки Izvestiya SFedU. Engineering Sciences 146

2. каждая строка сигнальной матрицы содержит сумму отраженных от разных объектов непрерывных сигналов на интервале повторения ; при этом каждый отдельный эхосигнал в строке в общем случае состоит из двух частей, представляющих собой окончание и начало двух смежных периодов отраженных ЛЧМ-импульсов (см. рис. 1);

3. длина строки сигнальной матрицы согласована с длительностью периода излучения ЛЧМ-импульсов и соответветствует обрабатываемому диапазону дальностей;

4. одиночному отраженному ЛЧМ сигналу в отсутствие помех в ДСП соответствует точечный отклик как по координате дальности, так и по координате скорости. Количество итераций с масштабированием в процедурах БПФ и ОБПФ рассчитывается, исходя из требования, что амплитуда преобразумых сигналов на всех этапах получения ДСП не должна превышать максимально допустимое значение в используемой разрядной сетке. При расчете будем опираться на ранее написанные статьи, в которых рассматривались вопросы определения неоходимого количества этапов с масштабированием при вычислении БПФ и при быстрой свертке.

UDC 628.336.42

FFT OVERFLOW AND SCALING ERRORS

Kopyl M.I. st.933701

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Daneiko T.M. – Senior Lecturer of the Department of ICT

Annotation This article is devoted to the issue of preventing bit grid overflows in high-performance reconfigurable computing systems (RCS) based on FPGAs, leading to fatal data processing errors in the process of obtaining a radar range-velocity portrait (RDS) of a target. The existing methods for solving this problem are briefly considered, and a method for a priori determination of the number of scaling points in pipelined-parallel computing structures is proposed.

Keywords: Scaling, overflow, correlation function, fast Fourier transform, time shift, mathematical expectation.

УДК 628.336.42

МОДЕЛЬ ВОЗДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИЗ-ЛУЧЕНИЯ ДИАПАЗОНА 2,4 - 5,0 ГГЦ НА ТКАНИ ТЕЛА ЧЕЛОВЕКА

Бекабаев Д.Д., магистрант гр.167001

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Шевчук О.Г. – канд. техн. наук

Аннотация. В статье обзорно рассматривается технологии 5G New Radio, а также ее применение для IoT, частотные и мощностные режимы работы устройств, в соответствии со спецификацией на данный стандарт, поднимается вопрос о необходимости оценки влияния устройств, поддерживающих данную технологию на организм человека.

Ключевые слова. 5G New Radio, IoT, электрическое поле, магнитное поле, электромагнитое поле, раковые заболевания.

Принципиально новым отличием эволюции систем связи и передачи данных на данный момент является использование технологий IoT (интернет вещей) с применением сетей сотовой связи 5-го поколения 5G NR. Концепция построения глобальной сети подразумевает внутренние передачи данных между физическими объектами – «вещами» с применением технологий WiFi, Bluetooth, ZigBee и др., а также взаимодействие с внешней средой по средствам широкополосного радиодоступа используя стандарты 5G NR. Технология IoT предусматривает одновременное использование до миллиона устройств на квадратный километр, что требует использование высокоскоростной и широкополосной связи для построения внешних сетей. Нежелательной стороной данного вопроса является использование большого количества передающих устройств, что ухудшает электро-магнитную обстановку (ЭМО), а следовательно влияние на здоровье человека.

5G New Radio (5G NR) – новая технология радиодоступа, разработанная 3GPP для мобильной сети 5G. Существует два диапазона частот, в которых может работать 5G NR в соответствии со спецификацией 3GPP TS 38.104 []: FR1 – 410 МГц – 7125 МГц; FR2 – 24250 МГц – 52600 МГц.

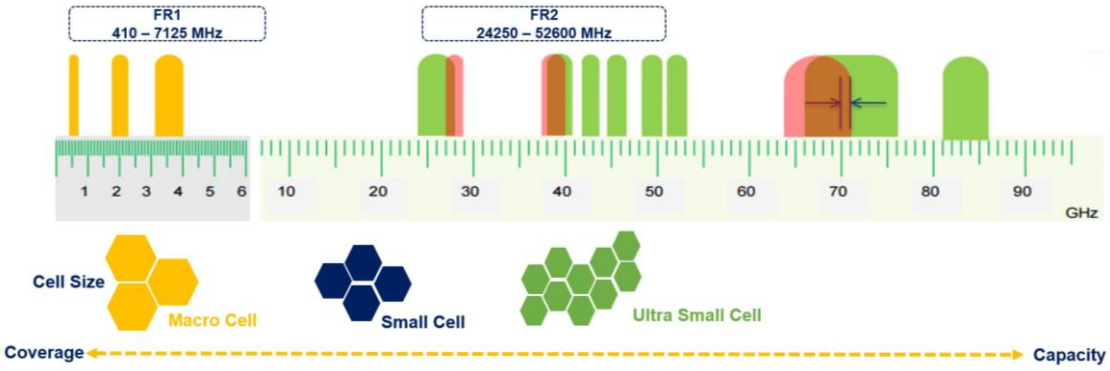


Рисунок 1 – Частотные диапазоны 5G NR

В соответствии со спецификацией 3GPP TS 38.101-1 определено два класса мощности, а именно: класс 2 и класс 3 для FR1. При этом класс мощности 2 используется только для определенных рабочих диапазонов, в то время как класс мощности 3 применим ко всему диапазону частот.

Classes	Max Output Power	Operating Band
Power Class 2	26 dBm	n 41, n77, n78, n79
Power Class 3	23 dBm	All Bands within FR1

Рисунок 2 – Классы мощности диапазона FR1

В соответствии со спецификацией 3GPP TS 38.101-2 определено четыре класса мощности для FR2. Стандарт определяет рпредполагаемый вариант использования для каждого класса мощности:

1. Устройства класса мощности 1 предназначены для FWA и имеют максимальную мощность передачи. Эти устройства можно использовать для обеспечения широкополосного подключения в жилых и офисных помещениях.

2. Классы мощности от 2 до 4, имеющие достаточно большую излучаемую мощность предполагается использовать для мобильных устройств, а также стационарных устройств с высокой мощностью излучения.

Classes	Max TRP	Max EIRP	Min EIRP	Application
Power Class 1	35 dBm	55 dBm	40,38,	FWA UEs
Power Class 2	23 dBm	43 dBm	29	Vehicular
Power Class 3	23 dBm	43 dBm	22.4, 20.6	Handheld UEs
Power Class 4	23 dBm	43 dBm	34, 31	High Power non-Handheld UEs

Рисунок 3 – Классы мощности диапазона FR2

В зависимости от дальности от передающего устройства вклад в ухудшение ЭМО будет определятся следующим образом:

В ближней зоне напряженность электрического и/или магнитного поля;

В дальней зоне интенсивность электромагнитного поля.

Определение ближней и дальней зоны обусловлено частотой излучения и размером передающие антенны.

Воздействия электрических, магнитных и электромагнитных полей неблагоприятно влияет на организм человека: низкочастотные магнитные поля индуцируют циркулирующие токи в организме человека, сила этих токов зависит от интенсивности внешнего магнитного поля, если токи достаточно сильные, они могут оказывать возбуждающее действие на нервную систему и мышечную ткань, а также влиять на другие биохимические процессы, приводить к внутриклеточной поляризации и разогреву тканей. Существуют открытые вопросы о влияние электромагнитных полей на развитие катаракты, неблагоприятного исхода беременности, гиперчувствительности к электромагнитным полям и депрессии, наиболее остро стоит вопрос о влиянии электромагнитных полей на развитие раковых заболеваний.

Окружающие нас уровни воздействия электрических и магнитных полей в домах и в окружающей среде в настоящее время не превышают установленных пороговых значений (5000 В/м – для электрического поля, 100 мкТ – для магнитного поля). Но из-за возрастающей мощности и количества приемо-передающих устройств возникает необходимость оценить наводимую мощность, глубину проникновение сигнала в зависимости от частоты. Данное исследование планируется провести с помощью средств моделирования ЭМИ на различные ткани и органы человека.

Список использованных источников:

1. Thermal behavior of the YAG precursor prepared by sol–gel combustion process / F. Qiu [et al.] // Ceramics International, 2005. – P. 663-665.
3. Третьяков, Ю.Д. Введение в химию твердофазных материалов : учеб. пособие / Ю.Д. Третьяков, В.И. Путляев. – М.: Изд-во Моск. ун-та : Наука, 2006. – 400 с.
4. Цитраты алюминия (III) / В.В. Чевела [и др.] // Ученые записки казанского университета: Естественные науки, 2011. – С.61-69.

УДК 628.336

СИНТЕЗ ОПТИМАЛЬНЫХ ПО ЧЕБЫШЕВУ КИХ-ФИЛЬТРОВ

Чижик А. А., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – магистр технических наук

Аннотация. КИХ-фильтры с ФЧХ. Синтез оптимальных по Чебышеву КИХ-фильтров. Амплитудные характеристики КИХ-фильтров. Теорема чередования. Алгоритм замены Ремеза.

Ключевые слова. КИХ-фильтры. ФЧХ. АЧХ. Синтез. Минимаксная аппроксимация. Оптимальное решение.

В классе КИХ-фильтров с линейной фазочастотной характеристикой (ФЧХ), существует возможность получить множество условий, для которых доказывается, что решение задачи синтеза цифровых фильтров является оптимальным по Чебышёву, то есть оптимальным в смысле минимума максимальной ошибки аппроксимации (иногда называемой минимаксной ошибкой или ошибкой Чебышёва). Фильтры, обладающие свойством оптимальности, отмеченным выше, называются фильтрами с равномерными (равноволновыми) пульсациями, поскольку ошибка аппроксимации данного типа фильтров является равномерно распределенной по его 2 частотным полосам. Как следствие последнего, цифровые фильтры, оптимальные в смысле минимума максимальной ошибки аппроксимации, будут иметь более низкий порядок, чем цифровые фильтры, синтезированные с использованием метода окон, при одинаково заданных спецификациях на синтез фильтров. Фильтры с линейной ФЧХ могут быть классифицированы на 4 типа в зависимости от симметрии или антисимметрии импульсной характеристики h(n), а также четности или нечетности N. Каждый из этих типов имеет собственные ограничения на расположение нулей передаточной функции H(z), которая в свою очередь накладывает ограничения на характер частотной характеристики:

$$H(e^{j\hat{\omega}}) = e^{j\beta} e^{-jN\hat{\omega}/2} A(\hat{\omega}), \qquad (1)$$

где β – константа, зависящая от типа КИХ-фильтра с линейной ФЧХ, $A(\hat{\omega})$ – амплитудная характеристика, представляющая собой действительную функцию частоты $\hat{\omega}$ [рад] и принимающая как положительные, так и отрицательные значения. Модуль амплитудной характеристики есть АЧХ КИХ-фильтра с линейной ФЧХ.

Необходимо отметить, что общее выражение для представления амплитудных характеристик КИХ-фильтров с линейной ФЧХ может быть записано в виде:

$$A(\hat{\omega}) = Q(\hat{\omega})P(\hat{\omega}), \qquad (2)$$

где выражения для $Q(\hat{\omega})$ и $P(\hat{\omega})$ приведены в таблице 1.

Таблица 1 – $Q(\omega)$, L , $P(\omega)$ для КИХ-фильтров с линейной ФЧХ.

Тип КИХ-фильтра с линейной ФЧХ	$Q(\hat{\omega})$	L	$P(\hat{\omega})$
тип 1	1	$\frac{N}{2}$	$\sum_{k=0}^{L} a(n)\cos(k\hat{\omega})$
тип 2	$\cos\left(\frac{\hat{\omega}}{2}\right)$	$\frac{N-1}{2}$	$\sum_{k=0}^{L} \tilde{b}(n)\cos(k\hat{\omega})$
тип 3	$\sin(\hat{\omega})$	$\frac{N-2}{2}$	$\sum_{k=0}^{L} \tilde{c}(n)\cos(k\hat{\omega})$
тип 4	$\sin\left(\frac{\hat{\omega}}{2}\right)$	$\frac{N-1}{2}$	$\sum_{k=0}^{L} \tilde{d}(n)\cos(k\hat{\omega})$

Рассматривая теорему чередования необходимо сказать, что она гарантирует для минимаксной аппроксимации, существование и единственность решения, однако она не дает никакого представления об алгоритме, с использованием которого оптимальное решение может быть получено. Паркс и Макклеллан предложили итерационную процедуру, основанную на алгоритме замены Ремеза (рисунок 1) и позволяющую найти оптимальное решение задачи минимаксной аппроксимации амплитудной характеристики фильтра.

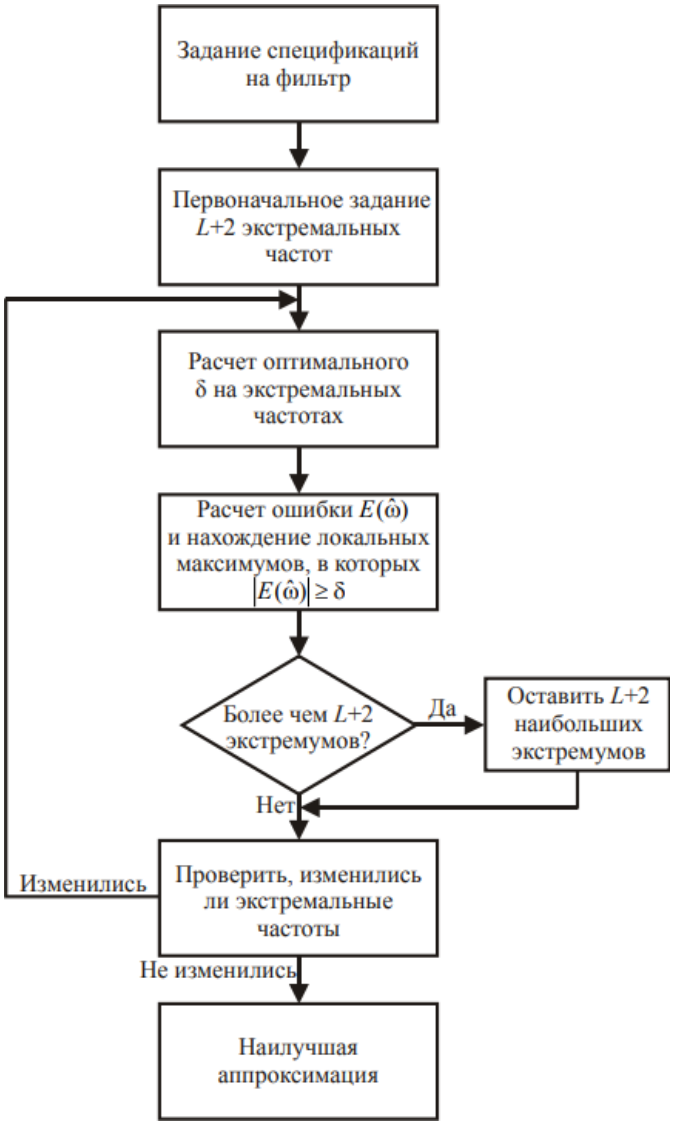


Рисунок 1 – Блок-схема алгоритма замены Ремеза

В заключении необходимо отметить, что приведенный выше оптимальный метод синтеза – это простой и эффективный путь вычисления коэффициентов КИХ-фильтра. Для большинства приложений оптимальный метод синтеза дает хорошие амплитудные характеристики фильтра при разумном порядке фильтра N. Однако, хотя метод и позволяет полностью контролировать спецификации, задаваемые на фильтр, необходимым требованием для его выполнения является наличие программной реализации разрабатываемого фильтра.

Список использованных источников:

1. Брюханов Ю.А., Приоров А.Л. Цифровые фильтры: Учеб. пособие. – Ярославль: ЯрГУ, 2002..
2. Айфичер Э., Джервис Б. Цифровая обработка сигналов: практический подход. 2-е изд. – Вильямс, 2004.
3. Сергиенко А.Б. Цифровая обработка сигналов. – 2-е изд. – СПб.: Питер, 2005.

UDC 628.336

SYNTHESIS OF CHEBYSHEV OPTIMAL FIR-FILTERS

Chizhik A.A., student gr. 960801

Belarusian State University of Informatics and Radioelectronics,

Minsk, Republic of Belarus

Daneiko T.M. – Master of Technical Sciences

Annotation. FIR-filters with phase response. Synthesis of optimal Chebyshev FIR-filters. Amplitude characteristics of FIR-filters. The alternation theorem. Remez replacement algorithm.

Keywords. FIR-filters. FCH. AFC. Synthesis. Minimax approximation. Optimal solution.

УДК 628.336

ЧАСТОТНЫЕ ПРЕОБРАЗОВАНИЯ ЦИФРОВЫХ БИХ-ФИЛЬТРОВ НИЖНИХ ЧАСТОТ

Конон М.С., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – канд. физ.-мат. наук

Аннотация. Фильтры сигналов разделяются на аналоговые и цифровые. Выделяют два класса: КИХ-фильтры и БИХ-фильтры. В зависимости от полосы частот прохождения сигнала фильтры могут быть: ФНЧ, ФВЧ, ПФ и режекторные. В случае цифровых частотно-избирательных фильтров можно сначала рассчитать аналоговый частотно-избирательный фильтр требуемого типа и затем преобразовать этот фильтр в цифровой.

Ключевые слова. Фильтр нижних частот, бесконечно импульсная характеристика, цифровой фильтр.

Фильтром называется цепь (система, устройство), обеспечивающая необходимую реакцию на заданный входной сигнал. Основное применение фильтров заключается в выделении полезного сигнала из аддитивной смеси его с шумом. То есть фильтр преобразует входной сигнал таким образом, что определенные полезные гармоники входного сигнала сохраняются в выходном сигнале, а нежелательные подавляются.

Фильтры сигналов разделяются на аналоговые и цифровые. В аналоговых фильтрах производится преобразование аналоговых (непрерывных) сигналов. Цифровой фильтр, работающий в реальном масштабе времени, оперирует с дискретными по времени данными. При этом очередной отсчет, соответствующий отклику фильтра, формируется по окончании каждого периода дискретизации. Среди цифровых фильтров, в свою очередь, выделяют два фундаментальных класса: фильтры с конечной импульсной характеристикой (КИХ-фильтры или нерекурсивные) и фильтры с бесконечной импульсной характеристикой (БИХ-фильтры или рекурсивные) [1].

В зависимости от полосы частот прохождения сигнала фильтры подразделяются фильтры нижних частот (ФНЧ), верхних частот (ФВЧ), полосовые (ПФ) и режекторные (см. рис.1). Традиционный подход к расчету подобных частотно-избирательных фильтров сводится, во-первых, к расчету нормированного по частоте низкочастотного фильтра-прототипа и затем, на основе алгебраического преобразования, к расчету требуемого фильтра нижних частот, верхних частот, полосового или режекторного типа по данным низкочастотного фильтра-прототипа [2].

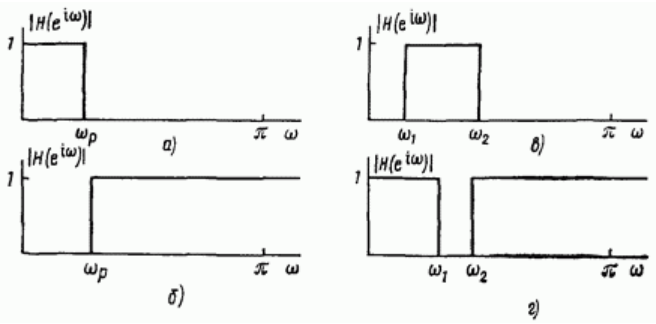


Рисунок 1 - Частотные характеристики идеальных фильтров: а) нижних частот; б) верхних частот; в) полосового; г) режекторного

В случае цифровых частотно-избирательных фильтров можно сначала рассчитать аналоговый частотно-избирательный фильтр требуемого типа и затем преобразовать этот фильтр в цифровой. Другая процедура заключается в расчете цифрового низкочастотного фильтра-прототипа с последующим выполнением для него алгебраического преобразования для того, чтобы получить требуемый частотно-избирательный цифровой фильтр. Эта процедура может

применяться вне зависимости от вида процедуры расчета, использованной для получения цифрового низкочастотного фильтра-прототипа.

Частотно-избирательные фильтры низкочастотного, высокочастотного, полосового и режекторного типов могут быть получены из низкочастотного цифрового фильтра путем использования рациональных преобразований, очень сходных с билинейным преобразованием, которое применялось для преобразования аналоговой передаточной функции в цифровую. Чтобы увидеть, как это выполняется, будем считать, что комплексная переменная z связана с низкочастотной передаточной функцией $H_l(z)$, а комплексная переменная Z — с требуемой передаточной функцией $H_d(Z)$. Затем определим отображение из z-плоскости на Z-плоскость в виде $z^{-1}=G(Z^{-1})$ так, что $H_d(Z)=H_l(G^{-1}(Z^{-1}))$, где $G^{-1}()$ обозначает обратное отображение, т. е. $Z^{-1}=G^{-1}(z^{-1})$. При этом отображение должно быть таким, чтобы рациональная передаточная функция $H_l(z)$, соответствующая устойчивому и физически реализуемому цифровому фильтру, была преобразована в рациональную передаточную функцию $H_d(Z)$, соответствующую снова устойчивому и физически реализуемому цифровому фильтру. Поэтому требуется, чтобы: 1) $G(Z^{-1})$ была рациональной функцией Z^{-1} (или Z); 2) внутренняя область единичного круга z-плоскости должна отображаться во внутреннюю область единичного круга Z-плоскости [3].

Таким образом, если Θ и w являются переменными от частоты в плоскостях z и Z соответственно, т. е. $z=e^{j\Theta}$ и $Z=e^{iw}$, тогда $e^{-i\theta}=|G(e^{-iw})|e^{i\arg[G(e^{-iw})]}$ при $|G(e^{-iw})|=1$ и $\Theta=-\arg[G(e^{-iw})]$.

Приведенное выше выражение определяет соотношение между частотами в плоскостях z и Z. Было показано, что наиболее общая форма функции $G(Z^{-1})$, удовлетворяющая всем вышеуказанным требованиям, имеет вид

$$G(Z^{-1})=\pm\prod_{k=1}^{N}[(Z^{-1}-\alpha_k)/(1-\alpha_k Z^{-1})], \quad (1)$$

где $|\alpha_k|<1$ для устойчивости. Путем выбора соответствующих значений для N и констант α_k можно получить множество отображений. Простейшим является то, которое преобразует один фильтр нижних частот в другой фильтр нижних частот. Для этого случая

$$z^{-1}=G(Z^{-1})=(Z^{-1}-\alpha)/(1-\alpha Z^{-1}). \quad (2)$$

Если подставить $z=e^{i\Theta}$ и $Z=e^{iw}$, то получим выражение $e^{-i\Theta}=(e^{-iw}-\alpha)/(1-\alpha e^{-iw})$, из которого можно увидеть, что

$$w=arctg[(1-\alpha^2)sin\theta/(2\alpha+(1+\alpha^2)cos\theta)]. \quad (3)$$

Характер этой взаимозависимости для различных значений α показан на рис. 2.

Хотя искажение шкалы частот очевидно на рис. 2 (за исключением α=0) в случае, если исходная система имеет кусочно-постоянную частотную характеристику в области нижних частот с частотой среза Θ_p, то преобразованная система будет также иметь подобную низкочастотную характеристику с частотой среза w_p, определенную выбором α. Выразив α через Θ_p и w_p, получим

$$\alpha=\sin((\theta_p-w_p)/2)/\sin((\theta_p+w_p)/2). \quad (4)$$

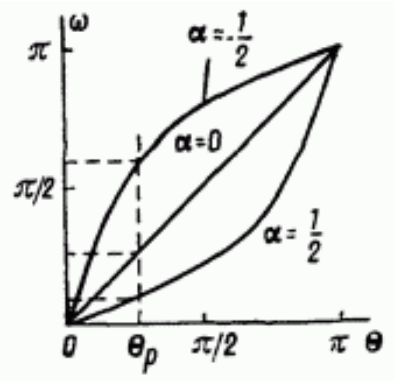


Рисунок 2 - Искажения шкалы частот при преобразовании типа нижние частоты — нижние частоты

Таким образом, чтобы использовать эти результаты для получения $H_d(Z)$ фильтра нижних частот с частотой среза w_p из уже имеющейся $H_l(z)$ фильтра нижних частот с частотой среза Θ_p, следовало бы воспользоваться вышеприведенным соотношением для определения α из выражения $H_d(\mathrm{Z}) = H_l(\mathrm{z})|_{z^{-1}=(z^{-1}-\alpha)/(1-\alpha z^{-1})}$.

Список использованных источников:

1. Голышев Н.В., Щетинин Ю.И. Теория и обработка сигналов: Учеб.пособие.- Новосибирск: Изд-во НГТУ, 1998
2. Сергиенко А.Б. Цифровая обработка сигналов.- СПБ.:Питер,2003
3. Оппенгейм А. В., Шафер Р. В. Цифровая обработка сигналов: Пер. с англ / Под ред. С. Я. Шаца. — М.: Связь, 1979.

UDC 628.336

FREQUENCY CONVERSION OF DIGITAL IIR LOW-PASS FILTERS

Konon M.S.

Belarusian State University of Informatics and Radioelectronics[1], Minsk,Republic of Belarus

Daneyko T.M. – PhD in Physics and Mathematics

Annotation. Signal filters are divided into analog and digital filters. There are two classes: FIR filters and IIR filters. Depending on the bandwidth of the signal, filters can be: VLF, VHF, PF, and regenerative. In the case of digital frequency selective filters, you can first calculate an analog frequency selective filter of the desired type and then convert this filter to digital.

Keywords. Low-pass filter, infinite-pulse response, digital filter.

УДК 628.336

ХАРАКТЕРИСТИКИ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ ВЕСОВЫХ ФУНКЦИЙ В ЗАДАЧАХ ЦОС

Ревтович П.И., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель

Аннотация. В данной работе описаны основные весовые функции, использующиеся в цифровой обработке сигналов, а также отмечены их основные характеристики.

Ключевые слова. весовые функции, цифровая обработка сигналов, характеристики, спектр, оконные функции, окна

В цифровой обработке сигналов широко применяются весовые функции, которые также называются оконными либо же просто окнами. Использование такого рода функций в первую очередь обусловлено тем, что с их помощью можно добиться существенного уменьшения растекания спектра при дискретном преобразовании Фурье (ДПФ). Такой эффект достигается путем приведения отсчетов в начале и конце последовательности к одному общему значению, вследствие чего уменьшается уровень боковых лепестков спектра. Следует также отметить, что АЧХ идеального окна должна соответствовать АЧХ идеального фильтра нижних частот, имеющего предельно узкую полосу пропускания, что на практике невозможно, поэтому полностью устранить растекание спектра при помощи весовых функций невозможно.

В настоящее время известно несколько десятков различных по эффективности весовых функций. Наиболее распространенные и часто используемые из них представлены в таблице 1.

Таблица 1 – Весовые функции и выражения для них

Наименование окна	Выражение в дискретном виде
Прямоугольное окно	$w(n) = 1$
Окно Хемминга	$w(n) = 0,54 - 0,46\cos\left(\frac{2\pi n}{N-1}\right)$
Окно Ханна	$w(n) = 0,5 - 0,5\cos\left(\frac{2\pi n}{N-1}\right)$
Окно Барлетта (треугольное окно)	$w(n) = 1 - \left\lvert\frac{n}{A} - 1\right\rvert, \quad A = \frac{N-1}{2}$
Окно Гаусса	$w(n) = \exp\left(-\frac{1}{2}\cdot\left(\frac{n-A}{\sigma\cdot A}\right)^2\right), \quad A = \frac{N-1}{2}$

Для описания эффективности весовых функций введены несколько параметров:

1. Приведенная ширина основного лепестка F_γ – данный параметр равен произведению ширины основного лепестка АЧХ и длительности весовой функции. Смысл параметра в том, что, зная его,

а также частоту, с которой необходимо подавлять пульсации, не составит труда определить длительность окна.

2. Максимальный уровень боковых лепестков γ_{max} – характеристика показывает отношение наибольшего бокового лепестка к амплитуде основного лепестка, как правило измеряется в децибелах.

3. Коэффициент ослабления оконной функции β – показывает, во сколько раз уменьшаются амплитуды всех спектральных составляющих по сравнению с прямоугольным окном. Выражается в логарифмической шкале.

4. Нормированная ширина главного лепестка по уровню 0,5 $\Delta F_{0,5}$

5. Нормированная ширина главного лепестка по нулевому уровню ΔF_0

Различия в эффективности весовых функций можно увидеть на рисунке 1. Так, спектр прямоугольного окна в основном используется как эталон для оценки спектров других окон, в то время как окна Хемминга, Хеннинга и Барлетта заметно снижают уровень боковых лепестков.

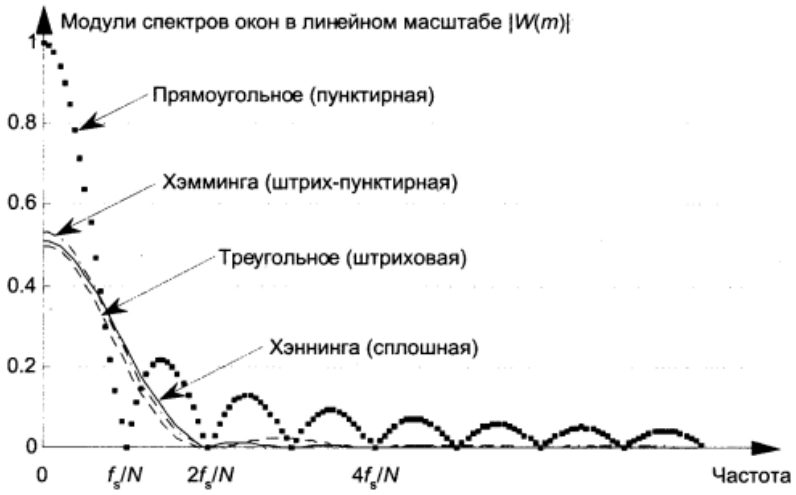


Рисунок 1 – Спектры различных оконных функций

В таблице 2 приведены все основные характеристики для весовых функций, указанных ранее.

Таблица 2 – Характеристики весовых функций

Наименование функции	F_γ	$\Delta F_{0,5}$	ΔF_0	γ_{max}, дБ	β, дБ
Прямоугольное окно	–	0,89	2	-13	0
Окно Хемминга	1,92	1,33	4	-42	-5,37
Окно Ханна	1,88	1,5	4	-31,5	-6
Окно Барлетта (треугольное окно)	1,63	1,33	4	-26,5	-6
Окно Гаусса	3,34	1,82	8	-65	-8,52

Список использованных источников:

1. Understanding digital signal processing / Richard G. Lyons // Prentice Hall, 2004. – P. 91-97.
2.Сергиенко А.Б. Цифровая обработка сигналов / – СПб.: Питер, 2003. – С. 273-274.

UDC 628.336

CHARACTERISTICS OF THE MOST COMMON WEIGHT FUNCTIONS IN DSP PROBLEMS

Revtovich P.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Daneiko T.M. – Senior Lecturer

Annotation. This paper describes the main weight functions used in digital signal processing, and also notes their main characteristics.

Keywords. weight functions, digital signal processing, characteristics, spectrum, rectangular function, window.

УДК 629.735

МЕТОД МОДИФИЦИРОВАННЫХ ПЕРИОДОГРАММ БАРТЛЕТТА ДЛЯ ОПРЕДЕЛЕНИЯ ЭНЕРГЕТИЧЕСКОГО СПЕКТРА СИГНАЛОВ

Криволап М.В., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Исследована сущность метода модифицированных периодограмм Бартлетта для определения энергетического спектра сигнала. Изучили этапы вычисления СПМ, расчет периодограмм

Ключевые слова. Основные свойства, среднее значение, разрешающая способность и дисперсия.

Пусть заданы шаг дискретизации Δt анализируемого процесса x(t) и число отсчетов L действительной последовательности x (k) . Выделим следующие этапы вычисления СПМ:

1) Разделим последовательность x (k) на P неперекрывающихся сегментов по N отсчетов в каждом (рис. 1), т. е. L=P*N. Выбор N= 2^{ν}, ν –целое, позволяет использовать стандартный алгоритм БПФ.

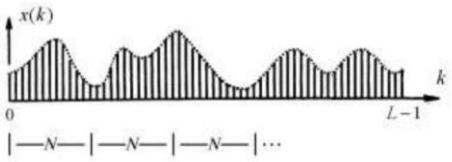


Рисунок 1– Секционирование входной последовательности при вычислении СПМ по методу Бартлетта

2) Вычисление ДПФ последовательности по каждому сегменту:

$$X_P(n) = \frac{1}{N}\sum_{k=0}^{N-1} x_P(k\,\Delta t)e^{-j\frac{2\pi}{N}nk}$$

где $x_P(k) = x(pN + k), p = 0, 1, 2, \dots P - 1$

3) Расчет периодограмм:

$$G_P(n\Delta f) = N\Delta t[X_P(n)]^2$$

где $\Delta \mathrm{f} = 1/\mathrm{N}\Delta \mathrm{t}$– шаг сетки частот при ДПФ

Основные свойства периодограммы Бартлетта:

Среднее значение: $E\{S_{\text{Б}}(w)\} = \frac{1}{2\pi} S_x(w) * W_{\text{Б}}(w)$

Разрешающая способность: $\Delta w = 0.89K\frac{2\pi}{N}$

Дисперсия: $D\{S_{\text{Б}}(w)\} \approx \frac{1}{K} S_x^2(w)$

Список использованных источников:

1. Кошелев, В. И. Адаптивная обработка радиолокационных сигналов на базе процессора БПФ / В. И. Кошелев // Цифровая обработка сигналов. – 2001. — 4. – С. 12-17.
2. Марпл, С. Л. Цифровой спектральный анализ и его применения: Пер. с англ. / С. Л. Марпл. – М.: Мир, 1990. – 584 с
3. Шахтарин, Б. И. Методы спектрального оценивания случайных процессов / Б. И. Шахтарин, В. А. Ковригин. – М.: Гелиос АРВ, 2005. – 248 с
4. Глухоманюк, Г. Г. Роль высокочастотной области спектра вибрационного сигнала в вибродиагностике механизмов / Г. Г. Глухоманюк // Контроль. Диагностика. – 2001. — 2. – С. 28-32.

UDC 629.735

Method of modified bartlett periodograms for determining the energy spectrum

Krivolap M.V.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Daneiko T.M. – Senior Lecturer of department of ICT

Annotation. The essence of the method of modified Bartlett periodograms for determining the energy spectrum of a signal is investigated/ Studied the steps of calculating SPM, calculating periodograms.

Keywords. Basic properties mean value, resolution and dispersion

УДК 621.391

РЕКУРСИВНЫЕ КИХ-ФИЛЬТРЫ ЧАСТОТНОЙ ВЫБОРКИ

Кутасин И.А.[1], студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Был рассмотрел рекурсивный способ реализации КИХ-фильтров, основанный на задании коэффициентов ДПФ. После этого была произведена оценка для получения частотной характеристики фильтра. Реализация КИХ-фильтра методом частотной выборки с использованием гребенчатого фильтра и рекурсивного фильтра с передаточной функцией. Вывод на примере отношения функций в виде полиномов.

Ключевые слова. Коэффициент ДПФ, выборочные значения, сумма частотных откликов, гребенчатый фильтр, рекурсивный фильтр.

Одним из трех методов расчета КИХ-фильтров с линейной фазой является метод частотной выборки. Используем передаточную функцию.

$$H(z) = \sum_{k-0}^{N-1} h(k) z^{-k} \cdot \quad (1)$$

Для этого представим через выборочное значение функции полинома *H(n)* с помощью обратного ДПФ, где частотные выборки берутся с шагом *1/NΔt* и подставим это в выражение (1).

$$h(k) = 1/N \sum_{n=0}^{N-1} H(n) exp\left(\frac{j2\pi k}{N}\right) \cdot \quad (2)$$

Получим выражение

$$H(z) = \sum_{n=0}^{N-1} \frac{H(n)}{N} \sum_{k=0}^{N-1} z^{-k} \exp\frac{j2\pi nk}{N} = \sum_{n=0}^{N-1} \frac{H(n)}{N} \frac{1-z^{-N}}{1-z^{-1}\exp(j2\pi n/N)}. \quad (3)$$

Произведя оценку из выражения (3), где $z = exp(2\pi f\Delta t)$,получаем частотную характеристику фильтра:

$$\begin{aligned} H(f) &= \sum_{n=0}^{N-1} \frac{H(n)}{N} \frac{1-\exp(-j2\pi fN\Delta t)}{1-\exp\left[-j2\pi(f\Delta t - n/N)\right]} = \\ &= \sum_{n=0}^{N-1} \frac{H(n)}{N} \frac{\exp(-j\pi fN\Delta t)\cdot \le \operatorname{Sin} \pi fN\Delta t}{\exp\left[-j\pi(f\Delta t - n/N)\right]\cdot \operatorname{Sin}\pi(f\Delta t - n/N)} = \\ &= e^{-j\pi f\Delta t(N-1)} \sum_{n=0}^{N-1} \frac{H(n)}{N} e^{-j\pi n/N} \frac{\operatorname{Sin} n\pi fN\Delta t}{\operatorname{Sin} n\pi(f\Delta t - n/N)}. \end{aligned} \quad (4)$$

где при *f=n/NΔt* имеет место *H(f)=H(n).*

Отношения (3) и (4) показывают, что частотный отклик КИХ-фильтра является суммой частотных откликов вида *Sin(Nx)/Sin(nx),* которое можно увидеть на рисунке 1. Каждый из них имеет комплексный вес H(n) и центральную частоту *n/NΔt,* где *n=0,1,2,…,N-1.*

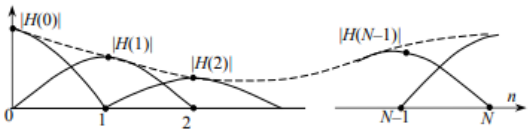


Рисунок 1 – Формирование частотного отклика КИХ-фильтра

Для реализации КИХ-фильтра методом частотной выборки построим его схему:

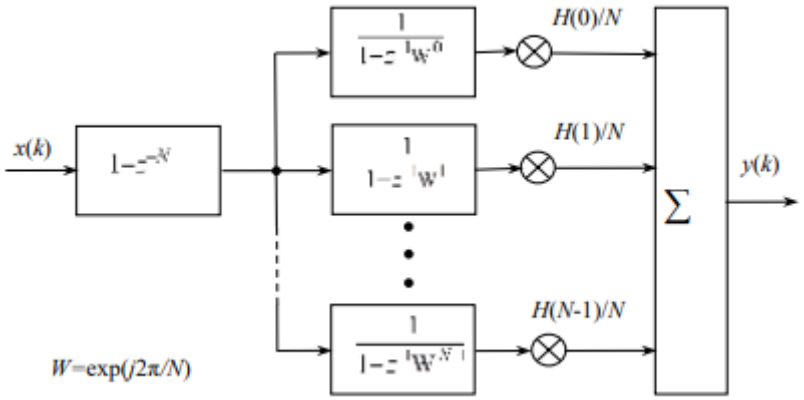


Рисунок 2 – Реализация КИХ-фильтра методом частотной выборки $(W = exp\left(\frac{j2\pi}{N}\right))$.

В данной схеме блок с передаточной функцией *(1-z^{-N})* является общим. По виду частотной характеристики является гребенчатым фильтром. Идущий следом рекурсивный фильтр с передаточной функцией $\frac{1}{1-z^{-1}w^{n}}$ имеет полюс в точке *z = W^n* и имеет отклик бесконечной длительности $exp\left(\frac{j2\pi}{N}\right)$, *n=0,1,2,…,N-1; 0 ≤ k< ∞*. Однако использование гребенчатого фильтра импульсная характеристика каждого подфильтра является конечной, делая его КИХ-фильтром.

Вывод: в ходе ряда вычислений мы ознакомились с рекурсивным методом реализации КИХ-фильтра, подставив в передаточную функцию выборочные значения функции полинома и используя ДПФ. После этого произведя оценку и сравнив полученные функции увидели связь частотного отклика КИХ-фильтра с суммой частотных откликов. После этого была построена схема КИХ-фильтра с использованием гребенчатого и рекурсивного фильтра.

Список использованных источников:

1. Цифровая обработка сигналов КИХ-фильтры //Лекционный материал Московского физико-технического института

UDC 621.391

RECURSIVE FREQUENCY SAMPLING FIR FILTERS

Kutasin I.A.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Daneyko T.M. – Lecturer department of ICT

Annotation. A recursive way to implement FIR filters was considered, based on setting the DFT coefficients. After that, an estimate was made to obtain the frequency response of the filter. FIR filter implementation by frequency sampling method using a comb filter and a recursive filter with a transfer function. Derivation on the example of the ratio of functions in the form of polynomials.

Keywords. DFT coefficient, sampled values, sum of frequency responses, comb filter, recursive filter.

One of the three methods for calculating linear phase FIR filters is the frequency sampling method. We use the transfer function.

$$H(z) = \sum_{k-0}^{N-1} h(k) z^{-k} \cdot \quad (1)$$

To do this, we represent through the sample value of the polynomial function H(n) using the inverse DFT, where frequency samples are taken with a step of 1/NΔt and substitute this into expression (1).

$$h(k) = 1/N \sum_{n=0}^{N-1} H(n) exp\left(\frac{j2\pi k}{N}\right) \cdot \quad (2)$$

We get the expression

$$H(z) = \sum_{n=0}^{N-1} \frac{H(n)}{N} \sum_{k=0}^{N-1} z^{-k} \exp\frac{j2\pi nk}{N} = \sum_{n=0}^{N-1} \frac{H(n)}{N} \frac{1 - z^{-N}}{1 - z^{-1} \exp\left(j2\pi n/N\right)} \cdot \quad (3)$$

Having estimated from expression (3), where z = exp(2πfΔt), we obtain the frequency response of the filter:

$$\begin{aligned} H(f) &= \sum_{n=0}^{N-1} \frac{H(n)}{N} \frac{1 - \exp\left(-j2\pi fN\Delta t\right)}{1 - \exp\left[-j2\pi\left(f\Delta t - n/N\right)\right]} = \\ &= \sum_{n=0}^{N-1} \frac{H(n)}{N} \frac{\exp\left(-j\pi fN\Delta t\right) \cdot \leq \operatorname{Sin} \pi fN\Delta t}{\exp\left[-j\pi\left(f\Delta t - n/N\right)\right] \cdot \operatorname{Sin} \pi\left(f\Delta t - n/N\right)} = \\ &= e^{-j\pi f\Delta t(N-1)} \sum_{n=0}^{N-1} \frac{H(n)}{N} e^{-j\pi n/N} \frac{\operatorname{Sin} n\pi fN\Delta t}{\operatorname{Sin} n\pi\left(f\Delta t - n/N\right)} \cdot \end{aligned} \quad (4)$$

where for f=n/NΔt we have H(f)=H(n).

Relations (3) and (4) show that the frequency response of the FIR filter is the sum of the frequency responses of the form Sin(Nx)/Sin(nx), which can be seen in Figure 1. Each of them has a complex weight H(n) and a central frequency n/NΔt, where n=0,1,2,…,N-1.

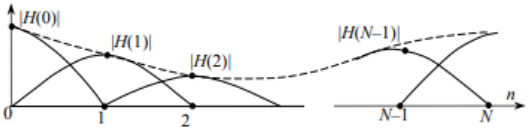


Рисунок 1 – Формирование частотного отклика КИХ-фильтра

To implement the FIR filter using the frequency sampling method, we construct its circuit:

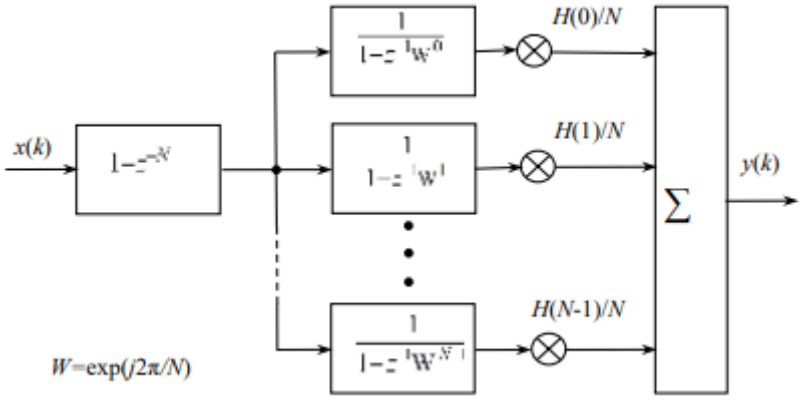


Рисунок 2 – Реализация КИХ-фильтра методом частотной выборки $(W = exp\left(\frac{j2\pi}{N}\right))$.

In this scheme, the block with the transfer function $(1-z^{-N})$ is common. In terms of frequency response, it is a comb filter. Following recursive filter with transfer function. The next recursive filter with transfer function $\frac{1}{1-z^{-1}w^{n}}$ has a pole at the point $z = W^n$ and has a response of infinite duration $exp\left(\frac{j2\pi}{N}\right)$, $n=0,1,2,\ldots,N-1;\ 0 \le k < \infty$. However, using a comb filter, the impulse response of each subfilter is finite, making it a FIR filter.

Conclusion: in the course of a series of calculations, we got acquainted with the recursive method of implementing the FIR filter by substituting the sample values of the polynomial function into the transfer function and using the DFT. After that, after evaluating and comparing the obtained functions, we saw the relationship between the frequency response of the FIR filter and the sum of the frequency responses. After that, a FIR filter circuit was built using a comb and recursive filter.

List of sources used:

1. Digital signal processing FIR filters // Lecture material of the Moscow Institute of Physics and Technology.

UDC 628.336

NOISE REDUCTION METHOD FOR SKELETONIZED IMAGES

Yuan Liu, Master student

Belarusian state university of informatics and radioelectronics

г. Minsk, Republic of Belarus

S. B. Salomatin

Annotation. Thinning framework that based on the scale space technique to automatically extract skeletons from images without manual-tuning. The proposed framework can increase the robustness of the thinning algorithm, it not only can suppress the boundary noise, but also can alleviate the inner noise. These two types of noise generally cause the appearance of the abundant of the unwanted branches in the outcome of the thinning algorithm, which arise the difficulties of the later recognition or matching process in skeleton.

Keywords. Skeleton. Robustness. inner noise. boundary noise.

Skeletons, that extracted by the thinning algorithms, preserve the topology and connectivity of the original objects, hence they are compact and useful image descriptors that can used in many various fields of pattern recognition [1]. However, one of the challenges of the applying of the skeleton is that almost all the thinning algorithms fail to well suppress the effect of the noise, which may cause much unwanted branches in skeletons.

The noise can divided into two classes, which are border noise and inner noise. Border noise is the noise that along the boundary of the foreground pixels and background pixels. They may cause the appearance of many extra branches. Whereas inner noise is the noise that appear in the inner of the objects and far from the boundary, they may cause the appearance of the false hole. Both of these noise may dramatically influence the resulting skeletons.

Pruning methods [2] are proposed in the past decade for removing the redundant branches. These methods can dramatically improve the thinning algorithm robustness against to the border noise. These methods are generally applied directly on the skeleton that extracted by the thinning procedure from the original pattern. However, one of the limitations of these methods is that it fails to suppress the inner noise.

Another type of methods for promoting the performance of the robustness of the thinning algorithms are the methods that based on scale-space filter. When there is a suitable smooth parameter, these methods can not only deal with the border noise but also offset the effects that caused by the inner noise. However, it is a tough task to find a suitable smooth parameter. As we know, a large smooth parameter may deform the original pattern and a small smooth parameter may not be able to suppress all the types of noise.

A scale-space method for thinning both grayscale and binary images has proposed by Hoffman and Wong[3]. This method first produces filtered versions of an input image and then extracts skeleton by searching some special pixels from it, which includes peak, ridge and saddle pixels. These pixels are named as the most prominent ridge line pixels (MPRL) by authors and they are used to form the skeleton. In the image scale space pyramid, each MPRL pixel is a pixel such that all ridge-line pixels have greater second derivatives in sub-pyramid. The robustness of the skeleton against to the noise strongly depends on a parameter, which requires manual tuning.

Cai has proposed a robust filtering-based thinning algorithm [] for pattern recognition in 2012 to offset the effects of the contour noise caused by pen perturbations and image scanning in the field of handwriting and fingerprints by introducing Oriented Gaussian Filters. The Oriented Gaussian Filters are used to divide the pixels into edges, valleys and ridges, which presents information for the trimming. The skeleton extracted by this method does not have any redundant branch. However, their method can only be applied on the field of handwriting and fingerprints, and the Oriented Gaussian Filters should predetermine in advance.

Houssem Chatbri and Keisuke Kameyama proposed a framework to make thinning algorithms robust against noise in sketch image. By using sensitive measure to evaluate skeletons extracted from different grayscale images which filtered by different scales, they can automatically obtain the skeleton that has the lowest value on sensitive measure. Their sensitive measure focus on the skeleton variation, which counts the numbers of the connected points and fake skeletal points (which exist in the skeleton, but not in the original pattern) in skeleton. Therefore, their methods prefer to selecting the concise skeleton rather than a complex one. However, the connectivity and topology of the skeleton produced by their methods may change.

In this paper, an improved thinning framework based on Houssem's method is presented. The framework uses different scales to blur the original image so that internal and boundary noise can be filtered out. Then, we pass the blurred image to the binarization procedure, the skeletonization procedure and the evaluation procedure in turn to obtain an ideal skeleton. The whole framework is described as follows.

Input: Original grayscale image I, maximum scale σ_{max}, increase step st.

Output: The best skeleton I_{mth}

Step 1: Initialize the scale of the Gaussian filter σ_0 with 0;

Step 2: use Gaussian filter with a scale of σ to blur the image I and obtain a grayscale image I_g;

Step 3: Binarize I_g to generate a binary image I_b;

Step 4: Extract the skeleton I_{th} from I_b using the FPSA thinning algorithm;

Step 5: Calculate the sensitivity measure S_σ of the skeleton I_{th} and record it in the memory;

Step 6: If the sum of σ and the st is less than σ_{max}, increase σ with a given step st and go to the step 2; Otherwise, go to step 7;

Step 7: Find the smallest S_m and then obtain corresponding skeleton I_{mth}

The input and output of the proposed frameworks are the original grayscale image I and the best skeleton S_m respectively. The framework iteratively generates the various skeletons that are extracted from the grayscale image that is blurred by gaussian filters with different scale parameters which is gradually increased from 0 (denote we do not conduct the filter operation) to a given number. In each iteration, the original image should be processed by the four procedures, which are gaussian filter procedure, binarization procedure, thinning procedure and evaluation procedure.

The input of this procedure is the grayscale image and outputs the blurred grayscale image I_G. The Gaussian filter is defined by the following formula.

$$\mathrm{G}(\mathrm{x},\mathrm{y},\sigma)=\frac{1}{2\pi\sigma^2}e^{-\frac{(\mathrm{x}+\mathrm{y})^2}{2\sigma^2}}$$

where σ is the smoothing parameter that controls the scale, and x and y are the pixel coordinates.

The input of this procedure is the blurred image that is obtained from the previous procedure. The output is the binary image. Here we adopt an adaptive binarization, using the average of non-white grayscale intensities as the threshold for binarization th:

$$th=\frac{1}{N_b}\sum_{i=0}^{N}\sum_{j=0}^{M}f(i,j)$$

Here N_b is the number of foreground pixels in the image, M and N are the dimensions of image I, and function f is defined as follows:

$$f(i,j)=\begin{cases}0, & \text{if} \quad I_{G(i)}(i,j)=255,\\ I_{G(i)}(i,j), & \text{otherwise.}\end{cases}$$

Experiments and results

It is clear that in the following figure, the skeleton extracted by FPSA has many skeleton rings caused by internal noise. And both Houssem's method and the proposed method can eliminate these rings very well. But Houssem's method fails to maintain the original topology because there is a ring at the tail of the skeleton. The proposed method in this paper can basically obtain a good skeleton.

a b c

Conclusion

It is experimentally demonstrated that the proposed method in this paper can suppress internal noise and boundary noise and has better performance than the existing Houssem framework in terms of topology preservation and connection preservation.

References:

1. M. Fons, F. Fons and E. Cantó, "Fingerprint Image Processing Acceleration Through Run-Time Reconfigurable Hardware," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 57, no. 12, pp. 991-995, Dec. 2010, doi: 10.1109/TCSII.2010.2087970.

2. X. Bai, L. J. Latecki and W. Liu, "Skeleton Pruning by Contour Partitioning with Discrete Curve Evolution," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 3, pp. 449-462, March 2007, doi: 10.1109/TPAMI.2007.59.

3. *M. E. Hoffman and E. K. Wong, "Scale-space approach to image thinning using the most prominent ridge-line in the image pyramid data structure.", in: Photonics West'98 Electronic Imaging, International Society for Optics and Photonicss, 1998.*

УДК 621.391

КИХ-ФИЛЬТР С АНТИСИММЕТРИЧНОЙ ИМПУЛЬСНОЙ ХАРАКТЕРИСТИКОЙ

Морозов К.В.[1], студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. Проведено исследование цифровых фильтров с конечной импульсной характеристикой, обладающей нечетной симметрией. Установлено, что антисимметричная импульсная характеристика фильтра позволяет обеспечить линейность фазо-частотной характеристики фильтра. При этом, в отличие от КИХ-фильтров с импульсной характеристикой с четной симметрией, обеспечивается постоянство только групповой задержки, но не фазовой.

Ключевые слова. Цифровой фильтр, конечная импульсная характеристика, нечетная симметрия, фазо-частотная характеристика, групповое время запаздывания, фазовая задержка.

В ряде практических задач требуется обеспечивать линейность фазо-частотной характеристики цифрового фильтра. Это можно выразить через следующую формулу:

$$\varphi(\omega) = \varphi_0 - \alpha\omega, \tag{1}$$

где φ_0 – постоянная величина;

α – постоянная фазовая задержка.

В данном случае, линейность ФЧХ будет обеспечивать постоянство только группового времени запаздывания τ(ω), равного произведению (-1) и производной от ФЧХ по частоте, но не фазовой задержки θ(ω), равной произведению (-1) и отношения фазы к частоте.

Проведя ряд преобразований, можно получить условия, обеспечивающие линейную ФЧХ вида (1):

$$\alpha = (N - 1)/2, \tag{2}$$

$$\varphi_0 = \pm(\pi/2), \tag{3}$$

$$g(n) = -g(N - 1 - n), \quad 0 \le n \le N - 1. \tag{4}$$

N может быть как четным, так и нечетным целым числом. На рисунке 1 представлен вид антисимметричных импульсных характеристик при нечетном (а) и четном (б) N [1].

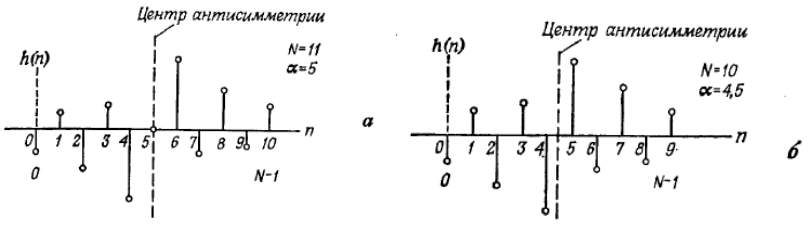


Рисунок 1 – Антисимметричные импульсные характеристики при нечетном (а) и четном (б) N

Вывод: основной причиной использования КИХ-фильтров с антисимметричной импульсной характеристикой является возможность обеспечить в данном случае линейность ФЧХ фильтра. При этом, в отличие от КИХ-фильтров с симметричной импульсной характеристикой, также способных обеспечить линейную ФЧХ, фильтры с антисимметричной ИХ имеют постоянное только групповое время запаздывания, но не фазовую задержку. Рассмотренные условия используются при расчете дифференциаторов и преобразователей Гильберта.

Список использованных источников:

1. Рабинер, Л. Теория и применение цифровой обработки сигналов / Л. Рабинер, Б. Гоулд. – М. : Изд-во Мир, 1978. – 848 с.

UDC 621.391

FIR-FILTER WITH ANTISYMMETRIC IMPULSE RESPONSE

Morozov K.V.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Daneiko T.M. – senior lector of department of ICT

Annotation. A study was made of digital filters with a finite impulse response with odd symmetry. It has been established that the antisymmetric impulse response of the filter makes it possible to ensure the linearity of the phase-frequency response of the filter. In this case, unlike FIR-filters with an impulse response with even symmetry, only the group delay is constancy, but not the phase delay.

Keywords. Digital filter, finite impulse response, odd symmetry, phase-frequency response, group delay, phase delay.

УДК 628.336

МАТЕМАТИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ НЕЙРОННЫХ СЕТЕЙ

Колодей Г.А., студент гр.133702

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Чепикова В.В. – магистр технических наук

Аннотация. В докладе приводится пример математического представления нейронных сетей и их виды.

Ключевые слова. Нейронная сеть, математика, виды нейронных сетей, принцип работы нейронных сетей.

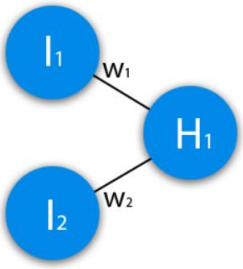
Введение

Нейронные сети, также известные как искусственные нейронные сети (ИНС) или смоделированные нейронные сети (СНС), представляют собой подмножество алгоритмов машинного обучения и служат основой алгоритмов глубокого обучения. Концепция «нейронных сетей» возникла в попытке смоделировать процессы, происходящие в человеческом мозгу при передаче сигналов между биологическими нейронами.

Искусственные нейронные сети (ANN) состоят из образующих слои узлов: слой входных данных, один или несколько скрытых слоев и слой выходных данных. Каждый узел (искусственный нейрон) связан с другими узлами с определенным весом и пороговым значением. Если вывод какого-либо узла превышает пороговое значение, то этот узел активируется и отправляет данные на следующий уровень сети. В противном случае данные на следующий уровень сети не передаются.

Для обучения и постепенного повышения точности нейронных сетей применяются обучающие данные. При достижении требуемой точности алгоритмы обучения превращаются в мощные инструменты для вычислений и искусственного интеллекта, что позволяет использовать их для классификации и кластеризации данных с высокой скоростью. Задачи из области распознавания речи или изображений можно выполнить за несколько минут, а не за несколько часов, как при распознавании вручную. Одной из наиболее известных нейронных сетей является алгоритм поиска Google.

Принцип работы нейронных сетей



$$1) H1_{input} = (I_1 * w_1) + (I_2 * w_2)$$

$$2) H1_{output} = f_{activation}(H1_{input})$$

Рис.1

В этом примере (рис.1) изображена часть нейронной сети, где буквами I обозначены входные нейроны, буквой H — скрытый нейрон, а буквой w — веса. Из формулы видно, что входная информация — это сумма всевозможных входных данных, умноженных на которые соответствуют им веса. В это время дадим на вход 1 и 0. Пускай w1=0.4 и w2 = 0.7 Входные данные нейрона H1 станут следующими: 1*0.4+0*0.7=0.4. Сейчас когда у нас имеется входные

данные, мы можем получить выходные данные, подставив входное значение в функцию активации (подробнее о ней далее). Сейчас, когда у нас имеется выходные данные, мы передаем их дальше. И так, мы воспроизводим для всевозможных слоев, пока не дойдем до выходного нейрона. Запустив такую сеть в первый раз мы увидим, что ответ далек от верно, потому что сеть не натренирована. Дабы усовершенствовать итоги мы будем ее тренировать. Но прежде чем узнать как это делать, давайте введем немного терминов и свойств нейронной сети.

Виды нейронных сетей

Нейронные сети можно разделить на несколько типов в зависимости от целевого назначения. Вот список наиболее распространенных типов нейронных сетей, имеющих практическое применение:

Персептрон — первая нейронная сеть, созданная Фрэнком Розентблаттом в 1958 году.

Эта статья посвящена в основном нейронным сетям с прямой связью или многослойным персептронам (MLP). Они состоят из следующих слоев: входной, один или несколько скрытых слоев и выходной. Хотя такие нейронные сети формально классифицируются как MLP, на самом деле они состоят из сигмовидных нейронов, а не персептронов, поскольку большинство реальных проблем не линейны. Данные, поступающие в эти модели, используются для обучения; они лежат в основе алгоритмов компьютерного зрения, обработки естественного языка и других нейронных сетей.

Сверточные нейронные сети (CNN) похожи на сети с прямой связью, но обычно используются для распознавания изображений, обнаружения образов и/или компьютерного зрения. Для обнаружения закономерностей на изображениях с помощью таких сетей применяются законы линейной алгебры, в частности правила перемножения матриц.

Рекуррентные нейронные сети (RNN) включают обратную связь. Эти алгоритмы обучения в основном используются на данных временных рядов для прогнозирования будущих событий, таких как курсы акций на фондовых биржах или объем продаж.

Математическое представление нейронных сетей

Под катом простое и лаконичное введение в математическое представление нейронных сетей для практиков, интересующихся теорией: от персептрона до сети с двумя скрытыми слоями.

1.Однослойная нейронная сеть (перцептрон, рис.2)

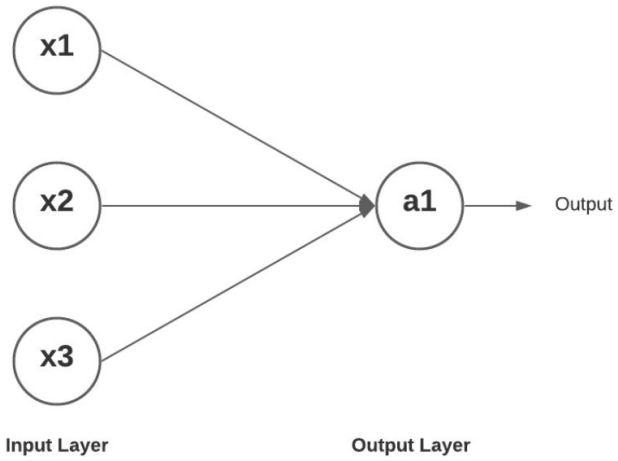


Рис.2

Вот как будет выглядеть математическое уравнение, чтобы получить значение a1 (выходной узел) как функцию входных данных x1, x2, x3.

$$a_1^{(2)} = g(\theta_{10}^{(1)} x_0 + \theta_{11}^{(1)} x_1 + \theta_{12}^{(1)} x_2 + \theta_{13}^{(1)} x_3)$$

В приведенном выше уравнении верхний индекс веса представляет слой, а нижний индекс веса представляет собой вес соединения между входными и выходными узлами. Таким образом, вес первого уровня представляет собой между узлом 1 в следующем слое и узлом 2 в текущей смене.

2. Нейронная сеть с одним открытым слоем (рис.3).

Ниже представлена нейронная сеть со скрытым слоем с тремя нейронами, входным слоем с тремя входными нейронами и выходным слоем с одним нейроном.

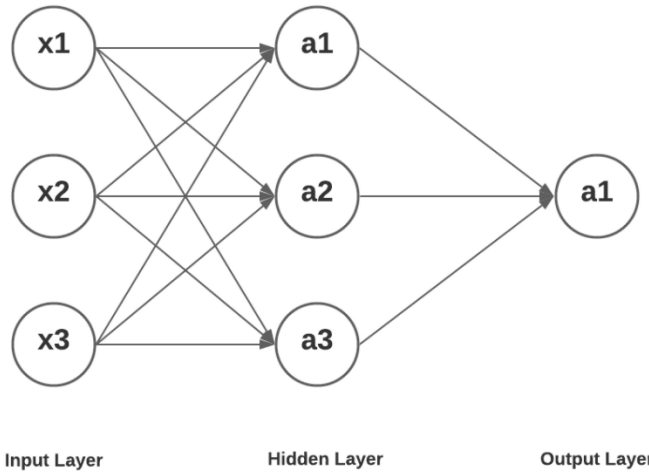


Рис.3

Вот как может выглядеть математическое уравнение (рис.4) для получения значений a1, a2 и a3 в слое 2 в зависимости от входных данных x1, x2, x3. Кроме того, значение a1 в слое 3 отображается как функция значений a1, a2 и a3 в слое 2.

Во-первых, давайте представим выходные значения, обработанные в трех скрытых нейронах скрытого слоя. Входной слой представлен как слой 1, скрытый слой — это слой 2, а выходной слой — это слой 3 (рис.5).

$$a_1^{(2)} = g(\theta_{10}^{(1)} x_0 + \theta_{11}^{(1)} x_1 + \theta_{12}^{(1)} x_2 + \theta_{13}^{(1)} x_3)$$

$$a_2^{(2)} = g(\theta_{20}^{(1)} x_0 + \theta_{21}^{(1)} x_1 + \theta_{22}^{(1)} x_2 + \theta_{23}^{(1)} x_3)$$

$$a_3^{(2)} = g(\theta_{30}^{(1)} x_0 + \theta_{31}^{(1)} x_1 + \theta_{32}^{(1)} x_2 + \theta_{33}^{(1)} x_3)$$

Рис.5

Давайте определим выходное значение узла в выходном слое. Значение представлено как функция a1, a2 и a3 в предыдущих узлах, которые могут быть представлены как значения x1, x2 и x3 во входном слое (рис.6).

$$a_1^{(3)} = g(\theta_{10}^{(2)} a_0^{(2)} + \theta_{11}^{(2)} a_1^{(2)} + \theta_{12}^{(2)} a_2^{(2)} + \theta_{13}^{(2)} a_3^{(2)})$$

Рис.6

3. Нейронная сеть с одним скрытым слоем (3 нейрона) и выходным слоем (2 нейрона)
Ниже представлена нейронная сеть со скрытым слоем с тремя нейронами, входным слоем с двумя входными нейронами и выходным слоем с двумя нейронами (рис.7).

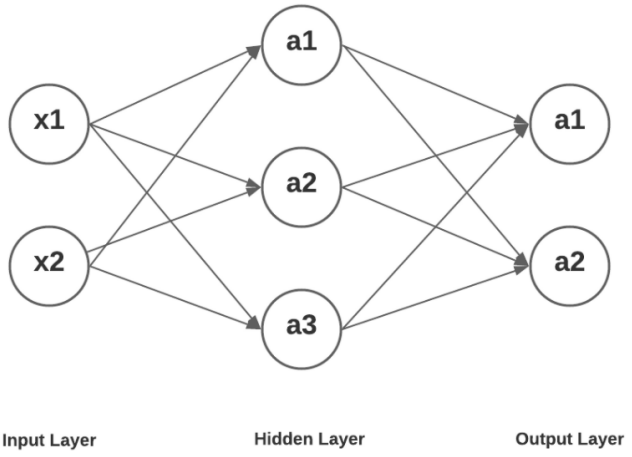


Рис.7

Вот как может выглядеть математическое уравнение для получения значения a1, a2, a3 в слое 2 как функции входных значений x1, x2. Также значение a1, a2 в слое 3 представлено как функция значений a1, a2, a3 в слое 2.
Во-первых, давайте представим выходные значения, обработанные тремя скрытыми нейронами в скрытом слое. Входной слой представлен как слой 1, скрытый слой — как слой 2, а выходной слой — как слой 3.

$$a_1^{(2)} = g(\theta_{10}^{(1)} x_0 + \theta_{11}^{(1)} x_1 + \theta_{12}^{(1)} x_2)$$

$$a_2^{(2)} = g(\theta_{20}^{(1)} x_0 + \theta_{21}^{(1)} x_1 + \theta_{22}^{(1)} x_2)$$

$$a_3^{(2)} = g(\theta_{30}^{(1)} x_0 + \theta_{31}^{(1)} x_1 + \theta_{32}^{(1)} x_2)$$

Давайте определим выходное значение узлов в выходном слое. Значение представлено в предыдущих узлах как функция a1, a2, a3, которые могут быть представлены во входном слое как значения x1, x2, x3.

$$a_1^{(3)} = g(\theta_{10}^{(2)} a_0^{(2)} + \theta_{11}^{(2)} a_1^{(2)} + \theta_{12}^{(2)} a_2^{(2)} + \theta_{13}^{(2)} a_3^{(2)})$$

$$a_2^{(3)} = g(\theta_{20}^{(2)} a_0^{(2)} + \theta_{21}^{(2)} a_1^{(2)} + \theta_{22}^{(2)} a_2^{(2)} + \theta_{23}^{(2)} a_3^{(2)})$$

4. Сети глубокого обучения с двумя скрытыми слоями.

Наконец, давайте посмотрим, как выходные значения узлов a1 в выходном слое могут быть математически выражены как функция входных данных x1, x2. Вот схема сети глубокого обучения, которая имеет два скрытых слоя, один с тремя узлами, а другой с двумя узлами. Затем есть входной слой с двумя входными узлами и выходной слой с одним выходным узлом. Вот схема упрощенной сети глубокого обучения.

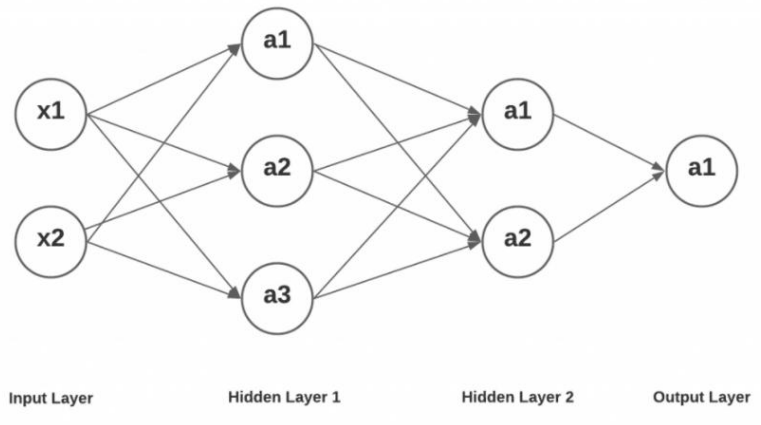


Рис.8

Значения в слое 2 (a1, a2, a3) и слое 3 (a1, a2) остаются такими же, как и в предыдущем разделе. Давайте построим значение 1 в выходном слое как функцию значений a1 и a2 в предыдущем слое (слой 3) (рис.8).

$$a_1^{(4)} = g(\theta_{10}^{(3)} a_0^{(3)} + \theta_{11}^{(3)} a_1^{(3)} + \theta_{12}^{(3)} a_2^{(3)})$$

Выводы

Современные искусственные нейронные сети — это устройства, использующие огромное количество искусственных нейронов и связей между ними. Несмотря на то, что конечная цель развития нейронных сетей — полная имитация мыслительного процесса человека — не достигнута, они уже используются для решения многих задач обработки изображений, управления роботами и непрерывного производства, для понимания речи и синтеза, для диагностики заболеваний человека и технических неисправностей в машинах и устройствах, для прогнозирования курсов валют и др. Если мы перейдем к более прозаическому уровню, нейронные сети — это просто сети, состоящие из простых частей взаимосвязанных _ формальных нейронов. В основе используемых концепций лежит идея о том, что нейроны можно моделировать довольно простыми автоматами и что вся сложность, гибкость и другие важные свойства мозга определяются связями между нейронами.

Краткое изложение о представления нейронных сетей в виде математических моделей:

1. Важно понимать обозначения, в которых вы будете представлять нейронную сеть как уравнение.
2. Первому или входному слою можно назначить номер 1, скрытому номер 2, а выходному
3. Весам между входным узлом в одном слое и узлом в следующем слое назначается верхний индекс — значение слоя, состоящего из входного узла. Нижний индекс веса состоит из двух чисел — числа, представляющего узел в следующем слое и номера входного узла.

Материал был взят на ресурсах:

1. https://habr.com/ru/post/254773/
2. Книга «Введение в системы баз данных» Криса Дж. Дейта

UDC 628.336

MATHEMATICAL REPRESENTATION OF NEURAL NETWORKS

Kolodey G.A.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Chepikova V.V – Master of Technical Sciences

Annotation. The report provides an example of the mathematical representation of neural networks and their types.

Keywords. Neural network, mathematics, types of neural networks, the principle of neural networks.

УДК 628.336

СРАВНИЕТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ УПРАВЛЕНИЯ СОДЕРЖИМЫМ ИНТЕРНЕТ-РЕСУРСА

Михно К.В.[1], студент гр.133702

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Чепикова В.В. – магистр техн. наук

Аннотация. Сравнение разных систем управления содержимым контента (CMS).

Ключевые слова. CMS,

CMS (англ. Content Management System) — это система создания и управления сайтом. Это визуально удобный интерфейс, с помощью которого можно добавлять и редактировать содержимое сайта.

Современные CMS используются крайне широко: без них сложно обойтись любой компании, которая выходит на интернет-площадки и нуждается в собственном сайте. В отличие от специализированных IT-фирм, обладающих профессиональными командами специалистов, большинство непрофильных организаций не может обеспечить себе создание ресурса с нуля и потому применяет распространенные CMS для разработки типового сайта. Это отличное решение для тех, кто нуждается в ресурсе со стандартным набором функций, будь то визитка или интернет-магазин. CMS позволяет: наполнять сайт контентом, изменять и администрировать ресурс, при этом не являясь IT-специалистом и не имея серьезных навыков программирования, создавать новые страницы в короткие сроки без лишних затрат, оптимизировать внешний вид сайта и улучшать качество его наполнения. От CMS во многом зависят функциональность ресурса, его возможности и удобство для пользователя. Правильно выбранная система позволит успешно создать и раскрутить сайт, сделав его привлекательным для клиента, надежным и работающим ровно так, как требуется[1].

CMS могут решать конкретные задачи, например, построение многостраничного интернет-магазина, лендинга, блога или форума, а могут отвечать за множество функций и предоставлять полноценную среду проектирования и программирования для разработчиков. Системы могут быть специализированными, универсальными, с внесением доработок или использованием только готовых шаблонов. Чтобы выбрать CMS, узнайте, какие есть.

Перед непосредственным созданием сайта для начала стоит изучить рынок: он предлагает множество вариантов с разными возможностями, условиями использования и ограничениями. Можно сказать, что все CMS делятся на две большие группы: открытые системы, которые распространяются бесплатно и позволяют пользователям редактировать исходный код, и проприетарные закрытые решения, которые не открывают код и, как правило, предоставляются на платной основе. Выделяют также автономные и динамические движки: первые используются для создания статичных сайтов, вторые – для интерактивных. На рынке существует несколько популярных систем: Drupal , 1С Битрикс , Joomalo , MODx , WordPress , DLE.

В зависимости от лицензии CMS бывают свободно распространяемыми и коммерческими, то есть платными и бесплатными. По типам проектов CMS делятся на универсальные и нишевые, которые подходят для одной конкретной задачи. По степени отчуждаемости они делятся на индивидуальные или студийные, коробочные и SaaS-платформы.

Коробочные — платный софт, содержащий заранее установленный набор функций для быстрого создания сайта. Такие системы имеют закрытый вид лицензии и высокий уровень безопасности. Используются крупными компаниями для проектов с большим объемом данных. Например, коробочная версия 1С-Битрикс.

Конструкторы — готовые сервисы, позволяющие создать структуру сайта при помощи шаблонов и плагинов. Функционал таких систем ограничен: не все они интегрированы друг с другом и для решения вопросов совместимости саппорту требуется время. Например, Tilda, Wix, Nethouse.

Движки для сайтов в виде онлайн-сервиса, или SaaS. Это платный софт, для начала работы в котором достаточно зарегистрироваться. Он представляет собой полноценную CMS с консолью

управления, подключенным хостингом и расширенными возможностями для настройки сайта, а для решения проблем нужно лишь обратиться в техподдержку. Например, InSales.[2]

В большинстве случаев для интернет-магазина, персонального блога или корпоративного сайта услуг подойдет и CMS с бесплатной лицензией.

На платную CMS соглашайтесь только в том случае, когда функционал бесплатных продуктов не сможет решить поставленные задачи или будет сделать дешевле на шаблоне, чем дорабатывать бесплатный движок.

Что касается самописных решений, запускать блог, сайта услуг или интернет-магазин, из-за дороговизны разработки и доработок - не рекомендую.

Самопис может подойти только в том случае, если проект будет иметь нестандартный функционал и преследовать совсем другие цели (например, дальнейшую продажу или разработку какого ни будь сервиса/портала с нестандартным функционалом). Для всех остальных задач, подойдут коробочные решения, расширенные бесплатными или платными модулями.

Что важно понимать перед выбором CMS:

1. **Сайт можно сделать на любом решении.** Главное, чтобы он выполнял нужные функции и его можно было оптимизировать под продвижение в поисковых системах с минимальными затратами на разработку и доработку.
2. **Взломать можно любой сайт.** Все будет зависеть от желания и целей это сделать. Ломают Вордпресс, 1С-Битрикс и самописные фреймворки. Это только вопрос цены, времени и желания [1].

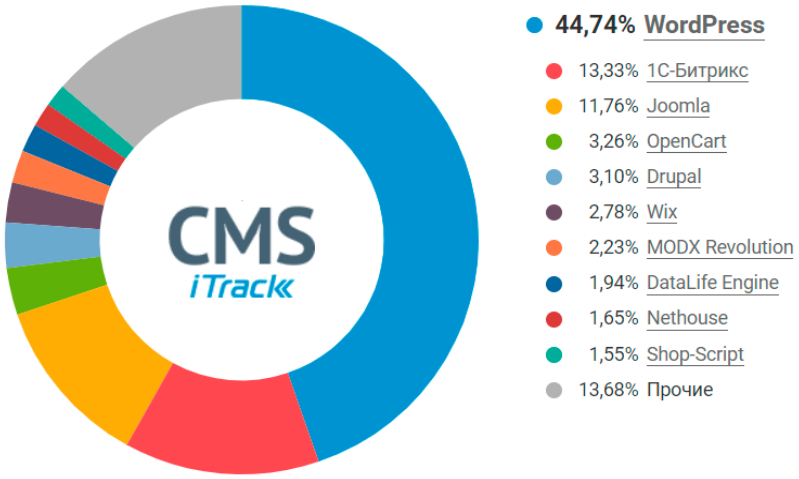


Рисунок 1 – Общий рейтинг CMS

Разбирая бесплатные движки сайтов. Мы рассмотрим два первых места.

WordPress — бесплатный движок для сайта с доступом к исходному коду и с возможностью подключения платных расширений.

Преимущества:

– Подходит для большинства хостингов — например, Bluehost;
– Большая библиотека бесплатных расширений;
– Возможность редактирования исходного кода;
– Удобный текстовый редактор;

Недостатки:

– Не подойдет для создания больших проектов: крупных интернет-магазинов с более чем 10000 товаров или корпоративных ресурсов для компаний с численностью более 1000 сотрудников
– со временем появляются проблемы со скоростью загрузки сайта;
– Большое количество установленных плагинов перегружает CMS;

– Низкий уровень безопасности системы из-за уязвимостей в расширениях;
– Некоторые плагины несовместимы между собой. Это приводит к сбою в работе платформы;
Joomla! — бесплатная CMS с гибкими настройками, для работы с которой желательно знать основы программирования и верстки — HTML и CSS. Софт поддерживает большое количество шаблонов и расширений.
Преимущества:
– Широкий функционал в базовой версии;
– Настройка достаточно простая, новичок быстро сможет разобраться в опциях;
– В системе есть возможности для SEO продвижения, вам не нужно дополнительно искать для этого плагины;
– Быстрая загрузка страниц;
– Удобный редактор страниц;
– Встроенная система отладки и отчетности об ошибках.
Недостатки:
– Необходимо отслеживать версии установленных плагинов — старые тормозят систему или полностью нарушают работу всей CMS;
– Если скачиваете расширения со сторонних ресурсов, будьте готовы к тому, что безопасность CMS и ваших данных может пострадать;
– Для настройки красивого сайта требуется покупка шаблонов или разработка собственного кода. Стандартные шаблоны на платформе однотипные;
На рисунке 2 представлен рейтинг бесплатных движков сайтов.

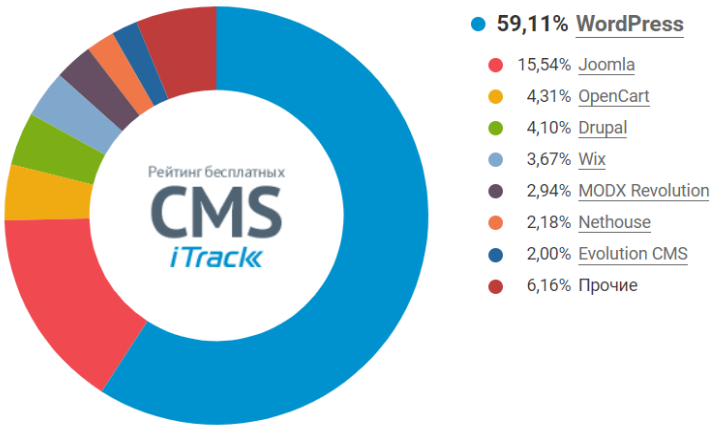


Рисунок 2 – Рейтинг бесплатных CMS

В этом разделе рассмотрим популярный варианты платных CMS, а именно 1С-Битрикс.

1С-Битрикс — коммерческая платформа для создания сайтов любого типа. Это закрытое решение для проектов, у которых большое количество данных.

Преимущества:
– Большое количество инструментов;
– Простая настройка;
– Есть возможность кастомизации;
– В маркетплейсе можно приобрести готовый сайт;
– Безопасная CMS. В системе есть облачное резервирование данных с помощью распределения
– файлов на несколько серверов, защита от DDoS-атак, а также аудит безопасности кода;
Недостатки:
– Неудобный редактор;

– Для настройки интеграции требуется программист, работающий с 1С-Битрикс, а его не так легко найти на рынке. Саппорт отвечает редко и требует дополнительную оплату за решение задач. Дорогая лицензия;
– Снижает качество изображений;
– Для SEO продвижения необходимо изучить меню администратора, так как настройки находятся в разных разделах;

Какие рекомендации могу дать, прежде чем заказывать сайт
Любой сайт всегда планируют запустить для привлечения посетителей и заработка на нем.
К сожалению, в текущих условиях конкуренции сделать ресурс и не продвигать его - выброс денег на ветер, т.к. скорее всего, запущенный новорег не даст, никакого трафика или он будет минимальный и не позволит работать бизнесу в плюс. Бывают, конечно, исключения, но в большинстве случаев, бизнес без вложений «умирает» в первые 1-2 года.
Чтобы такого не произошло, перед тем как заказать где-то разработку, рекомендую:

1. **Определиться с CMS заранее.** Подумать на перспективу, какой функционал может быть нужен в будущем, выбрать правильный шаблон и сразу начать разработку на нужной CMS с учетом внедрения нужного функционала в будущем, но на сайте его пока не реализовывать. Так получится снизить затраты на разработку, т.к. не придется переезжать еще раз на новый движок и платить повторно за разработку.
2. **Определиться будет использован шаблон или индивидуальный дизайн.** Индивидуальный дизайн — всегда дороже на порядок. Поэтому, чаще всего выбирают шаблонное решение с минимальными доработками для запуска. Со временем, если появятся инвестиции или проект «стрельнет», шаблон можно доработать или перенести на новую платформу, если нужен будет какой-то нестандартный функционал.
3. **Выделить бюджет на контекст/таргет/ретаргет.** Если трафик, нужен сразу же после запуска сайта, заложите затраты на контекст или таргет. Платный трафик обычно выходит дороже трафика из поисковых систем, но зато не придется долго ждать первых продаж.
4. **Запланировать расходы на SEO продвижение.** В зависимости от типа проекта, планируйте бюджет на 6-12 месяцев продвижения, если требуется получить органический трафик из результатов выдачи Яндекс и Google. На данный момент, это самый дешевый источник трафика, если работать в долгую. Заявки выходят от 110 рублей, в зависимости от ниши, что в 1,5-2 раза дешевле чем при использовании других каналов.
5. **Заложить расходы на доработку.** Сделанный сайт 100% будут дорабатывать под требования поисковых роботов. На чем бы он ни был сделан и кто бы его ни делал, что бы ни говорили — у всех свои методы, чек листы для продвижения + алгоритмы поисковых роботов постоянно меняются. Правки 100% будут. Поэтому, рекомендую посмотреть сводную таблицу с примерными ценами ниже. Для разных CMS, стоимость работа одного часа программиста может отличаться в разы.
6. Если бюджет сильно ограничен. Хорошим решением будет заказать сайт на конструкторе и настроить один из платных каналов трафика. Со временем, можно будет увеличить бюджет и подключить другие. Если в будущем будет нужно продвижение в поисковых системах, сайт можно будет перенести на cms[2].

В заключении хотим отметить, что выбор CMS зависит от ваших идей, желаний и возможностей для вложения в разработку.

Список использованных источников:

1. Толстенко Александр Рейтинг CMS [Электронный ресурс]. URL: Рейтинг ТОП 10 CMS сайтов: Какую лучше выбрать / Хабр (habr.com) .(Дата обращения:17.01.2022)
2. Виталий Веселов Сравнение CMS [Электронный ресурс]. URL: Сравнение CMS: анализ популярных систем управления контентом - SendPulse Blog. (Дата обращения:20.01.2021)

UDC 628.336

COMPARATIVE ANALYSIS OF CONTENT MANAGEMENT SYSTEMS OF AN INTERNET RESOURCE

Mikhno *K.V.*

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Chepikova V.V – Master of Technical Sciences

Annotation. Comparison of different content management systems (CMS).

Keywords. CMS.

УДК 628.336

ИНТЕГРАЛЬНАЯ И ДИСКРЕТНАЯ СВЕРТКИ

Ревтович П. И.

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. В данной статье рассмотрено применение свертки как основной операции в цифровой обработке сигналов, а также отмечены их основные свойства. Приведены примеры использования свертки для решения различных задач цифровой обработки. Смоделирована схема генерации дискретной свертки в приложении к пакету MATLAB Simulink.

Ключевые слова. Цифровая обработка сигналов, дискретная свертка, Simulink, схема генерации, моделирование, операции, свойства.

Введение

В век информационных технологий ключевую роль играет цифровая обработка сигналов (ЦОС), которая оказывает существенное влияние на многие технологические области: обработка изображений, распознавание речи, телекоммуникации, биомедицина, потребительские цели. Обусловлено это многими преимуществами ЦОС:
- *превосходная производительность*, позволяющая выполнять функции невозможные при аналоговой обработке;
- *гарантированная точность*, обусловленная количе- ством битов;
- *большая гибкость* — важнейшая особенность ЦОС. Возможность перепрограммирования систем без изменения оборудования;
- *совершенная воспроизводимость*, которая позволяет многократно воспроизводить и копировать цифровые записи без ухудшения качества сигнала.

На данный момент существует несколько различных алгоритмов ЦОС, для которых, впрочем, используются одни и те же операции, несмотря на различную сложность этих алгоритмов. Основными из этих операций являются: свертка, фильтрация, корреляция, модуляция и преобразования. Однако, несмотря на кажущуюся сложность цифровой обработки, все операции базируются на простых арифметических действиях — сложения, умножения, вычитания и операции сдвига.

Интегральная свертка в цифровой обработке сигналов

В теории сигналов и цифровой обработке информации важное значение имеют две теоремы: о свертке и произведении сигналов. Представить их можно в следующем виде:

$$S_{12}(t) = S_1(t) \otimes S_2(t) \leftrightarrow \dot{U}_1(f)\dot{U}_2(f)\text{,} \quad (1)$$

$$S_1(t)S_2(t) \leftrightarrow \dot{U}_1(f) \otimes \dot{U}_2(f) = \dot{U}_{12}(f)\text{.} \quad (2)$$

Знаком $\otimes$ обозначена операция интегральной свертки, а знаком $\leftrightarrow$ — отображение по Фурье.

Свертка функций — особая математическая операция, одна из наиболее часто используемых в ЦОС. Возникновение такого рода операции обусловлено физическими задачами, связанными с наблюдением объектов с помощью приборов. Свертку можно представить как результат преобразования сигнала *S(t)* в линейной системе с постоянными параметрами:

$$S_{вых}(t) = \int_{-\infty}^{\infty} S(\tau)g(t-\tau)d\tau \quad (3)$$

Большая часть всех основных функциональных преобразований сигнала сводятся к подобному интегралу, который называются интегралом свертки. Отличительной особенностью такого интеграла является то, что одна из функций должна быть обращена во времени (в нашем случае это функция *g(t)*, которая представляет собой импульсную характеристику системы). Проверить это можно, представив результат в виде суммы двух компонент:

$$S_{вых}(t) = I_1(t) + I_2(t)\text{,} \tag{4}$$

где $I_1(t)$ и $I_2(t)$ соответственно равны следующим интегралам:

, (5)

$$I_1(t) = \int_{-\infty}^{t} S(\tau)g(t-\tau)d\tau$$

. (6)

$$I_2(t) = \int_{t}^{\infty} S(\tau)g(t-\tau)d\tau$$

Компонента $I_1(t)$ показывает реакцию системы до момента времени *t* (на «прошлое» воздействие), а $I_2(t)$ — реакция системы после момента времени *t* (на «будущее» воздействие). То есть теоретически двухсторонняя импульсная характеристика возможна, кроме того, она может иметь четную или нечетную симметрию. Однако реальные системы никоим образом не могут реагировать на «будущее» поведение сигнала *S(t),* на основании чего можно сделать вывод о том, что в реальных системах точный результат свертки не достижим.

Второй же неприятной особенностью свертки является протяженность свертываемых функций, то есть, если импульсная характеристика имеет большую протяженность, то реакция на воздействие будет затянутой.

Чтобы избежать указанные проблемы, при проектировании систем используют различные методы: аппроксимацию коэффициента передачи и импульсной характеристики, ввод задержки, обратные связи. Но в таком случае схемы получаются довольно дорогими и с невысоким качеством обработки сигналов. Поэтому более предпочтительным является перевод задачи свертки из интегрального в дискретный вариант:

. (7)

$$S_{вых}(m\Delta t) = \sum_{-\infty}^{\infty} S(n\Delta t)g((m-n)\Delta t)$$

Все компоненты в данном случае представлены своими отсчетами с одинаковым интервалом времени *Δt.* Но стоит отметить, что формальный переход к дискретному варианту не снимает вышеперечисленных проблем. Для этого необходимо модифицировать исходные данные.

Переход к модифицированным исходным данным и моделирование схемы вычислителя свертки в Simulink

Представим импульсную характеристику $g_0(t)$ и коэффициент передачи $K_0(f)$ идеализированного аналогового преобразователя в усеченном виде. Причем таким образом, чтобы сохранились взаимная однозначность и характерные свойства. Модифицированные импульсная характеристика и коэффициент передачи назовем эталонными и на их основе определим параметры дискретного преобразователя. При усечении необходимо сохранить строгие симметрию и асимметрию компонент в частотной и временной областях. Для формирования эталонных характеристик используем прямоугольную стробирующую функцию. Окончательный вид эталонных характеристик:

, (8)

$$\dot{K}_Э(f) = \int_{-F}^{F} \dot{K}_0(x) W(f - x; 2T) dx$$

$$g_Э(t) = g_F(t)\Pi(t; 2T) . \quad (9)$$

Данные характеристики устанавливают общие правила модификации исходных данных. Они снимают многие проблемы при разработке реальных систем обработки сигналов.
Следующим шагом необходимо перейти к дискретному времени. Для этого зададим частоту дискретизации. Следует обеспечить два условия. Первое условие связано с минимизацией перехлеста в частотной области. Частоту дискретизации выбирают с запасом в диапазоне:

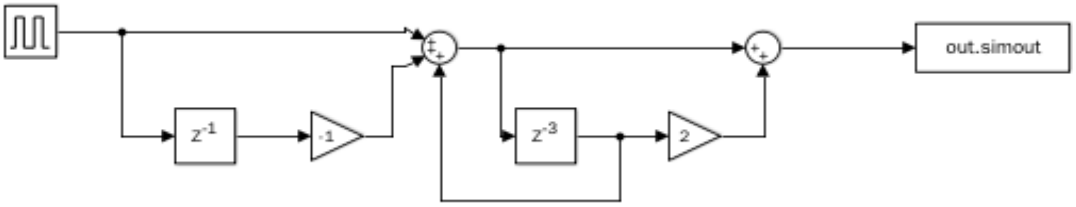


Рис. 1. Схема генерации дискретной свертки

$$f_д = (2,5)F_{\max}, F_{\max} = \max(F_s, F) , \quad (10)$$

где F_s и F — граничные частоты сигнала и преобразователя. Второе же условие связано с тем, что на отрезке $2T$ должно уложиться целое число интервалов Dt:

$$N = 2Tf_д + 1 , \quad (11)$$

где N — число отсчетов эталонной импульсной характеристики на указанном отрезке, определяющее порядок преобразователя.
Таким образом, импульсную характеристику реализуемого преобразователя должна представлять отсчеты смещенной эталонной импульсной характеристики $g(n) = g_Э(n-a), n = 0(1)N-1$. Тогда аналоговую свертку можно заменить на дискретную и реализуемую:

$$S_{вых}(m) = \sum_{n=m-N}^{m} S(n) g(m-n), \quad m = 0,1,... . \quad (12)$$

Простейшую схему вычислителя свертки (12) можно составить по системной функции, которая представляет собой Z-преобразование последовательности g(n):

$$D(z) = \sum_{n=0}^{N-1} g(n) z^{-n} . \quad (13)$$

Предположим, что системная функция явно определена и имеет вид:

$$D(z) = \frac{(1 - z^{-1})(1 + 2z^{-3})}{1 - z^2} . \quad (14)$$

Исходя из данной системной функции без проблем можно смоделировать схему генерации свертки в рекурсивном виде. Вид схемы вычислителя свертки представлен на рисунке 1.

Свойства свертки

Операция свертки обладает следующими тремя свойствами:
1. *Закон коммутативности* — независимость результата операции свертки от перестановки сигналов местами.

$$x_1(t) \otimes x_2(t) = x_2(t) \otimes x_1(t) . \quad (15)$$

2. *Закон дистрибутивности* — свертка сигнала $x_1(t)$ с суммой сигналов $x_2(t)$ и $x_3(t)$ равнозначна сумме двух сверток сигнала $x_1(t)$ с каждым из них.

$$x_1(t) \otimes \left[x_2(t) + x_3(t)\right] = x_1(t) \otimes x_2(t) + x_1(t) \otimes x_3(t) . \quad (16)$$

3. *Закон ассоциативности* — позволяет по-разному группировать операцию свертки.

$$x_1(t) \otimes \left[x_2(t) \otimes x_3(t)\right] = \left[x_1(t) \otimes x_2(t)\right] \otimes x_3(t) . \quad (17)$$

Все эти свойства можно доказать, расписав соответствующие интегралы, или же рассмотрев свертку как взаимную корреляцию одной последовательности с обращенной во времени другой.

Примеры использования

В данном разделе рассмотрим основные примеры использования свертки для различных задач.
1. БИХ- и КИХ-фильтры
Работа БИХ- и КИХ-фильтров является хорошим практическим примером свертки. Фильтры могут проектировать таким образом, чтобы они выполняли свертку последовательностей либо более общую цифровую фильтрацию. Спектр применения БИХ- и КИХ-фильтров обширен. Они могут использоваться как для обработки изображений (подавление шумов, распознавание, очистка изображений), так и для обработки речи (получение кодов PCM, субполосные кодеры).
2. *Сверточное кодирование*
Сверточные коды используются для корректировки возникающих ошибок. Это достигается путем введения в код цифр контроля четности.
3. *Обращение свертки*
Вход абсолютно всех существующих систем сворачивается с импульсной характеристикой системы и может искажать выход. В системах телекоммуникаций это приводит к необходимости использовать эквалайзер, который представляет собой линейный фильтр, восстанавливающий исходный сигнал по выходу. Для разработки эквалайзера необходимо определить импульсную характеристику системы. Такой процесс называется идентификацией системы.
4. *Речь*
Использование операции свертки в данной области обусловлено тем, что речевой сигнал можно смоделировать как свертку серии импульсов, представляющих основные тоны, активирующих импульсов и импульсной характеристики речевого тракта. Данную тройную свертку можно без проблем обратить в форму, подходящую для линейной независимой от времени системы.

Заключение

В результате проведенного исследования рассмотрена основополагающая операция цифровой обработки сигналов под названием свертка. Отмечены особенности интегральной свертки, не позволяющие ее использование в реальных системах цифровой обработки. Рассмотрен метод и необходимые параметры для перехода от интегральной свертки к дискретной и подходящей для реализации реальных систем. На основании всего вышеперечисленного представлен пример одной из возможных схем генерации дискретной свертки, смоделированный при помощи программного средства MATLAB Simulink. Также были отмечены основные свойства данной операции: ассоциативность, дистрибутивность, коммутативность.

Немаловажным пунктом является рассмотрение примеров использования свертки для совершенно различных задач цифровой обработки — от речевого синтеза до обработки изображений. Такой широкий спектр областей позволяет ощутить масштабы использования данной операции и подчеркивает необходимость ее изучения студентами технических специальностей.

Литература

1. *Солонина А.И.* Основы цифровой обработки сигналов: курс лекций. СПб.: БХВ-Петербург, 2005. 768 с.
2. *Рабинер Л., Гоулд Б.* Теория и применение цифровой обработки сигналов; пер. с англ. М.: Мир, 1978. С. 748
3. *Айфичер Э., Джервис Б.* Цифровая обработка сигналов, практический подход; пер. с англ. М.: Изд. Дом «Вильямс», 2004, 992 с.
4. *Сергиенко А.Б.* Цифровая обработка сигналов: учеб. для вузов. СПб.: Питер, 2002. 608 с.
5. *Лосев В.В.* Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки: учеб. для вузов. Минск: Выш. шк. 1990. 132 с.
6. *Солонина А.И.* Цифровая обработка сигналов и MATLAB. СПб.: БХВ-Петербург. 2013. 512 с.

УДК 621.391

ДОБРОТНОСТЬ ОЦЕНОК СПЕКТРАЛЬНОЙ ПЛОТНОСТИ МОЩНОСТИ

Корнеевец Т.А., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – канд. физ.-мат. наук

Аннотация. Оценивание спектральной плотности мощности является основной целью спектрального анализа, оно осуществляется с помощью быстрого преобразования Фурье. Существуют классические методы, которые позволяют наиболее эффективно обеспечить получение удовлетворительного результата. Но существует и ограничения в виде разрешающей способности, а также неявная весовая обработка данных.

Ключевые слова. Спектральная плотность мощности, быстрое преобразование Фурье, коррелограммная оценка, оконная функция.

Существуют классические методы оценки, которые используют БПФ. Они, в свою очередь, делятся на кореллограммные и перидограммные методы. Коррелограммными называются косвенные методы, основанные на формировании корреляционной оценки, а периодограммными – методы, основанные на прямом преобразовании данных и последующем усреднении. К перидограммным относятся следующие основные методы: метод периодограмм Шустера, метод модифицированных периодограмм, метод Бартлетта, метод Уэлча, метод Блекмена-Тьюки.

Реализация коррелограммного метода включает в себя автокорреляционную последовательность $r_{xx}[m]$ эргодического процесса как предел среднего по времени, которая определяется соотношением:

$$r_{xx} = \lim_{M\to\infty} \frac{1}{2M+1} \sum_{n=-M}^{M} x[n+m]x^*[n].$$

Для вычисления оценок дискретной автокорреляции можно применить быструю свертку, так получается оценка СПМ:

$$P_{xx}^{\wedge}(f) = T \sum_{m=-L}^{L} r_{xx}^{\wedge}[m]e^{-j2\pi fmT}, -\frac{1}{2T} \le f \le \frac{1}{2T},$$

где L – временной сдвиг [1].

Метод периодограмм Шустера обладает самой высокой разрешающей способностью, из-за неявного применения к данным прямоугольного окна, обладающего самым узким центральным лепестком, но в то же время самым высоким уровнем боковых. Оценка модифицированных периодограмм:

$$\tilde{S}_M(\bar{\omega}) = \frac{1}{NU}\left|\sum_{n=0}^{N-1} w[n]x[n]e^{-in\bar{\omega}}\right|^2, -\pi \le \bar{\omega} \le \pi,$$

где w[n] – весовая функция; x[n] – дискретные отсчеты; $\bar{\omega} = \omega T$ – безразмерная круговая частота; множитель U определяется как:

$$U = \frac{1}{L}\left|\sum_{n=0}^{L-1} w[n]\right|^2.$$

Метод Бартлетта дает состоятельную оценку энергетического спектра. Оценка периодограмм Бартлетта:

$$\tilde{S}_{\text{Б}}(\bar{\omega}) = \frac{1}{N}\sum_{i=1}^{K}\left|\sum_{n=0}^{L-1} x[iL+n]e^{-in\bar{\omega}}\right|^2, -\pi \le \bar{\omega} \le \pi,$$

где L – длина отдельного участка; K – число участков; x[i] – отсчеты входного сигнала.

Уэлч предложил две модификации метода сегментирования и усреднения Бартлетта. Первая заключалась в том, чтобы исходную запись данных следует разбить на подпоследовательности, которые перекрываются во времени. Вторая – перед вычислением периодограммы каждой из последовательностей этот сегмент обрабатывала с помощью окна данных. Оценка периодограмм Уэлча:

$$\tilde{S}_{\text{У}}(\bar{\omega}) = \frac{1}{KLU}\sum_{i=1}^{K-1}\left|\sum_{n=0}^{L-1} w[n]x[iD+n]e^{-in\bar{\omega}}\right|^2, -\pi \le \bar{\omega} \le \pi,$$

где K – число сегментов; L – длина одного сегмента; w[n] – весовая функция; x[n] – дискретные отсчеты; $\bar{\omega} = \omega T$ – безразмерная круговая частота.

Метод Блекмена-Тьюки представляет собой обобщение коррелограммного метода. В нем улучшения качества оценок путем ее свертки с подходящим спектральным окном. Оценка СПМ по методу Блекмена-Тьюки:

$$\tilde{S}_{\text{БТ}}(\bar{\omega}) = \sum_{m=-M}^{M} w[m]\bar{r}_x[m]e^{-in\bar{\omega}}, -\pi \le \bar{\omega} \le \pi,$$

где M – максимальное значение временного сдвига; w[n] – весовая функция; $\bar{r}_x[m]$ – коррелограмма входной последовательности; $\bar{\omega} = \omega T$ – безразмерная круговая частота [2].

Список использованных источников:

1. В.И. Кривошеев. Современные методы цифровой обработки сигналов (цифровой спектральный анализ) : учеб. пособие. М. : ННГУ : Наука, 2006. – 117 с.

2. В.Н. Овчарук. Спектральный анализ сигналов акустической эмиссии : учеб. пособие. М. : ТОГУ: Наука, 2013. – 13 с.

UDC 621.391

Q-factor of power spectral density estimates

Karneyavets T.A.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Daneiko T.M. – Senior Lecturer

Annotation. The estimation of the power spectral density is the main goal of spectral analysis; it is carried out using a fast Fourier transform. There are classical methods that allow you to most effectively ensure a satisfactory result. But there are also limitations in the form of resolution, as well as implicit weight processing of data.

Keywords. Spectral power density, fast Fourier transforms, correlogram estimation, window function.

УДК 621.391

СОЗДАНИЕ АВТОМАТИЗИРОВАННОГО ВЕБ-СЕРВИСА АГЕНСТВА НЕДВИЖИМОСТИ

Чайкин Н.Ю., студент группы 863102

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т. М.– ст. преподаватель каф. ИКТ

Аннотация. Работа представляет собой описание разработки автоматизированного веб-сервиса агентства недвижимости и средства для сбора данных с различных веб-сервисов агентств недвижимости, обоснование выбранных инструментов для разработки, описание самой системы в целом и описание разработанного сервиса.

Ключевые слова. Веб-сервис, клиент, сервер, база данных, архитектура «клиент-сервер», парсер, запрос, ответ.

В настоящее время существует огромное количество различных веб-сервисов агентств недвижимости, они предоставляют различный функционал: оформление договоров найма жилого помещения, размещение рекламных интеграций для увеличения продаж, отслеживание актуальной информации по объектам, поиск жилых помещений по различным фильтрам. Вся эта автоматизация экономит деньги и время конкретной риэлторской фирмы. Проблема с распределенностью данных всех веб-сервисов остаётся до сих пор актуальной поскольку каждый веб-сервис работает только для своих клиентов, что увеличивает время и сложность поиска имущества для человека. Таким образом можно выделить несколько проблем:

- отсутствие единой базы данных.
- коллизии, возникшие в результате дублирования одной и той же квартиры на нескольких веб-сервисах.

Для объединения информации в единую базу данных была разработана система, которая работает на основе cron. Cron - один из часто используемых инструментов для Unix-систем. Его используют для планирования выполнения команд на определённое время. Разработанная система функционально выполняет следующие задачи:

- автоматический сбор данных со всех источников в интервальном режиме;
- проверка наличия коллизий перед записью в базу данных, решение коллизий путем удаления дублирующихся записей;
- получение координат квартиры по ее адресу;
- форматирование информации перед записью в базу данных;

Система для сбора данных представлена на рисунке 1.

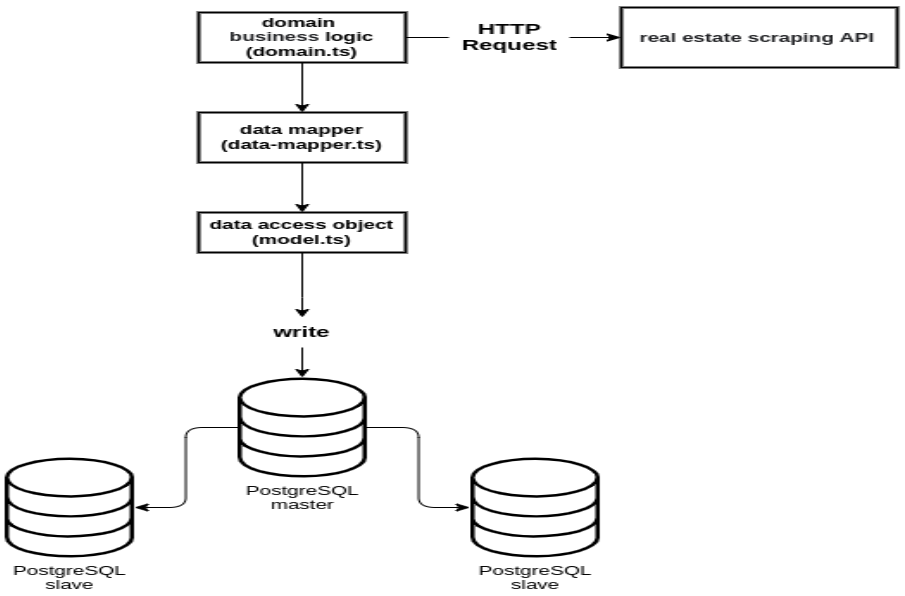


Рисунок 1 - схема системы для сбора данных

Для предоставления пользователю объединенной информации был создан веб-сервис агентства недвижимости. Созданный веб-сервис использует базу данных, в которой собрана информация с других веб-сервисов, а также функционально выполняет следующие задачи:

- поиск квартир с указанием радиуса поиска и координат на карте;
- фильтрация квартир по параметрам;
- оформление договоров найма жилого помещения;
- размещение рекламным интеграций;

Схема созданного веб-сервиса представлена на рисунке 2.

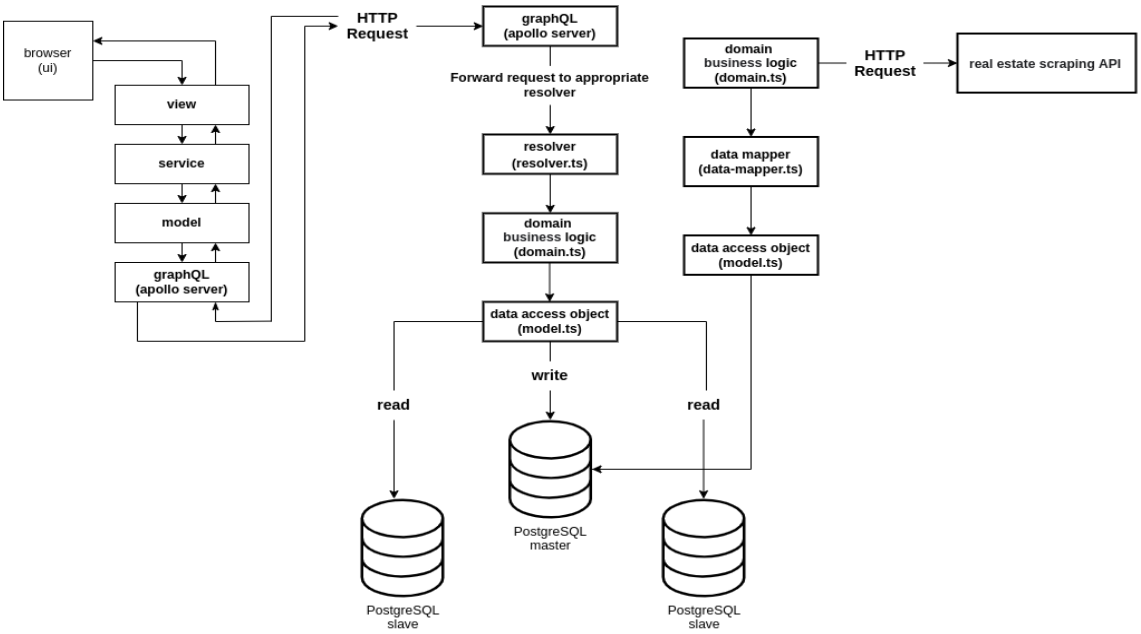


Рисунок 2 - схема автоматизированного веб-сервиса агентства недвижимости

Для написания клиентской стороны пользовательского интерфейса данного веб-сервиса была использована библиотека React от компании facebook. Данная библиотека предоставила возможность использовать такую функцию, как двустороннее связывание,

которая позволяет динамически изменять данные в одном месте интерфейса при изменении данных модели в другом. Одной из ключевых особенностей React является то, что он легко интегрируется с TypeScript [2].

Клиентская часть реализует пользовательский интерфейс, формирует запросы к серверу и обрабатывает ответы от него.

Таким образом был разработан веб-сервис агентства недвижимости соответствующий всем поставленным перед ним функциональным требованиям и нормам, были проанализированы и выбраны основные технологии и средства для разработки его клиентской и серверной частей.

Список использованных источников:

1. Kubernetes / B. Burns - https://kubernetes.io/en/docs/home/
2. Nestjs / K. Mysliwiec - https://nestjs.com/
3. Domain driven design / E. Evans, M. Fowler - https://docs.microsoft.com/en-us/dotnet/architecture/
4. Event driven design / H. Taylor
5. *Clean architecture / R. Martin*

УДК 621.391

МЕТОДИКА ПРИМЕНЕНИЯ БИЛИНЕЙНОГО Z-ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ КЛАССИЧЕСКИХ АНАЛОГОВЫХ ФИЛЬТРОВ

Довыденко Е.О., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель каф. ИКТ

Аннотация. Во многих практических ситуациях аналоговая передаточная функция *H(s)*, по которой вычисляется *H(z)*, может быть неизвестной, и ее нужно определить по спецификациям желаемых фильтров. В стандартных задачах частотно-избирательной цифровой фильтрации *H(s)* можно получить на основе классических фильтров. В данной работе описаны важные особенности классических аналоговых фильтров. Рассматриваются только фильтры-прототипы нижних частот, поскольку, фильтры других частот обычно выводятся из нормированных фильтров нижних частот

Ключевые слова. Фильтр нижних частот, фильтр верхних частот, полосовой фильтр, режекторный фильтр, билинейное z-преобразование.

1. Фильтр нижних частот

Преобразование передаточной функции в передаточную функцию фильтра нижних частот происходит по следующему закону:

$$S = \frac{s}{\omega'_p} \tag{1}$$

Если в этом выражении заменить s на iω и записать частоты фильтра-прототипа как ω^p, а частоты разрабатываемого фильтра нижних частот как $\omega_{нч}$ (что бы как то их разделять), формула(1) переходит в следующую форму:

$$i\omega^{\,p} = i\frac{\omega_{нч}}{\omega'_p}, \text{т.е. } \omega'_p = \frac{\omega_{нч}}{\omega'_p} \tag{2}$$

Уравнение (2) определяет связь между частотами фильтра-прототипа и фильтра нижних частот, который требуется разработать. Зная критичные частоты денормированного фильтра нижних частот, можно использовать формулу (2) и найти критичные частоты фильтра-прототипа, а следовательно, определить его спецификации.

Фильтр-прототип имеет три критичные частоты: 0, граничная частота полосы пропускания, граничная частота полосы подавления:

1) если $\omega_{нч}=0$, $\omega^p=0$ (из формулы (2));
2) если $\omega_{нч}=\omega'_p$ (т.е. граничной частоте полосы пропускания), $\omega^p = \frac{\omega'_p}{\omega'_p} = 1 = \omega_p^p$;
3) если $\omega_{нч}=\omega'_s$, $\omega^p = \frac{\omega'_s}{\omega'_p} = \omega_s^p$.

2. Фильтр верхних частот

Используя преобразование “Нч-фильтр в Вч-фильтр”, $S = \frac{\omega'_p}{s}$ и обозначив через $\omega_{вч}$ частоты денормированного фильтра верхних частот, а через ω^p – частоты ФНЧ-прототипа, получим следующую связь между частотами ФНЧ-прототипа и нужного фильтра верхних частот:

$$\omega^p = -\frac{\omega'_p}{\omega_{вч}} \tag{3}$$

Используя формулу (3), критичные частоты ФНЧ-прототипа можно выразить через частоты искомого фильтра верхних частот:

1) если $\omega_{вч}=0$, $\omega^p= \infty$ (используем формулу (3));
2) если $\omega_{вч}= \omega'_p$ (т.е. граничной частоте полосы пропускания), $\omega^p= 1$;
3) если $\omega_{вч}= \omega'_s$, $\omega^p = -\frac{\omega'_p}{\omega'_s}$;
4) если $\omega_{вч}= -\omega'_p$, $\omega^p= 1$;
5) если $\omega_{вч}= -\omega'_s$, $\omega^p = \frac{\omega'_p}{\omega'_s}$.

Следовательно, при разработке фильтра верхних частот тремя критичными частотами ФНЧ-прототипа являются 0,1 и $\frac{\omega'_p}{\omega'_s}$.

3. Полосовой фильтр

Преобразование “фильтр нижних частот в полосовой фильтр” записывается следующим образом:

$$s = \frac{s^2+\omega_0^2}{W_s} \tag{4}$$

Согласно этому правилу частоты полосового фильтра $\omega_{пп}$ и частоты ФНЧ-прототипа ω^p связаны следующим соотношением:

$$i\omega^p = \frac{(iw_{пп})^2+\omega_0^2}{iW\omega_{пп}}, \text{т.е. } \omega^p = \frac{\omega_{пп}^2-\omega_0^2}{W\omega_{пп}} \tag{5}$$

Полосовой фильтр имеет четыре граничные и центральную частоты:

ω'_{p1}, ω'_{p2}= верхняя и нижняя граничные частоты полосы пропускания.

ω'_{s1}, ω'_{s2}= верхняя и нижняя граничные частоты полосы поглощения.

ω_0=центральная частота ($\omega_0^2 = \omega'_{p1}\omega'_{p2}$).

Используя соотношение (5), граничные частоты ФНЧ-прототипа можно выразить через граничные частоты полосового фильтра:

1) если $\omega_{пп} = \omega'_{s1}$, $\omega^p = \omega'^p_{s1} = \frac{\omega'^2_{s1}-\omega_0^2}{W\omega'_{s1}}$;
2) если $\omega_{пп} = \omega'_{p1}$, $\omega^p = \frac{\omega'^2_{p1}-\omega_0^2}{W\omega'_{p1}} = \frac{\omega'^2_{p1}-\omega'_{p1}\omega'_{p2}}{(\omega'_{p1}-\omega'_{p2})\omega'_{p1}} = -1$;
3) если $\omega_{пп} = \omega'_{p2}$, $\omega^p = \frac{\omega'^2_{p2}-\omega_0^2}{W\omega'_{p2}} = \frac{\omega'^2_{p2}-\omega'_{p1}\omega'_{p2}}{(\omega'_{p2}-\omega'_{p1})\omega'_{p2}} = 1$;
4) если $\omega_{пп} = \omega'_{s2}$, $\omega^p = \omega'^p_{s2} = \frac{\omega'^2_{s2}-\omega_0^2}{W\omega'_{s2}}$;
5) если $\omega_{пп} = \omega'_0$, $\omega^p = \frac{\omega'^2_0-\omega_0^2}{W\omega_0^2}$;
6) если $\omega^s_p = \min(\omega'^p_{s1}, \omega'^p_{s2})$.

Следовательно. Важными критическими частотами ФНЧ-прототипа являются:0,1, $\min(\omega'^p_{s1}, |\omega'^p_{s2}|)$.

4. Режекторный фильтр

Преобразование “фильтр нижних частот в режекторный фильтр” записывается следующим образом:

$$s = \frac{W_s}{s^2+\omega_0^2} \tag{6}$$

Частота режекции $\omega_{пр}$ и частота фильтра-прототипа ω^p связаны соотношением:

$$i\omega^{p} = \frac{iW\omega_{\text{пп}}}{(iw_{\text{пп}})^2+\omega_0^2}, \text{т.е. } \omega^{p} = \frac{W\omega_{\text{пп}}}{\omega_{\text{пп}}^2-\omega_0^2} \quad (7)$$

Из соотношения (7) можно определить граничные частоты ФНЧ-прототипа по известным частотам нужного режекторного фильтра:

1) если $\omega_{\text{пр}} = \omega'_{s1}$, $\omega^{p} = \omega_s^{p(1)} = \frac{W\omega'_{s1}}{\omega_0'^2-\omega_{s1}^2}$;

2) если $\omega_{\text{пр}} = \omega'_{p1}$, $\omega^{p} = \frac{W\omega'_{p1}}{\omega_0'^2-\omega_{p1}^2} = \frac{(\omega_{p2}-\omega_{p1})\omega'_{p1}}{\omega'_{p1}\omega'_{p2}-\omega_{p1}'^2} = 1$;

3) если $\omega_{\text{пр}} = \omega'_{p2}$, $\omega^{p} = \frac{W\omega'_{p2}}{\omega_0^2-\omega_{p2}'^2} = \frac{(\omega'_{p2}-\omega'_{p1})\omega'_{p2}}{\omega'_{p1}\omega'_{p2}-\omega_{p2}'^2} = -1$;

4) если $\omega_{\text{пр}} = \omega'_{s2}$, $\omega^{p} = \omega_s^{p(2)} = \frac{W\omega'_{s2}}{\omega_0'^2-\omega_{s2}^2}$;

5) если $\omega_{\text{пр}} = \omega'_0$, $\omega^{p} = \frac{W\omega_0^2}{\omega_0^2-\omega_0^2} = \infty$.

Следовательно, существенными критическими частотами фильтра нижних частот являются: 0,1, ω^{p}_s (где $\omega^{p}_s = \min(\omega^{p(1)}_s, \omega^{p(2)}_s)$).

Из спецификации ФНЧ-прототипа можно определить порядок и передаточную функцию фильтра. Порядок режекторного фильтра равен удвоенному порядку фильтра прототипа, т.е.2N.

Список использованных источников:

1. Айфичер Э.,Джервис Б.У. Цифровая обработка сигналов: практический подход 2-е издание : Пер. с англ / Под ред. А. В. Назаренко. — М: Издательский дом “Вильямс”, 2004.
2. Сергиенко А.Б. Цифровая обработка сигналов. - СПБ.: Питер,2003.

UDC 621.391

BILINEAR Z-TRANSFORM APPLICATION TECHNIQUE BASED ON CLASSICAL ANALOG FILTERS

Dovydenko E.O.

Belarusian State University of Informatics and Radioelectronics, Minsk,Republic of Belarus

Daneiko T.M. – Senior Lecturer

Annotation. In many practical situations, the analog transfer function H(s) from which H(z) is computed may be unknown and must be determined from the specifications of the desired filters. In standard problems of frequency-selective digital filtering, H(s) can be obtained based on classical filters. This paper describes the important features of classical analog filters. Only prototype low-pass filters are considered, since other filters are usually derived from normalized low-pass filters.

Keywords. Low pass filter, high pass filter, bandpass filter, reduction filter, bilinear z-transform.

УДК 681.5

МЕТОД ОТОБРАЖЕНИЯ НУЛЕЙ И ПОЛЮСОВ S-ПЛОСКОСТИ

Жингилевич В.А., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель каф. ИКТ

Аннотация. Работа представляет собой описание метода отображения нулей и полюсов s-плоскости на z-плоскость.

Ключевые слова. Фильтр, полюса, нули, *s*- и *z*-плоскость, преобразование.

Для расчета коэффициентов конкретного БИХ-фильтра используется метод отображения нулей и полюсов подходящего аналогового фильтра с *s*- на *z*-плоскость с последующим выводом коэффициентов цифрового фильтра по нулям и полюсам на *z*-плоскости.

Процесс начинается с нормированного аналогового фильтра нижних частот *N*-го порядка типа Баттерворта, Чебышева или эллиптической. Далее находятся полюса нормированного фильтра Баттерворта:

$$s_k = e^{\pi i(2k+N-1)/2N} = \cos\left[\frac{(2k+N-1\pi)}{2N}\right] + i\sin\left[\frac{(2k+N-1\pi)}{2N}\right], \quad (1)$$

для фильтра Чебышева:

$$s_k = sh(\alpha)\cos(\beta_k) + icsh(\alpha)\sin(\beta_k), \quad (2)$$

для эллиптического фильтра каждый полюс комплексный и в общем случае имеет вид:

$$s_{l,k} = \alpha_{p,k} + i\beta_{p,k}, \quad (3)$$

где

$$\alpha = \frac{1}{N}sh^{-1}\left(\frac{1}{N}\right);\ \beta_k = \frac{(2k+N-1)\pi}{2N},\ k = 1,2,\dots,N.$$

Для фильтров Баттерворта и Чебышева нули фильтра-прототипа находятся на бесконечности, а для эллиптического они полностью мнимые.

Далее полюса и нули нормированного аналогового фильтра нижних частот преобразуются в полюса и нули фильтра нижних частот, верхних, полосового или режекторного фильтра.

Для цифрового фильтра нижних или верхних частот *N* полюсов нормированного фильтра нижних частот преобразуется следующим образом:

$$s_{l,k} = s_{1,k}/\omega_p^{`};\ s_{h,k} = \omega_p^{`}/s_{l,k}\ k = 1,2,\dots,N, \quad (4)$$

где $\omega_p^{`}$ – желаемая граничная частота полосы пропускания, $s_{l,k}$ – полюса аналогового фильтра нижних частот, а $s_{h,k}$ – полюса аналогового фильтра верхних частот.

Для классических фильтров преобразования переводят нули ФНЧ-прототипа на мнимую ось *s*-плоскости. В фильтрах Баттерворта и Чебышева нули фильтра-прототипа расположены на бесконечности. Преобразование переводит нули с бесконечности на бесконечности или с бесконечности в начало координат, как показано на рисунке 1.

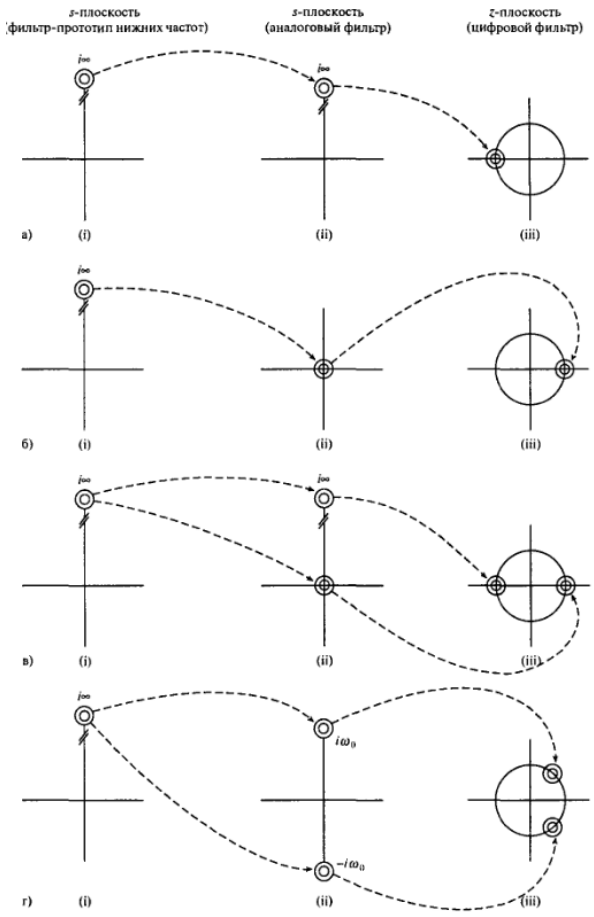


Рисунок 1 – Отображение нулей фильтра-прототипа нижних частот

Преобразования для полюсов аналогового полосового фильтра:

$$s_{b,k} = \frac{W}{1}\left[s_{l,k} \pm \left(s_{l,k}^2 - \frac{2\omega_0^2}{W^2}\right)^2\right], \tag{5}$$

где *W* – ширина полосы пропускания фильтра, ω_0^2 – определяет центральную частоту полосы пропускания.

Выражение для полюсов аналогового режекторного фильтра через полюса фильтра-прототипа:

$$s_{r,k} = \frac{W}{2}\left[s_{l,k}^{-1} \pm \left(s_{l,k}^{-2} - \frac{2\omega_0^2}{W^2}\right)^{1/2}\right] \tag{6}$$

где *W* – ширина полосы подавления фильтра, ω_0^2 – определяет центральную частоту полосы подавления.

Для фильтров Баттерворта и Чебышева преобразование «фильтр нижних частот в полосовой фильтр» отображает *N* нулей ФНЧ-прототипа с бесконечности на бесконечность и в начало координат *s*-плоскости. Преобразование «фильтр нижних частот в режекторный фильтр» переводит *N* нулей фильтра-прототипа бесконечности в точки $\pm i\omega_0$ *s*-плоскости. Для эллиптических полосовых и режекторных фильтров преобразование отображает полностью мнимые нули фильтра-прототипа в другие точки на ось $i\omega_0$.

После указанных действий применяется билинейное *z*-преобразование, переводящее полюса и нули с *s*-плоскости на цифровую *z*-плоскость. Каждый полюс *s*-плоскости $s_{p,k}$ отображается согласно следующему правилу:

$$z_{p,k} = \frac{1+s_{p,k}}{1-s_{p,k}}. \quad (7)$$

Подобным образом каждый нуль *s*-плоскости преобразованного аналогового фильтра следующим образом отображается на *z*-плоскость:

$$z_{z,k} = \frac{1+s_{z,k}}{1-s_{z,k}}. \quad (8)$$

Отображение нулей *s*-плоскости на *z*-плоскость с помощью билинейного *z*-преобразование продемонстрировано на рисунке 1. Для фильтров нижних частот нули располагаются на бесконечности *s*-плоскости, и билинейное *z*-преобразование переводит их в точку z = -1 *z*-плоскости, тогда как для полосового фильтра нули *s*-плоскости отображаются с начала координат в точку z = 1 , а с бесконечности – в точку z = -1 [1].

Список использованных источников:

1. Цифровая обработка сигналов, практический подход (II) / Айфичер Э., Джервис Б // Издательский дом «Вильямс», 2004. – С.544-548.

UDC 681.5

METHOD FOR DISPLAYING ZEROS AND POLES OF THE S-PLANE

Zhinghilevich V.A., student group 960801

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Daneiko T.M. – senior lecturer of the Department of ICT

Annotation. The work is a description of the method of mapping zeros and poles of the s-plane to the z-plane.

Keywords. Filter, poles, zeros, s- and z-plane, transformation.

УДК 004.052.32

ПРОГРАММНЫЕ СРЕДСТВА АВТОМТИЗИРОВАННОЙ КОНФИГУРАЦИИ УСТРОЙСТВ ИНТЕГРИРОВАННОГО ДОСТУПА

Ипатович А.А., магистрант гр.067041

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Давыдова Н.С.– к. т. н., доцент

Аннотация. В докладе рассмотрен способ автоматизированной конфигурации абонентских устройств интегрированного доступа с использованием программных инструментов для взаимодействия с веб-браузерами.

Разнообразие абонентских устройств интегрированнго доступа (IAD) накладывает ряд ограничений на методы автоматического конфигурирования IAD. Например, не все модели IAD поддерживают протокол Telnet для быстрой настройки и контроля основных параметров. Однако для всех моделей устройств предусмотрен веб-интерфейс, хоть и значительно отличающийся по архитектуре. Поэтому для автоматизации конфигурирования устройств интегрированного доступа используются программные средства по взаимодействию с веб-браузерами, например такие как Selenium Webdriver, Chromedriver.

Selenium Webdriver — программный инструмент для автоматизации взаимодействия с веб-браузерами. Чаще всего он используется для тестирования веб-приложений, рутинных задач администрирования, а также автоматизированного сбора информации с сайтов [1]. ChromeDriver — программный инструмент web-разработчика для браузера Google Chrome, отвечающий за управление им с помощью внешних инструментов [2].

Автором разработана система автоматизированного тестирования устройств интегрированного доступа, которая представляет собой аппаратно-программный комплекс, обеспечивающий полный автоматический цикл тестирования всех функциональных узлов IAD [3]. Система поддерживает автоматическое конфигурирование IAD через веб-интерфейс посредствам программных инструментов Selenium Webdriver и Chromedriver. При этом, Selenium используется в качестве внешней библиотеки для основного языка программирования Python.

В разработанной системе, автоматическая конфигурация устройств интегрированного доступа происходит следующим образом:

1. При обнаружении тестируемого устройства по IP-адресу (по умолчанию 192.168.1.1) происходит запуск браузера Google Crome в режиме «headless» (фоновый режим без отображения окна браузера) и переход к IAD по заданному адресу. В режиме «headless» возможно открытие нескольких вкладок и переход между ними, взаимодействие со всплывающими окнами, контроль состояния страниц (скорость загрузки, доступность и т. д.) [4]. Использование этого режима позволило значительно сократить системные требования к программному обеспечению системы автоматизированного тестирования в целом.

2. Далее происходит анализ стартовой страницы устройства. С помощью программы Selenium Webdriver производится поиск определенных элементов HTML кода страницы: форма ввода логина, пароля и т.д. При обнаружении элементов, характерных для определенной модели IAD, выбирается соответствующий сценарий дальнейшего конфигурирования. Для каждой модели устройств интегрированного доступа создан отдельный сценарий, который содержит необходимые логин и пароль для входа в режим конфигурации с правами администратора, а также заданные адреса («пути») необходимых HTML элеметнов.

3. Дальнейшее конфигурирование IAD заключается в автоматическом переходе на необходимые вкладки меню веб-интерфейса, поиск текстовых HTML элементов и их чтение, поиск и заполнение форм «input» необходимыми данными (телефонный номер, SIP сервер, IP адрес, SSID и т. д.), автоматическое подтверждение ввода данных. Все данные своевременно заносятся, либо считываются из базы данных системы автоматизированного тестирования устройств интегрированного доступа.

Для поиска и взаимодействия с необходимыми HTML элементами web-страницы выполняются команды вида:

«browser.find_element_by_xpath(«*путь к элементу в html коде*»).text» - чтение текста элемента,

«browser.find_element_by_id(«*ID элемента в html коде*»).click()» - «клик» по элементу,

«browser.find_element_by_name(«*ID элемента в html коде*»).clear()» - очистка элемента «input»,

«browser.find_element_by_name(«*ID элемента в html коде*»).send_keys(«*текст*»)» - ввод заданного текста в форму «input».

Таким образом, использование программных средств автоматизированного взаимодействия с веб-браузерами позволило создать унифицированный способ конфигурирования и контроля основных параметров IAD, что в целом повысило эффективность разработанной системы автоматизированного тестирования устройств интегрированного доступа.

Список использованных источников:

1. Selenium Webdriver [Электронный ресурс] - https://www.selenium.dev/
2. ChromeDriver [Электронный ресурс] - https://chromedriver.chromium.org/
3. Ипатович А.А. // Инфокоммуникации: 57-я научная конференция аспирантов, магистрантов и студентов. Минск. БГУИР, 2021. С. 86–88.
4. Headless Chrome [Электронный ресурс] - https://developers.google.com/web/updates/2017/04/headless-chrome

УДК 004.932.4

OBJECT DETECTION ON IMAGES BASED ON YOLOX

Gao Haoxuan., студент гр.167011 магистрант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Шевчук О.Г. – доц, кан. тех. наук

Abstract. The article presents a method of image object detection based on YOLOX. It is shown that how to use the YOLOX model for inference to complete target detection, including image preprocessing, decode outputs of model and NMS algorithm. The test results show that the method can be applied to Android system and client-server scenario.

Keywords*:* object detection, image preprocessing, model inference, NMS algorithm.

1.Introduction

Object detection is a computer vision technique that allows us to identify and locate objects in an image or video. With this kind of identification and localization, object detection can be used to count objects in a scene and determine and track their precise locations, all while accurately labeling them.

Traditional object detection relies on sophisticated manual feature design and extraction, such as Histogram of Oriented Gradient, HOG. In 2012, AlexNet based on deep convolutional neural network (CNN) won the ImageNet competition with a significant advantage. Since then, deep learning has received widespread attention. In recent years, the rapid development of deep learning techniques has led to remarkable breakthroughs. Object detection has now been widely used in many real-world applications, such as autonomous driving, robot vision, video surveillance, etc.

YOLO is an advanced single-stage object detection algorithm, which has undergone the evolution of v1~v4, and has so far developed to YOLOX that does not rely on anchor boxes. In this article, the method of image object detection based on YOLOX is proposed, mainly including image preprocessing, how to decode, and the process of executing NMS. And the test result is shown.

2. Method of image object detection based on YOLOX

The method of image object detection based on YOLOX – image preprocessing, output decoding and the strategy for choosing prediction boxes – is offered. The method can be used for images of any size, and the final target detection result can be obtained.

The flowchart of the method of image object detection based on YOLOX is provided in figure 1.

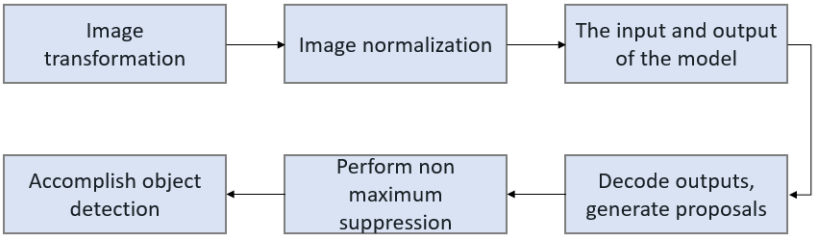


Figure 1 Flowchart of the method of image object detection based on YOLOX

1) Image transformation.

For the images of any size images, they need to be transformed to the specified size. Because the size of the input image to the YOLOX model is 640×640 pixels. Apply the affine transformation to the original image to transform its size. According to the affine transformation theory, the scaling factor scale and the transformation matrix M can be obtained:

$$scale = \min(\frac{w'}{w}, \frac{h'}{h})$$

$$M = \begin{pmatrix} \text{scale} & 0 & -\frac{scale \cdot w}{2} + \frac{w'}{2} \\ 0 & \text{scale} & -\frac{scale \cdot h}{2} + \frac{h'}{2} \end{pmatrix}$$

where w and h are the width and height of the original image, w' and h' are the width and height of the target image. Meanwhile, the matrix M^{-1} can be obtained:

$$M^{-1} = \begin{pmatrix} \frac{1}{\text{scale}} & 0 & -\frac{b1}{scale} \\ 0 & \frac{1}{\text{scale}} & -\frac{b2}{scale} \end{pmatrix}$$

$$where\ b1 = -\frac{scale \cdot w}{2} + \frac{w'}{2}, b2 = -\frac{scale \cdot h}{2} + \frac{h'}{2}$$

Through the matrix M, the original image can be transformed easily. And through the matrix M^{-1}, the transformed image can be restored, showed in Figure 2.

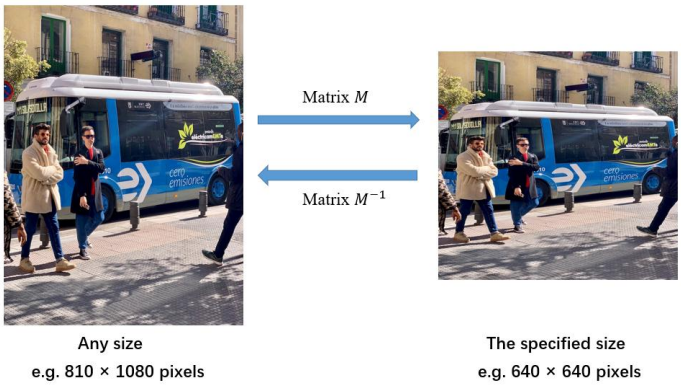


Figure 2 Image transformation

2) Image normalization.

Using the mean and std of Imagenet is a common practice. All models expect input images normalized in the same way, mini-batches of 3-channel RGB images of shape (3×H×W), where H and W are expected to be at least 224. The images have to be loaded in to a range of [0, 1] and then normalized using mean = [0.485, 0.456, 0.406] and std = [0.229, 0.224, 0.225].

3) The input and output of the model.

The original image can be converted into the input image by image transformation and image normalization. The output data of the YOLOX model is the tensor of 8400 ×85 elements, in which 8400 represents 8400 predicted boxes and 85 represents 85 the elements of the same type contained in every predicted box, shown in Figure 3.

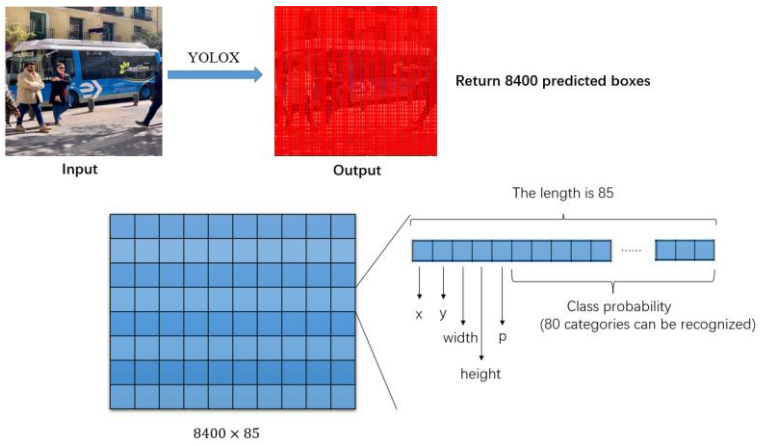


Figure 3 The output of the model

In Figure 3, the output of the model is the tensor of 8400 ×85 elements, meaning that the model predicts 8400 prediction boxes and every box has 85 properties. And x represents the abscissa of the center point of the prediction box, y represents the ordinate of the center point of the prediction box. Width represents the width of the prediction box. Height represents the height of the prediction box. P represents the probability that there is an object in the predicted box. Class probability represents the probability of being that class.

4) Decode outputs, generate proposals.

For an image, there are often only a few objects that need to be identified. However, there are 8400 boxes based on the output data. Obviously, the prediction boxes need to be further selected. In this step, it is necessary to manually set threshold to generate proposals with more accurate prediction boxes.

Before manually setting the threshold, it is necessary to know that the output 8400 prediction boxes are merged from three different sizes of anchors (shown in Figure 4). Because in the decoding process, the coordinates of the prediction boxes are related to the corresponding anchor.

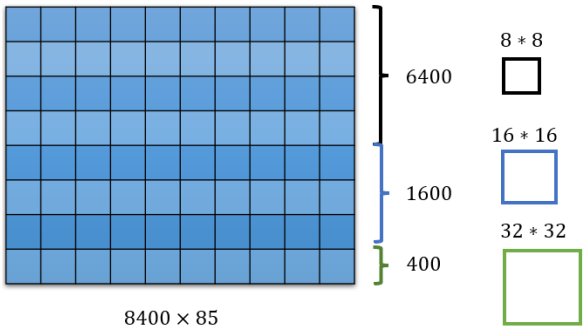


Figure 4 Three different sizes of anchors

In Figure 4, among the 8400 prediction boxes, the anchor size corresponding to 6400 prediction boxes is 8*8. This means that the original image of size 640*640 is divided into 80*80 anchors with stride of 8. Similarly, the anchor size corresponding to 1600 prediction boxes is 16*16, and the anchor size corresponding to 400 prediction boxes is 32*32.

Through the anchor, the coordinates of the prediction box can be obtained, and the probability threshold is further set manually. Here the probability threshold is set to 0.6. Then the confidence C that each prediction box has the corresponding category of objects can be given:

$$\mathrm{C} = p * \max(class\ \mathrm{probability})$$

where p represents the probability that there is an object in the predicted box. Class probability represents the probability of being that class (shown in Figure 3). Then if the confidence C is greater than 0.6, save the proposal (the coordinates of the prediction box) and the corresponding the confidence

C. After generating the proposals, the possibly correct prediction boxes will be saved, shown in Figure 5.

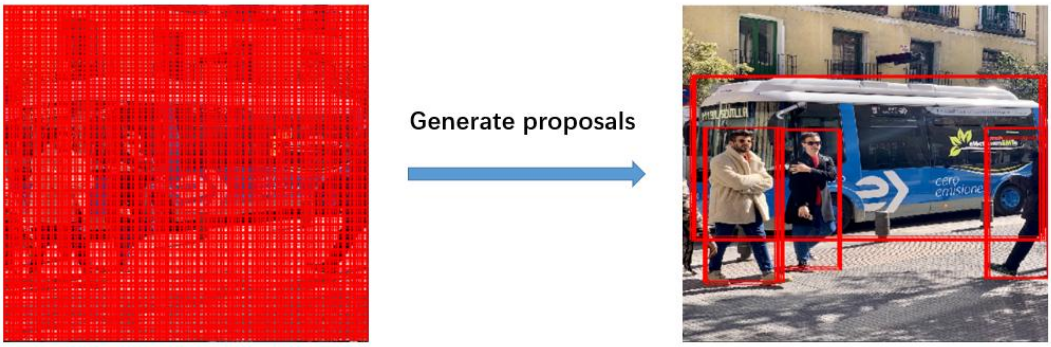


Figure 5 Generate proposals

5) Perform non maximum suppression.

The purpose of performing the algorithm is to eliminate redundant overlapping boxes with lower confidences. The algorithm steps are as follows:

Step 1: Start

Step 2: Given the proposal list, the confidence list, nms threshold that equals

0.6 and the empty list D.

Step 3: Select the proposal with highest confidence using the proposal list and the confidence list, remove it from the proposal list and add it to the list D.

Step 4: Compare this proposal with all the proposals in the proposal list, then calculate the IOU (Intersection over Union) of this proposal with every other proposal. If the IOU is greater than the nms threshold, remove that proposal from boxes.

Step 5: If there are elements in the proposal list

Go to Step 3

Step 6: End

In the end, the list D can be obtained, which contains the coordinate information of the final prediction boxes, which contains the objects to be detected, shown in Figure 6.

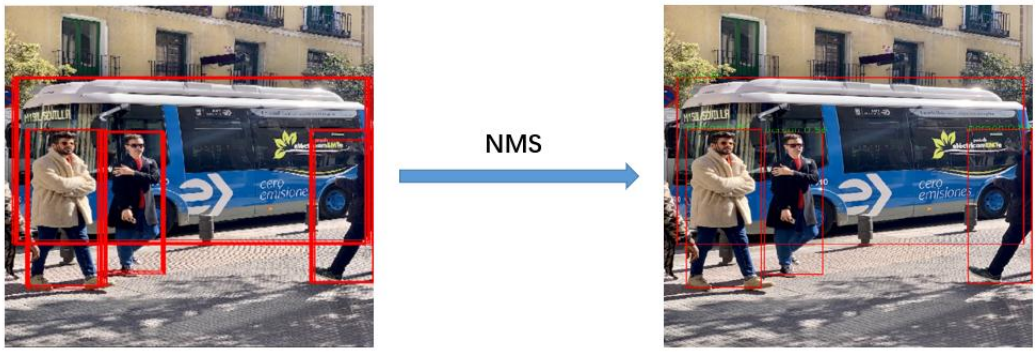


Figure 6 Perform NMS

6) Accomplish object detection

Based on the matrix M^{-1} from Image transformation (Figure 2), the coordinates of the final boxes can be converted to the coordinates in the original image. It accomplishes the object detection on the original image.

3. Test Result

The developed method is implemented in C ++ using library of OpenCV 4.5.4. The experiment was performed on a computer with the following specifications: Processor – Intel(R) Core (TM) i7-9750H CPU @ 2.60GHz 2.59 GHz; RAM – 16 GB; type of system - 64-bit operating system Windows 10.

Examples of test result are shown in Figure 7 and Figure 8.

In Figure 7, apply the method of image object detection to Android system, and the YOLOX model is also installed in Android system. Images in the file storage can be accessed and can be selected to preform object detection. And the size of image and the time of preforming object detection method are given.

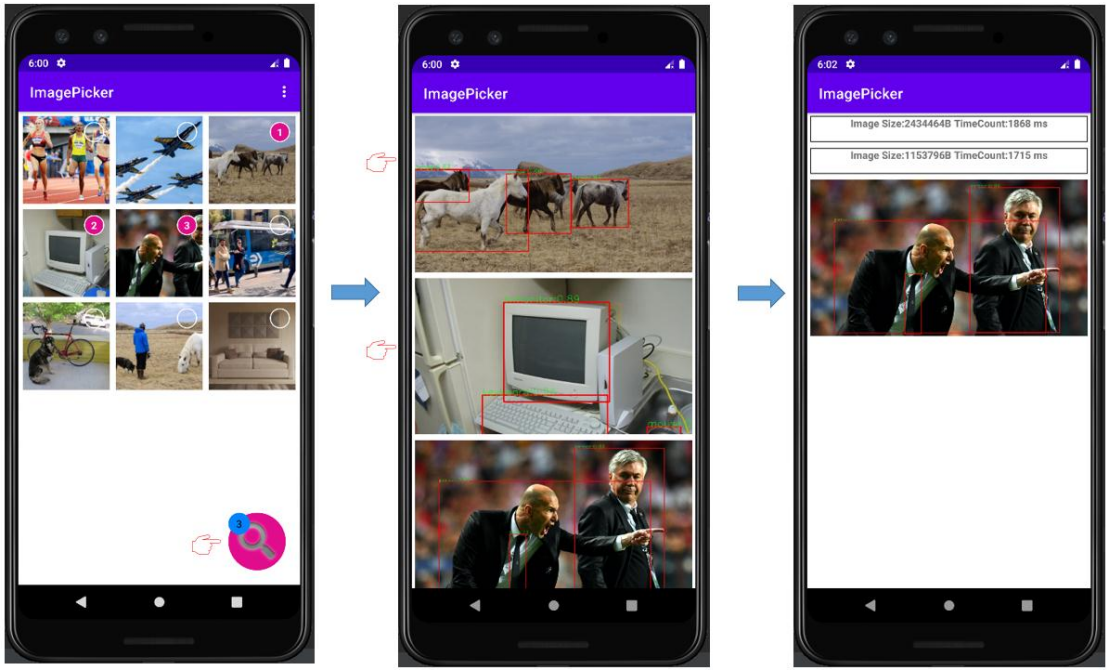


Figure 7 Test Result in Android system

In Figure 8, the test results in server-side and client-side scenario are shown. Client can select multiple images locally and upload them to the server. The server processes the request and returns the image information, the time of preforming object detection method and the result of object detection.

Figure 8 Test Result in C/S scenario

4. Conclusion

The proposed method mainly describes how to apply the YOLOX model for inference. For image preprocessing, affine transformation is applied, and image normalization is described. The problem of how to decode the output is analyzed, and the specific steps to perform NMS are given. Then the object detection on images is implemented. The test is carried out under the Android system and C/S scenarios, and the result is that the proposed method can effectively complete the object detection task.

References

1. Redmon J , Divvala S , Girshick R , et al. You Only Look Once: Unified, Real-Time Object Detection[J]. IEEE, 2016.
2. Redmon J , Farhadi A . YOLOv3: An Incremental Improvement[J]. arXiv e-prints, 2018.
3. Ge Z , Liu S , Wang F , et al. YOLOX: Exceeding YOLO Series in 2021[J]. 2021.
4. Neubeck A , Gool L . Efficient Non-Maximum Suppression[C]// International Conference on Pattern Recognition. IEEE Computer Society, 2006.
5. Stearns C C , Kannappan K . Method for 2-D affine transformation of images: US, US5475803 A[P]. 1995.

УДК 004.932.4

MATHEMATICAL SIMULATION OF DIGITAL FILTERS WITH FINITE PULSE CHARACTERISTICS

Pesetskaya A.A., Sosna I.A.

Belarusian State University of Informatics and Radioelectronics,

Minsk, Belarus

Daneiko T.M. – PhD in Physics and Mathematics

Abstract. The article discusses the methodology for optimizing the structure of decimation filters using mathematical modeling. This can significantly reduce the requirements for FPGA resources. The study of the architecture of the FIR resampling filter with a buffer is divided into stages.

A finite impulse response (FIR) digital resampling filter is a filter which impulse response (response to any finite length input) has a finite duration, since it ends to zero in a finite time.

An FIR filter can be used to implement almost every kind of frequency response in digital form and is itself implemented with help of using multipliers, adders and delay elements [1].

When implementing FIR filters in field-programmable gate arrays (FPGA), their capabilities are significantly limited by some FPGA resources. The most "deficient" resource usually turns out to be a resource, such as multipliers.

Due to the lack of multipliers, developers have to use more expensive FPGAs, reduce the filter order, and reduce the number of available digital strip values. As a result, this negatively affects the technical characteristics of the final product.

The methodology for optimizing the structure of FIR decimation filters consists in performing the following actions:

– Calculate the corresponding coefficients of the FIR filter and the order of the digital filter.

The characteristic of a classical FIR filter can be represented as:

$$y(n) = \sum_{i=0}^{n} b_i x(n - \mathrm{i}) \qquad (1)$$

where n is the order of the filter,

b_i is filter coefficient.

The block diagram of a non-recursive FIR filter is shown in Figure 1.

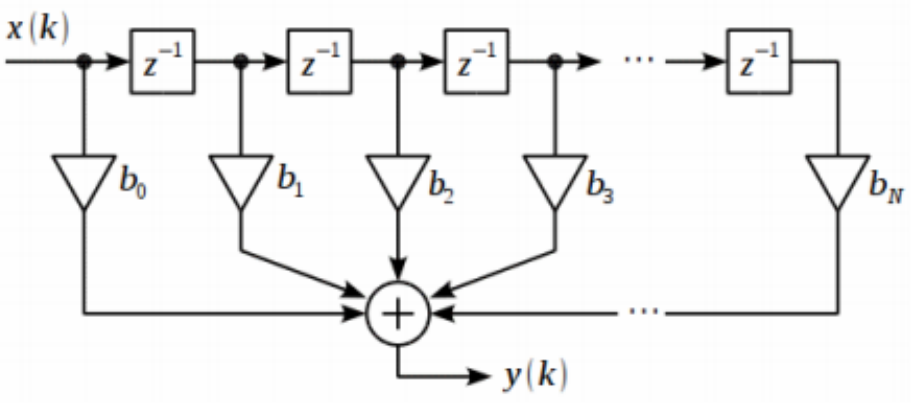


Fig. 1 – Block diagram of a non-recursive FIR filter

An order n FIR filter contains **n** delay lines and **n + 1** coefficients. If the coefficient **b0 = 1**, then we have an FIR filter of order **n**, for which multiplication by **b0 = 1** will be trivial.

The impulse response of an FIR filter is always finite and exactly matches the filter coefficients. The array of such filters allows us to implement **m** different nominal values of digital bands, where **m** is any integer.

– Estimate the need for resources (such as multipliers) for this filter array:

$$M = (n + 1) \times m \qquad (2)$$

– Consider as an alternative solution the architecture of the buffer FIR decimation filter shown in Figure 2.

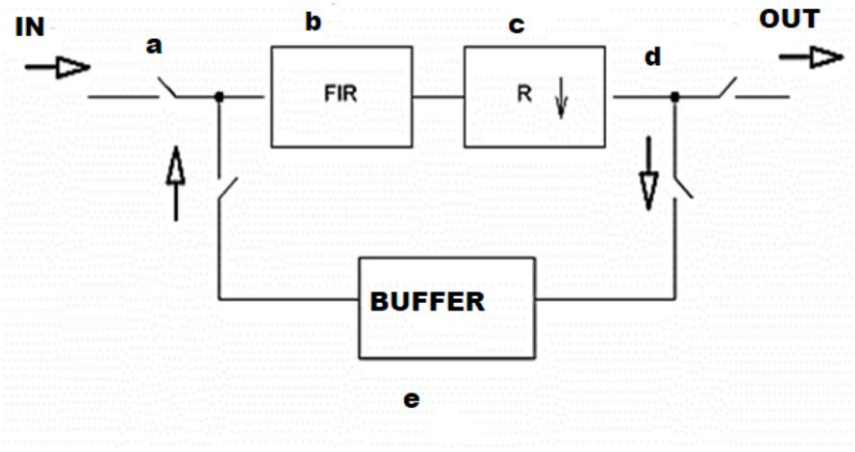


Fig. 2 – Block diagram of the buffer FIR filter:

a - input logic switch;

b - halfband FIR filter;

c - decimation block with a coefficient R = 2;

d - output logic switch;

e - buffer.

The input for this filter are samples of a digital signal, pre-converted to 0 Hz.

- Evaluate the data processing scheme with this filter.

1. Data enters the input logic switch a) and is redirected to the input of the FIR filter b), which is designed primarily to remove aliasing in the input signal during decimation.

2. After filtering, the clock frequency of the signal is halved using the decimator c).

3. After decimation, the data goes to the output switch d). If the required signal bandwidth is not reached, the data is redirected to the buffer e).

4. After being filled, the buffer returns the data block through the input switch a) for the next iteration to narrow the bandwidth.

5. Steps 2-4 are repeated until the required signal bandwidth is reached. It is obvious that for block data, that due to the cyclic structure of signal processing, it is possible to implement any decimation coefficients on one filter, if they are multiples of **2k**, where **k** = 1, 2, 3, ...

This filter allows you to process streaming (continuous) data with decimation by half and block data (data blocks with a fixed number of samples) with any decimation factor divisible by **2k**, i.e. it allows you to create unlimited digital signal bands.

For streaming data, the specified filter can be applied with a decimation factor of 2. In this case, the filter passes the data through itself once without using a buffer. The use of a filter with decimation coefficients of more than 2 is possible, but not so effective due to a significant reduction in suppression in the attenuation band.

- Consider additional possibilities for optimizing the FIR filter requirements for the number of multipliers required for its implementation in modern field-programmable gate arrays.

For the analysis, it is necessary to introduce the following restrictions into the filter structure: let us assume that every second filter coefficient is equal to zero and the filter coefficients are symmetric about the central coefficient. This filter requires only one multiplier for every four orders of magnitude for implementation, in contrast to the classical FIR filter.

- Take into account when designing the filter that a necessary and sufficient condition for the equality of every second coefficient to zero is that the filter should be half-band, or in other words, cutoff frequency (**Wpass**) and stop frequency (**Wstop**) should be symmetric about the half the sampling frequency (**Fs / 2**) [2].

The converse is also true. For a half-band filter with cutoff frequencies symmetric about the frequency **Fs / 2**, every second coefficient is equal to zero. It should be noted, however, that the cutoff and stop frequencies should be as close as possible to the half of the sampling rate as possible. Otherwise, the equality of every second sample to zero can significantly distort the filter characteristics.

- When implementing a filter buffer, it is necessary to take into account that an FIR filter is a non-recursive filter or a convolution filter. FIR filters convolve their coefficients with a sequence of input data samples, while the resulting data volume increases according to the formula:

$$\mathrm{K} = \mathrm{K}_d + \mathrm{K}_f - 1 \qquad (3)$$

where **K** is the number of elements in the output sequence;

$\mathbf{K_d}$ is the number of input data samples;

$\mathbf{K_f}$ is the number of filter coefficients.

In this case, the first $\mathbf{K_f - 1}$ samples of the output sequence are not valid.

The fact of an increase in the number of samples at the output can be explained as follows: the FIR filter is designed as a delay line, the outputs of which are multiplied by coefficients and summed up. The length of the delay line is equal to the order of the filter. Therefore, until the entire delay line is full, the output data is not valid.

In order for all output data to be valid and constant in size, the first $\mathbf{K_f - 1}$ samples must be discarded. It must be done also when data is returning to the next iteration.

One of the important properties of the filter is the linearity of its phase-frequency characteristic (PFC). The non-linear PFC of the filter distorts the signal, i.e. different frequencies acquire different phase shifts and, accordingly, different time delays at the filter output. This should be taken into account, since, for example, in coherent processing, phase distortion is unacceptable. Therefore, the more linear the PFC – the better the filter.

The proposed architecture has some restrictions on its application, namely: the filter can be effectively applied with a decimation factor of more than 2 only with block data; decimation coefficients can only be multiples of **2k**; the filter has a relatively "rigid" structure, namely, every second coefficient is equal to zero, and the coefficients must be symmetric about the central coefficient [3]. However, this structure is easily implemented by using standard mathematical modeling tools.

Thus, completing of an independent computational study for optimizing the structure of FIR decimation filters, according to the proposed method, will allow students to effectively master the material.

Sources

1. Karbushov, Ch.S. Development of an FIR filter using a distributed arithmetic architecture // Technical sciences: problems and prospects: materials of the V International scientific conference. - 2017.

2. Steven W. Smith, The Scientist and Engineer's Guideto Digital Signal Processing, Second Edition, 1999, California Technical Publishing, P.O. Box 502407, San Diego, CA 92150.

3. Theory and practice of digital signal processing [Digital resource]: Structures of digital filters and their characteristics. – Access mode: http://www.dsplib.ru/content/filters/ch10/ch10.html

УДК 621.39

КИХ-ФИЛЬТР С СИММЕТРИЧНОЙ ИМПУЛЬСНОЙ ХАРАКТЕРИСТИКОЙ

Барановская А.С., студентка гр.960801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Аннотация. Цель исследования – раскрыть особенности КИХ-фильтра с симметричной импульсной характеристикой. В статье рассматриваются КИХ-фильтры как с симметричной, так и с антисимметричной импульсной характеристикой и их различия.

Ключевые слова. Импульсная характеристика, фильтр, КИХ-фильтр, симметричная, антисимметричная, ФНЧ, фильтрация.

Цифровые фильтры могут быть двух видов – с конечной и с бесконечной импульсной характеристикой (КИХ и БИХ).

КИХ-фильтр (Конечная Импульсная Характеристика) — фильтры с конечной импульсной характеристикой. Фильтрация осуществляется посредством линейной свёртки отсчётов фильтра с отсчетами входного сигнала.

КИХ-фильтр является симметричным, только если его коэффициенты симметричны относительно центрального коэффициента. Это означает, что первый коэффициент равен последнему, второй равен предпоследнему и так далее. [1]

Для КИХ-фильтр с симметричной импульсной характеристикой необходима линейность фазочастотной характеристики(ФЧХ).

Отклик единичной выборки КИХ-фильтров симметричен или антисимметричен, если он удовлетворяет следующему условию соответственно:

Симметричен: $h(n)= h(N-1-n)$ $n=0,1,2$

Антисимметричен: $h(n)= -h(N-1-n)$ $n=0,1,2,$

где h(n) - импульсная характеристика, N – полное число отсчетов ДИХ, включая нулевой. [2]
Симметричная и антисимметричная импульсная характеристики представлены на рисунках 1 и 2 соответственно:

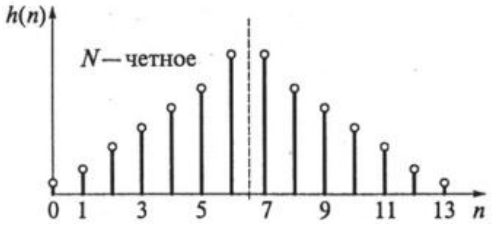


Рисунок 1 – Симметричная импульсная характеристика

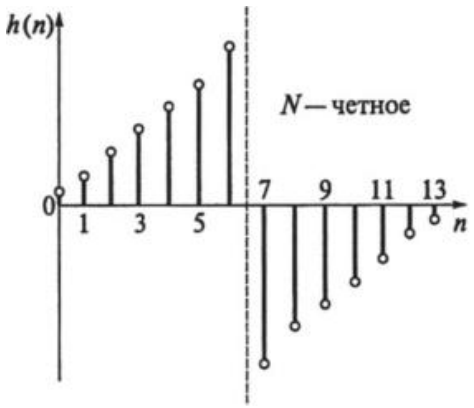


Рисунок 2 – Антисимметричная импульсная характеристика

Если g(n) = -h(N-1-n) и N нечетно, и передаточная функция H(0) = 0 он не подходит ни для фильтра нижних частот(ФНЧ), ни для фильтра высоких частот(ФВЧ). Аналогичный антисимметричный фильтр с четным N также приводит к H(0) = 0 и, следовательно, не подходит для фильтра низких частот (ФНЧ). Симметричный фильтр дает КИХ-фильтр с линейной фазой с ненулевым откликом при ω =0, поэтому подходит для ФНЧ[3]

Список использованных источников:

1. Дж. Г. Проакис, Д.Г. Манолакис Цифровая обработка сигналов: принципы, алгоритмы и приложения / Прентис Холл, 2007
2. Дж. Билмесс Обобщенные линейные фазы и типы КИХ / университет Сиэтл, 2001
3. Дж. Мэ Пак, С.К. Ан,КИХ-фильтрация для смягчения последствий/Электроника 64, 2017

UDC 621.39

FIR FILTER WITH SYMMETRIC IMPULSE RESPONSE

Baranouskaya A.S

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Baranouskaya A.S. – 960801 group student

Annotation.. The purpose of the study is to reveal the features of a FIR filter with a symmetrical impulse response. The article discusses FIR filters with both symmetric and antisymmetric impulse response and their differences.

Keywords. Impulse response, filter, FIR filter, symmetrical, anti-symmetrical, LPF, filtering.

Digital filters can be of two types - with finite and with infinite impulse response (FIR and IIR).

FIR filter (Final Impulse Response) - filters with a finite impulse response. Filtering is carried out by linear convolution of the filter samples with the input signal sample.

An FIR filter is symmetrical only if its coefficients are symmetrical about the center coefficient. This means that the first coefficient is equal to the last one, the second one is equal to the penultimate one, and so on. [1]

A FIR filter with a symmetrical impulse response requires a linear phase response (PFC).

The single-sample response of FIR filters is symmetric or antisymmetric if it satisfies the following condition, respectively:

Symmetric: h(n)= h(N-1-n) n=0,1,2

Antisymmetric: h(n)= -h(N-1-n) n=0,1,2,

where h(n) is the impulse response, N is the total number of DIR samples, including zero. [2] Symmetric and anti-symmetric impulse responses shown in Figures 1 and 2, respectively:

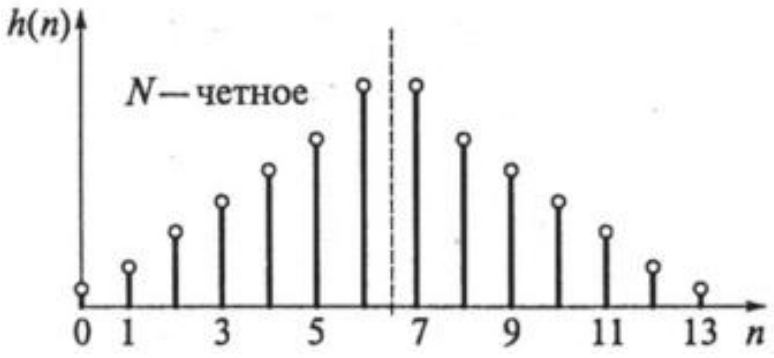


Figure 1 - Symmetrical impulse response

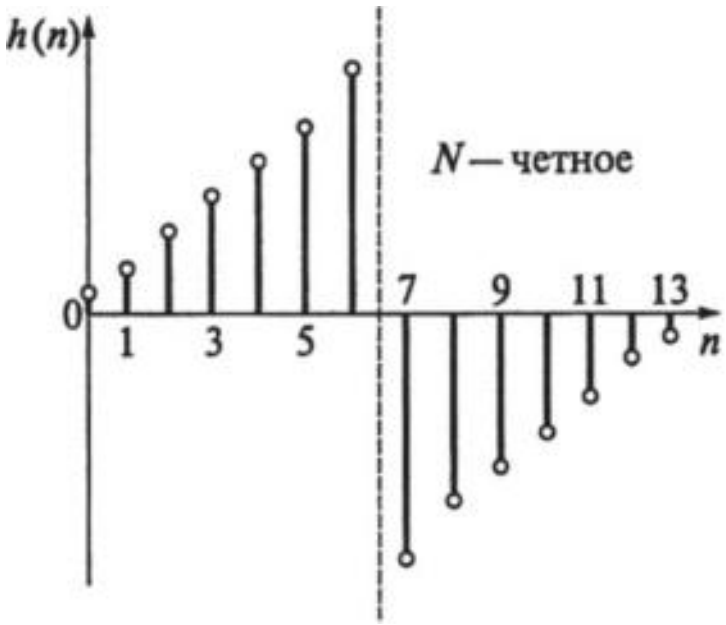


Figure 2 - Antisymmetric impulse response

If g(n) = -h(N-1-n) and N is odd and the transfer function H(0) = 0 is not suitable for either the high pass filter (LPF) or the high pass filter (HPF).A similar antisymmetric filter with even N also results in H(0) = 0 and is therefore not suitable for a low pass filter (LPF).The symmetrical filter gives a linear-phase FIR filter with a non-zero response at ω = 0, so it is suitable for a low-pass filter[3]

УДК 681.5

Частотная характеристика КИХ-фильтров с линейной фазой

Крыжевич Н.А., студент гр.960801

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель каф. ИКТ

Аннотация. Работа представляет собой описание частотной характеристики ких=фильтров с линейной фазой.

Ключевые слова. Ких-фильтр, частотная характеристика, уравнение, преобразование.

Зададим линейную ФЧХ цифрового фильтра вида:

$$\Phi(\omega) = K \cdot \omega + B\,, \tag{1}$$

где K - тангенс угла наклона ФЧХ, а $B = \Phi(0)$. Согласно определению, ФЧХ можно получить из комплексного коэффициента передачи цифрового фильтра $H\left(e^{j\cdot\omega}\right)$:

$$\Phi(\omega) = \arctan\left(\frac{\Im\left[H\left(e^{j\cdot\omega}\right)\right]}{\Re\left[H\left(e^{j\cdot\omega}\right)\right]}\right) = \ldots$$

$$\ldots = \arctan\left(\frac{-\sum_n h(n)\cdot\sin(n\cdot\omega)}{\sum_n h(n)\cdot\cos(n\cdot\omega)}\right) = K\cdot\omega + B \tag{2}$$

Групповая задержка фильтра при этом будет равна $\tau(\omega) = -K$. При отрицательном K мы получим положительную групповую задержку, что важно, так как отрицательная задержка соответствует физически нереализуемым фильтрам, когда отклик на воздействие возникает раньше самого воздействия.

Из выражения (5) можно выразить:

$$\frac{-\sum_n h(n)\cdot\sin(n\cdot\omega)}{\sum_n h(n)\cdot\cos(n\cdot\omega)} = \tan(K\cdot\omega + B) = \frac{\sin(K\cdot\omega + B)}{\cos(K\cdot\omega + B)}, \tag{3}$$

Откуда в свою очередь следует, что:

$$-\sum_n h(n)\cdot\sin(n\cdot\omega)\cdot\cos(K\cdot\omega + B) = \sum_n h(n)\cdot\cos(n\cdot\omega)\cdot\sin(K\cdot\omega + B). \tag{4}$$

Вспомним тригонометрические тождества, тогда (7) можно представить:

$$-\sum_n h(n)\cdot\frac{1}{2}\cdot\left[\sin\left((n+K)\cdot\omega+B\right)+\sin\left((n-K)\cdot\omega-B\right)\right]=\ldots$$
$$\ldots=\sum_n h(n)\cdot\frac{1}{2}\cdot\left[\sin\left((K+n)\cdot\omega+B\right)+\sin\left((K-n)\cdot\omega+B\right)\right]. \quad (5)$$

После переноса в одну сторону и упрощения выражения (8) получим:

$$\sum_n h(n)\cdot\sin\left((n+K)\cdot\omega+B\right)=0. \quad (6)$$

Таким образом выражение (6) задает уравнение, которому должна удовлетворять импульсная характеристика цифрового фильтра, чтобы фильтр имел линейную ФЧХ. Уравнение (6) должно выполняться при фиксированных K и B и для всех ω

Для вычисления нужно записать частотную характеристику КИХ-фильтров с линейной фазой в виде

$$H\left(e^{j\omega}\right)=H^*\left(e^{j\omega}\right)e^{j(\beta-\alpha\omega)} \quad (7)$$

где $H^*\left(e^{j\omega}\right)$ — действительная функция, а α и β определяются формулами (7), выразим функцию $H^*\left(e^{j\omega}\right)$ через значения коэффициентов импульсной характеристики для каждого из четырех видов фильтров с линейной фазой. Соответствующие формулы будут получены в данном разделе. Позже они будут использованы при изложении различных методов расчета КИХ- фильтров с заданными частотными характеристиками.

Фильтр вида 1. Симметричная импульсная характеристика, нечетное N . Для этого случая $H\left(e^{j\omega}\right)$ можно представить в виде

$$H\left(e^{j\omega}\right)=\sum_{n=0}^{(N-3)/2}h(n)e^{-j\omega n}+h\left(\frac{N-1}{2}\right)e^{-j\omega(N-1)/2}+\sum_{n=(N+1)/2}^{N-1}h(n)e^{-j\omega n} \quad (8)$$

Делая замену $m=N-1-n$ во второй сумме, получим

$$H\left(e^{j\omega}\right)=\sum_{n=0}^{(N-3)/2}h(n)e^{-j\omega n}+h\left(\frac{N-1}{2}\right)e^{-j\omega(N-1)/2}+\sum_{m=0}^{(N-3)/2}h(N-1-m)e^{-j\omega(N-1-m)} \quad (9)$$

Поскольку $h(n)=h(N-n-1)$, две суммы в (3.21) можно объединить, а член вынести за скобки, что дает

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}\left[\sum_{n=0}^{(N-3)/2}h(n)\left\{e^{j\omega\{(N-1)/2-n\}}+e^{-j\omega\{(N-1)/2-n\}}\right\}+h\left(\frac{N-1}{2}\right)\right] \quad (10)$$

или

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}\left\{\sum_{n=0}^{(N-3)/2}2h(n)\cos\left[\omega\left(\frac{N-1}{2}-n\right)\right]+h\left(\frac{N-1}{2}\right)\right\} \quad (11)$$

Подставив $m=(N-1)/2-n$, получим

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}\left[\sum_{n=0}^{(N-3)/2}2h\left(\frac{N-1}{2}-m\right)\cos\left(\omega m\right)+h\left(\frac{N-1}{2}\right)\right] \quad (12)$$

Окончательно при $a\left(0\right)=h\left[\left(N-1\right)/2\right]$ и $a\left(n\right)=2h\left[\left(N-1\right)/2-n\right]$, где $n=1,2,\ldots,\left(N-1\right)/2$, выражение (3.24) принимает вид

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}\left[\sum_{n=0}^{(N-1)/2}a\left(n\right)\cos\left(\omega n\right)\right] \quad (13)$$

что и дает искомую частотную характеристику. Таким образом, для фильтра вида 1

$$H^{*}\left(e^{j\omega}\right)=\sum_{n=0}^{(N-1)/2}a\left(n\right)\cos\left(\omega n\right) \quad (14)$$

Фильтр вида 2. Симметричная импульсная характеристика, четное N. В этом случае $H\left(e^{j\omega}\right)$ принимает вид

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}\left\{\sum_{n=0}^{(N-1)/2}2h\left(n\right)\cos\left[\omega\left(\frac{N}{2}-n-\frac{1}{2}\right)\right]\right\} \quad (15)$$

Подставляя в это выражение

$$b\left(n\right)=2h\left(\frac{N}{2}-n\right),\quad n=1,2,\ldots,\frac{N}{2}$$

получим

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}\left\{\sum_{n=1}^{N/2}b\left(n\right)\cos\left[\omega\left(n-\frac{1}{2}\right)\right]\right\} \quad (3.28)$$

Таким образом, для фильтра вида 2

$$H^{*}\left(e^{j\omega}\right)=\sum_{n=1}^{N/2}b\left(n\right)\cos\left[\omega\left(n-\frac{1}{2}\right)\right] \quad (3.29)$$

Необходимо отметить, что $H^{*}\left(e^{j\omega}\right)=0$ при $\omega=\pi$ независимо от значений $b\left(n\right)$ [или $h\left(n\right)$]. Отсюда следует, что нельзя использовать фильтры этого вида для аппроксимации частотной характеристики, отличной от нуля при $\omega=\pi$ (например, при проектировании фильтров верхних частот).

Фильтр вида 3. Антисимметричная импульсная характеристика, нечетное N.

В этом случае вывод формулы для $H^{*}\left(e^{j\omega}\right)$ почти такой же, как и для фильтров вида 1, за исключением того, что из-за антисимметрии $\left\{h\left(n\right)\right\}$ сумма косинусов заменяется на сумму синусов, умноженную на j, т. е. вместо формулы (3.24) следует записать

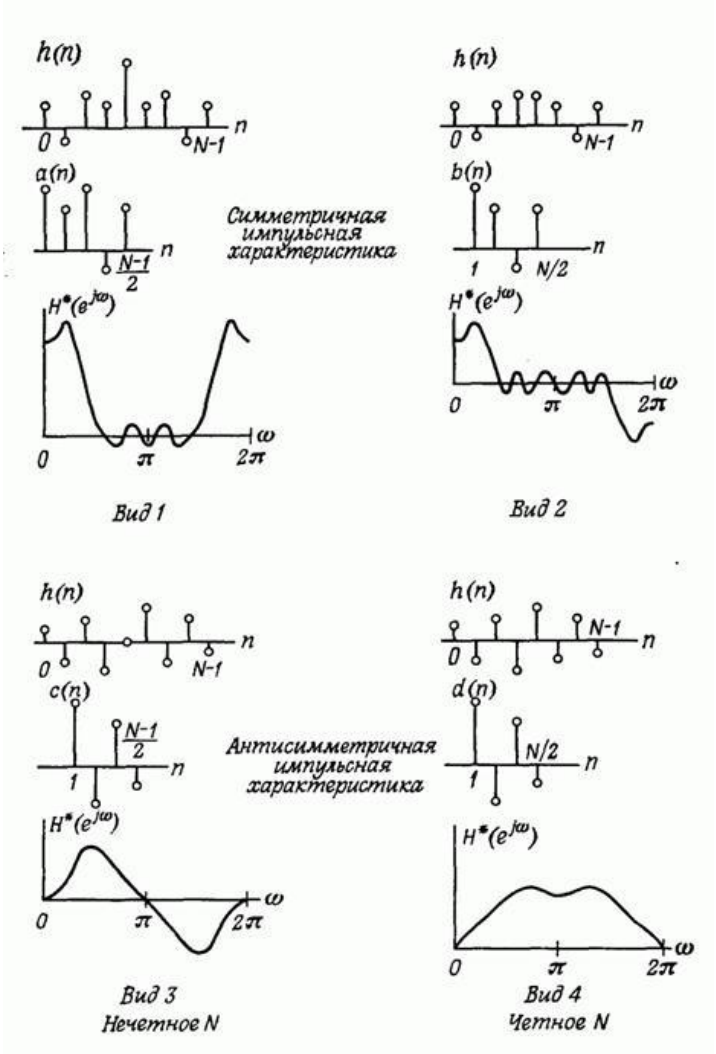
$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}e^{j\pi/2}\left[\sum_{m=0}^{N/2}2h\left(\frac{N-1}{2}-m\right)\cos\left(\omega m\right)\right] \quad (3.30)$$

где $h\left[\left(N-1\right)/2\right]=0$, как было показано выше. Делая подстановку $c\left(n\right)=2h\left[\left(N-1\right)/2-n\right]$ при $n=1,2,\ldots,\left(N-1\right)/2$, получим

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}e^{j\pi/2}\left[\sum_{n=1}^{(N-1)/2}c\left(n\right)\sin\left(\omega n\right)\right]. \quad (3.31)$$

Таким образом, для фильтра вида 3

$$H^{*}\left(e^{j\omega}\right)=\sum_{n=1}^{(N-1)/2}c\left(n\right)\sin\left(\omega n\right). \quad (3.32)$$



Фиг. 3.4. Четыре вида фильтров с линейной фазовой характеристикой.

Видно, что $H^{*}\left(e^{j\omega}\right)=0$ на частотах $\omega=0$ и $\omega=\pi$ независимо от значений $c\left(n\right)$ [или значений $h\left(n\right)$, что то же самое]. Более того, множитель $e^{j\pi/2}=j$ в формуле (3.31) показывает, что без учета множителя с линейным изменением фазы частотная характеристика

является чисто мнимой функцией. Поэтому этот вид фильтров наиболее пригоден для проектирования преобразователей Гильберта и дифференциаторов.

Фильтр вида 4. Антисимметричная импульсная характеристика, четное N .

В этом случае есть аналогия с фильтрами вида 2. Заменяя сумму косинусов суммой синусов, умноженной на j , вместо (3.27) получим

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}e^{j\pi/2}\left\{\sum_{n=0}^{N/2-1}2h\left(n\right)\sin\left[\omega\left(\frac{N}{2}-n-\frac{1}{2}\right)\right]\right\} \quad (3.33)$$

Подстановка в это выражение

$$d\left(n\right)=2h\left(\frac{N}{2}-n\right),\quad n=1,2,\ldots,\frac{N}{2}$$

дает

$$H\left(e^{j\omega}\right)=e^{-j\omega(N-1)/2}e^{j\pi/2}\left\{\sum_{n=1}^{N/2-1}d\left(n\right)\sin\left[\omega\left(n-\frac{1}{2}\right)\right]\right\}. \quad (3.34)$$

Таким образом, для фильтра вида 4

$$H^{*}\left(e^{j\omega}\right)=\sum_{n=1}^{N/2}d\left(n\right)\sin\left[\omega\left(n-\frac{1}{2}\right)\right] \quad (3.35)$$

причём $H^{*}\left(e^{j\omega}\right)=0$ при $\omega=0$. Следовательно, этот вид фильтров больше всего подходит для аппроксимации дифференциаторов и преобразователей Гильберта.

На фиг. 3.4 графически представлены все основные результаты, полученные в этом разделе, а именно типичные импульсные характеристики $h\left(n\right)$, соответствующие им сдвинутые последовательности [от $a\left(n\right)$ до $d\left(n\right)$ для каждого конкретного случая] и типичные частотные характеристики $H^{*}\left(e^{j\omega}\right)$ для каждого из четырех видов КИХ-фильтров с линейной фазой.

Список использованных источников:

1. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. М: Мир, 1978.Глава 3.5

UDC 681.5

FREQUENCY RESPONSE OF FIR FILTERS WITH LINEAR PHASE

Kryzhevich N.A., student group 960801

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Daneiko T.M. – senior lecturer of the Department of ICT

Annotation. The work is a description of the frequency response of FIR=filters with a linear phase.

Keywords. FIR filter, frequency response, equation, transformation..

УДК 628.336.42

КИХ-ФИЛЬТРОВ С ЛИНЕЙНОЙ ФЧХ

Гайтюкевич С.Д.1, студент гр.933701

Белорусский государственный университет информатики и радиоэлектроники1

г. Минск, Республика Беларусь

Данейко Т.М. – старший преподаватель кафедры ИКТ

Аннотация. В классе КИХ-фильтров можно синтезировать фильтры, обладающие заданной АЧХ и строго линейной а потому и постоянным групповым временем задержки (ГВЗ), т.е. начальные фазы всех частотных составляющих сигнала получают пропорциональный частоте сдвиг, поэтому не нарушаются их фазовые соотношения.

Ключевые слова. КИХ-фильтров, линейная ФЧХ, импульсная характеристика, групповое время задержки.

Теорема о КИХ-фильтрах с линейной ФЧХ:

Пусть имеются два многочлена

$$D(z)=\sum_{i=0}^{N_D-1} d_i z^{-i} \quad \text{и} \quad D(z^{-1})=\sum_{i=0}^{N_D-1} d_i z^{i}, \tag{1}$$

где: di — вещественные коэффициенты;

D(z) — минимально-фазовый многочлен, т. е. его нули лежат в пределах единичного круга z-плоскости.

Тогда цифровой фильтр с передаточной функцией

$$H(z)=\sum_{i=0}^{N-1} b_i z^{-i}=D(z)\pm z^{-R}D(z^{-1}) \tag{2}$$

При условии, что: $R \geq N_D-1$, имеет строго линейную ФЧХ вида

$$\varphi(\omega)=-\frac{\omega TR}{2}+(-1)^k\pi+m\frac{\pi}{2},\ k=1,2,\ldots,\ m=\{0,1\} \tag{3}$$

Следствие 1

Соотношение $\varphi(\omega)=-\frac{\omega TR}{2}+(-1)^k\pi+m\frac{\pi}{2},\ k=1,2,\ldots,\ m=\{0,1\}$ (4)

порождает два типа качественно различных ФЧХ:

$$1.\ \varphi_+(\omega T)=-\frac{\omega TR}{2}+(-1)^k\pi; \tag{5}$$

$$2.\ \varphi\_(\omega T)=-\frac{\omega T}{2}R+(-1)^k\pi+\frac{\pi}{2}.$$

Следствие 2

Скачки ФЧХ на πрадиан возможны только в полосах задерживания и переходных, где АЧХ может принимать нулевые значения.

Следствие 3

Групповое время задержки фильтра с линейной ФЧХ постоянно и равно, причем в зависимости от значения *N* (нечетное или четное) выделяются две группы фильтров: одна из них обладает

задержкой на целое число периодов дискретизации T (N нечетно), другая — на целое число периодов дискретизации T плюс полпериода дискретизации (N четно)

Следствие 4

Цифровой КИХ-фильтр обладает линейной ФЧХ с точностью до скачков на π рад на частотах, где АЧХ равна нулю, если его импульсная характеристика симметрична или антисимметрична

Следствие 5

Таблица типы КИХ-фильтров с линейной ФЧХ приведена на рисунке 1.

Длина импульсной характеристики (число коэффициентов) N	Порядок фильтра $R = N - 1$	Имцульсная характеристика	
		Симметричная	Антисимметричная
Нечетная	Четный	Тип 1, $m = 0$	Тип 3, $m = 1$
Четная	Нечетный	Тип 2, $m = 0$	Тип 4, $m = 1$

Рисунок 1. Типы КИХ-фильтров с линейной ФЧХ

Структурная схема КИХ-фильтров с линейной ФЧХ представлена на рисунке 2:

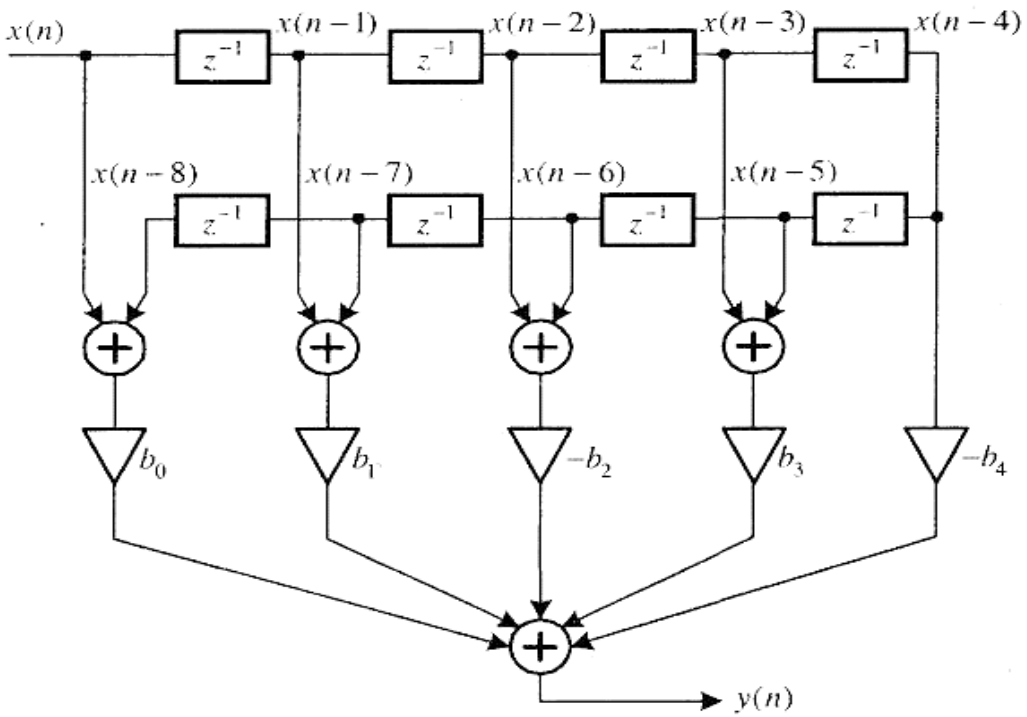


Рисунок 2. Структурная схема КИХ-фильтров с линейной ФЧХ

Список использованных источников:

1. Петровский А.А., Вашкевич М.И., Азаров И.С. Теория и применение цифровой обработки сигналов. Минск БГУИР 2016. URL: https://libeldoc.bsuir.by/bitstream/123456789/10281/2/Petrovskii_teoriya.pdf
2. Цифровые фильтры с линейной фазочастотной характеристикой. URL: http://www.dsplib.ru/content/filters/linphase/linphase.html

UDC 628.336.42

FIR FILTERS WITH LINEAR PHASE-FREQUENCY CHARACTERISTIC

Gaytyukevich S.D.1

Belarusian State University of Informatics and Radioelectronics1, Minsk, Republic of Belarus

Daneiko T.M. – senior lecturer of department of ICT

Annotation. In the class of FIR filters, it is possible to synthesize filters that have a given frequency response and a strictly linear and therefore constant group delay (GDT), i.e. the initial phases of all frequency components of the signal receive a shift proportional to the frequency, so their phase relationships are not violated.

Keywords. FIR filters, linear phase response, impulse response, group delay.

УДК 004.932.4

ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ БУФЕРА НА ОСНОВЕ СКОЛЬЗЯЩЕГО ОКНА НА CUDA

Горбуков А.Д., студент гр.067001 магистрант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Цветков В.Ю. – д-р тех. наук

Аннотация. В данной статье рассматривается алгоритм чтения изображения методом скользящего окна, оптимизированный для использования на видеопроцессорах CUDA. Алгоритм написан на языке CUDA, который является расширением языка C++. Он позволяет эффективно читать последовательнее блоки изображений, отличающиеся только одной строкой.

Ключевые слова. Цифровая обработка изображений, разделяемая память, видеокарта видеопроцессор, CUDA, Nvidia.

Алгоритм используется как часть системы цифровой стабилизации видео, написанной мной и описанной в моей статье [1].

Цель создания алгоритма состоит в том, чтобы за счет использования разделяемой памяти оптимизировать обработку областей изображения за счет оптимизации чтения из более медленной оперативной памяти. Разделяемая память в архитектуре CUDA представляет собой управляемый пользователем L1 кэш, что обеспечивает очень высокую скорость работы с ней. Быстрее в используемой архитектуре только регистры процессора.

Буфер состоит из строк, непрерывно выделенных в разделяемой памяти. Каждая строка является полем данных в ячейке очереди. Каждая ячейка хранит в себе саму строку и указатель на следующую ячейку. Отдельно хранится указатель на первую строку.

Алгоритм чтения использует тот факт, что архитектура CUDA позволяет одновременно всему пучку произвести чтение из оперативной памяти в разделяемую. На каждом шаге мы можем считать дополнительную строку в наш буфер за один такт, перезаписывая самую первую строку. При этом очередь позволяет сохранять последовательность доступа к остальным ячейкам. Теперь остается только перезаписать указатель бывшей последней строки и указатель на первую строку. Таким образом в нашей памяти всегда есть буфер части изображения, с которым мы можем в дальнейшем работать. Каждый блок может иметь у себя свой собственный буфер.

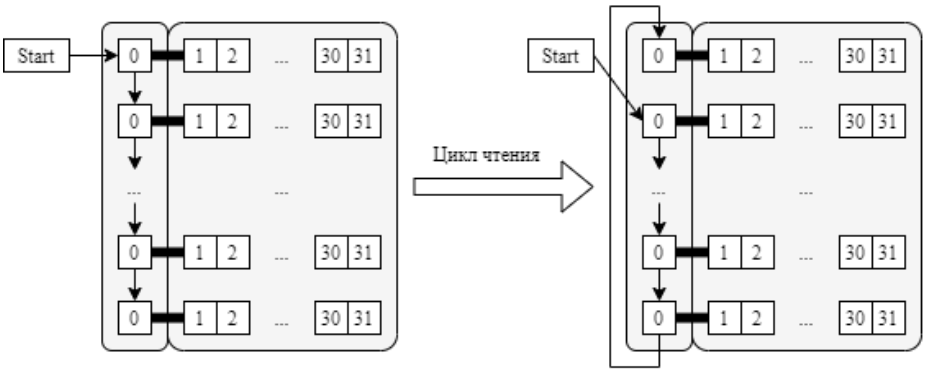


Рисунок 1 – Схема цикла чтения

Размер самого буфера, который потом можно будет передать для дальнейшей обработки ограничен размером доступной разделяемой памяти для каждого потока и пучка. Например, для одноплатного компьютера Jetson Nano количество доступной разделяемой памяти 49152 байт на поток, а размер пучка 32, что значит возможность одновременной обработки 32 ячеек памяти.

Таким образом можно держать в памяти максимальный буфер в 31 столбца и 1536 строки. В остальном это довольно эффективный способ параллельного чтения блоков изображения.

Список использованных источников:

1. Горбуков, А. Д. Система электронной стабилизации видеоизображения на базе встраиваемого одноплатного компьютера JETSON / Горбуков А. Д. // Инфокоммуникации: сборник тезисов докладов 56-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18 – 20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГУИР, 2020. – С. 69 – 70.

УДК 004.932.4

СОЗДАНИЕ СТЕНДА ДЛЯ ИЗМЕРЕНИЯ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ АСИНХРОННОГО ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ

Сороговец Е.В.[1], студент гр.067001 магистрант

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Шевчук О.Г. – канд. физ.-мат. наук

Аннотация. В данной работе представлен стенд, созданный для измерения эффективности алгоритмов асинхронного параллельного программирования.

Ключевые слова. Акторная модель, асинхронность, параллельность, C#, F#, Swagger, REST API.

Была поставлена цель реализовать систему анализа эффективности алгоритмов асинхронного параллельного программирования.

Стенд представляет собой Web API, выполненное на языках семейства Microsoft – C# и F#. Пользоваться данным стендом можно из браузера, посредством авто генерируемого из кода пользовательского интерфейса.

Стенд состоит из двух главных частей. Первая часть отвечает непосредственно за алгоритмы и вычислительную часть, вторая же предназначена для формирования графиков из полученных значений, на рисунке 1.

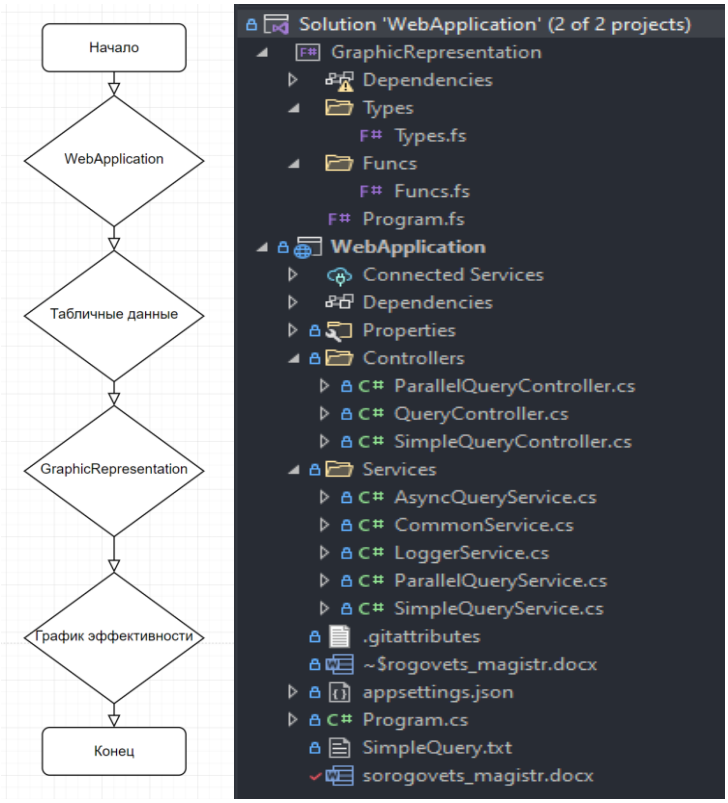


Рисунок 1 – Структурная и программная схема стенда

Стенд принимает на вход заданную от оператора сложность расчёта, а на выходе отдаёт таблицу времени выполнения по заданной сложности.

Для использования стенда достаточно сначала сгенерировать необходимый набор данных посредством нажатия соответствующей кнопки в разделах Query, SimpleQuery, ParallelQuery, на рисунке 2.

Рисунок 2 – Общий вид стенда

Стенд реализован как REST API сервис, благодаря чему является кроссплатформенным и удобным для проведения аналитики.

Ниже представлена таблица времени выполнения от сложности задачи для различных методов. Таблица времени от сложности для всех методов.

Таблица 1 – Время выполнения от сложности задачи

Мера сложности алгоритма	Синхронный	Параллельный	Асинхронный однопоточный	Акторный однопоточный
10	~0	~0	~0	~0
100	~0	~0	~0	~0
1000	~0	~0	5	~0
10000	2	~0	55	~0
500000	185	24	444	165
1000000	458	51	964	421

По полученным данным можно сделать вывод, что действительно существуют сценарии, в которых использование акторной системы оправданно, так как она может предоставить возможность единовременного исполнения большого количества одинаковых функций, за счёт горизонтального роста нагрузки на акторную систему.

Из табличных данных на входе, на выходе стенд предоставляет график, использующийся для анализа, пример на рисунке 2.

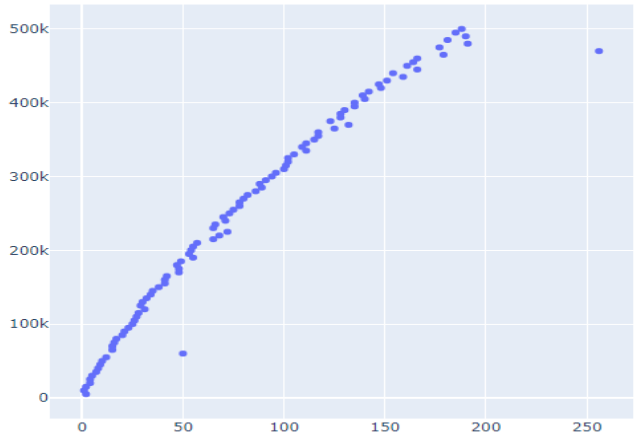


Рисунок 3 – График, построенный стендом

Был успешно создан тестовый стенд, демонстрирующий разницу между алгоритмами асинхронного и параллельного программирования.

С его помощью можно получать значения эффективности в виде таблиц либо графиков, получаемых из генерируемых в процессе выполнения файлов.

Стенд полностью отвечает всем поставленным требованиям и позволяет изменять сложность вычисления для алгоритмов, благодаря чему становится возможным увидеть разницу в скорости и потреблении памяти алгоритмом в условиях разной загруженности.

Список использованных источников:

1. Бессмертный, И. А. Системы искусственного интеллекта : учеб. пособие для СПО / И. А. Бессмертный. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 130 с.
2. Гниденко, И. Г. Технология разработки программного обеспечения : учеб. пособие для СПО / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — М. : Издательство Юрайт, 2017. — 235 с.
3. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2 : учебник для вузов / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 501 с.
4. Жмудь, В. А. Моделирование замкнутых систем автоматического управления : учеб. пособие для академического бакалавриата / В. А. Жмудь. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 128 с.
5. Зыков, С. В. Программирование. Объектно-ориентированный подход : учебник и практикум для академического бакалавриата / С. В. Зыков. — М. : Издательство Юрайт, 2019. — 155 с.
6. Иванов, В. М. Интеллектуальные системы : учеб. пособие для СПО / В. М. Иванов ; под науч. ред. А. Н. Сесекина. — М. : Издательство Юрайт, 2019. — 93 с.
7. Кубенский, А. А. Функциональное программирование : учебник и практикум для академического бакалавриата / А. А. Кубенский. — М. : Издательство Юрайт, 2019. — 348 с.
8. Кудрина, Е. В. Основы алгоритмизации и программирования на языке c# : учеб. пособие для СПО / Е. В. Кудрина, М. В. Огнева. — М. : Издательство Юрайт, 2019. — 322 с.
9. Кудрина, Е. В. Основы алгоритмизации и программирования на языке c# : учеб. пособие для бакалавриата и специалитета / Е. В. Кудрина, М. В. Огнева. — М. : Издательство Юрайт, 2019. — 322 с.
10. Кудрявцев, К. Я. Методы оптимизации : учеб. пособие для вузов / К. Я. Кудрявцев, А. М. Прудников. — 2-е изд. — М. : Издательство Юрайт, 2019. — 140 с.
11. Лаврищева, Е. М. Программная инженерия и технологии программирования сложных систем : учебник для вузов / Е. М. Лаврищева. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 432 с.
12. Лебедев, В. М. Программирование на vba в ms excel : учеб. пособие для академического бакалавриата / В. М. Лебедев. — М. : Издательство Юрайт, 2019. — 272 с.
13. Малявко, А. А. Формальные языки и компиляторы : учеб. пособие для вузов / А. А. Малявко. — М. : Издательство Юрайт, 2018. — 429 с
14. Мамонова, Т. Е. Информационные технологии. Лабораторный практикум : учеб. пособие для СПО / Т. Е. Мамонова. — М. : Издательство Юрайт, 2019. — 178 с.

UDC 004.932.4

CREATING A STAND FOR MEASURING THE EFFICIENCY OF ASYNCHRONOUS PARALLEL PROGRAMMING ALGORITHMS

Sorogovets E.V., student gr.067001

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Shevchuk O. - PhD in Physics and Mathematics

Annotation. This paper presents a bench designed to measure the effectiveness of asynchronous parallel programming algorithms.

Keywords. Actor model, asynchrony, parallelism, C#, F#, Swagger, REST API.

УДК 004.932.4

ПРЕИМУЩЕСТВА АКТОРНОЙ МОДЕЛИ АСИНХРОННОГО ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ

Сороговец Е.В.[1], студент гр.067001 магистрант

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Шевчук О.Г. – канд. физ.-мат. наук

Аннотация. В данной работе представлены преимущества акторной модели асинхронного параллельного программирования в сравнении со стандартными асинхронно-параллельными исполнениями.

Ключевые слова. Акторная модель, асинхронность, параллельность.

Модель акторов — математическая модель параллельных вычислений, строящаяся вокруг понятия актора считающегося универсальным примитивом параллельного исполнения. Актор в данной модели взаимодействует путём обмена сообщениями с другими акторами, и каждый в ответ на получаемые сообщения может принимать локальные решения, создавать новые акторы, посылать свои сообщения, устанавливать, как следует реагировать на последующие сообщения. Создана как теоретическая база для ряда практических реализаций параллельных систем.

По аналогии с философией объектно-ориентированного программирования, где каждый примитив рассматривается как объект, модель акторов выделяет в качестве универсальной сущности понятие «актора». Актор является вычислительной сущностью, которая в ответ на полученное сообщение может одновременно:

– отправить конечное число сообщений другим акторам;
– создать конечное число новых акторов;
– выбрать поведение, которое будет использоваться при обработке следующего полученного сообщения.

Не предполагается существования определённой последовательности вышеописанных действий и все они могут выполняться параллельно.

Данный алгоритм, за счёт распределения посредством менеджера акторов и взаимодействием между акторами посредством сообщений является самым затратным по ресурсам, но в тоже время самым универсальным и производительным, схема на рисунке 1.

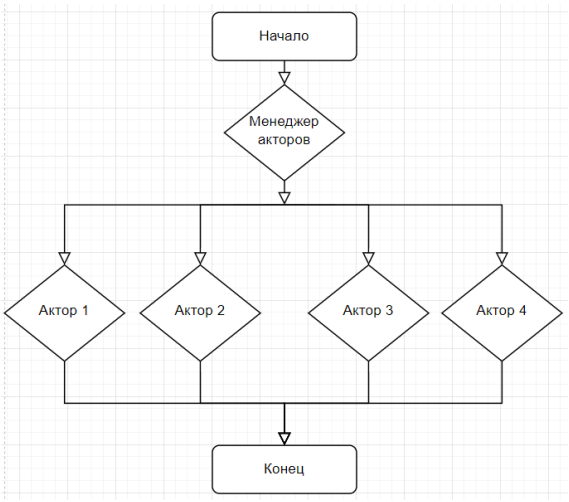


Рисунок 1 – Структурная схема выполнения акторного алгоритма

В некоторых случаях задача может потребоваться выполнить поэтапно, и задача на каждом этапе должна быть завершена до того, как задача будет создана на следующих этапах. Модель «ведущий-ведомый» может быть обобщена на иерархическую или многоуровневую модель «ведущий-ведомый», в которой мастер верхнего уровня передает большую часть задач ведущему устройству второго уровня, который дополнительно подразделяет задачи между своими собственными ведомыми устройствами и может выполнять часть самой задачи.

Ниже представлена таблица времени выполнения от сложности задачи для различных методов. Таблица времени от сложности для всех методов.

Таблица 1 – Время выполнения от сложности задачи

Мера сложности алгоритма	Синхронный	Параллельный	Асинхронный однопоточный	Акторный однопоточный
10	~0	~0	~0	~0
100	~0	~0	~0	~0
1000	~0	~0	5	~0
10000	2	~0	55	~0
500000	185	24	444	165
1000000	458	51	964	421

По полученным данным можно сделать вывод, что действительно существуют сценарии, в которых использование акторной системы оправданно, так как она может предоставить возможность единовременного исполнения большого количества одинаковых функций, за счёт горизонтального роста нагрузки на акторную систему.

Однако из-за некоторой сложности построения системы в акторной модели данный подход может оказаться неэффективным с точки зрения затрат часов рабочего времени, так как более стандартный подход асинхронного параллельного программирования даст примерно те же результаты в скорости выполнения и затратах на оперативную память, однако будет куда проще в написании кода.

Таким образом можно сделать вывод что данная модель актуальна для высоконагруженных систем, которым может потребоваться горизонтальное либо вертикальное расширение.

Список использованных источников:

1. Бессмертный, И. А. Системы искусственного интеллекта : учеб. пособие для СПО / И. А. Бессмертный. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 130 с.
2. Гниденко, И. Г. Технология разработки программного обеспечения : учеб. пособие для СПО / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — М. : Издательство Юрайт, 2017. — 235 с.
3. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2 : учебник для вузов / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 501 с.
4. Жмудь, В. А. Моделирование замкнутых систем автоматического управления : учеб. пособие для академического бакалавриата / В. А. Жмудь. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 128 с.
5. Зыков, С. В. Программирование. Объектно-ориентированный подход : учебник и практикум для академического бакалавриата / С. В. Зыков. — М. : Издательство Юрайт, 2019. — 155 с.
6. Иванов, В. М. Интеллектуальные системы : учеб. пособие для СПО / В. М. Иванов ; под науч. ред. А. Н. Сесекина. — М. : Издательство Юрайт, 2019. — 93 с.
7. Кубенский, А. А. Функциональное программирование : учебник и практикум для академического бакалавриата / А. А. Кубенский. — М. : Издательство Юрайт, 2019. — 348 с.
8. Кудрина, Е. В. Основы алгоритмизации и программирования на языке c# : учеб. пособие для СПО / Е. В. Кудрина, М. В. Огнева. — М. : Издательство Юрайт, 2019. — 322 с.
9. Кудрина, Е. В. Основы алгоритмизации и программирования на языке c# : учеб. пособие для бакалавриата и специалитета / Е. В. Кудрина, М. В. Огнева. — М. : Издательство Юрайт, 2019. — 322 с.
10. Кудрявцев, К. Я. Методы оптимизации : учеб. пособие для вузов / К. Я. Кудрявцев, А. М. Прудников. — 2-е изд. — М. : Издательство Юрайт, 2019. — 140 с.

11. Лаврищева, Е. М. Программная инженерия и технологии программирования сложных систем : учебник для вузов / Е. М. Лаврищева. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 432 с.
12. Лебедев, В. М. Программирование на vba в ms excel : учеб. пособие для академического бакалавриата / В. М. Лебедев. — М. : Издательство Юрайт, 2019. — 272 с.
13. Малявко, А. А. Формальные языки и компиляторы : учеб. пособие для вузов / А. А. Малявко. — М. : Издательство Юрайт, 2018. — 429 с
14. Мамонова, Т. Е. Информационные технологии. Лабораторный практикум : учеб. пособие для СПО / Т. Е. Мамонова. — М. : Издательство Юрайт, 2019. — 178 с.

UDC 004.932.4

ADVANTAGES OF THE ACTOR MODEL OF ASYNCHRONOUS PARALLEL PROGRAMMING

Sorogovets E.V.1, student gr.067001

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Shevchuk O. - PhD in Physics and Mathematics

Annotation. This paper presents the advantages of the actor model of asynchronous parallel programming in comparison with standard asynchronous-parallel executions.

Keywords. Actor model, asynchrony, parallelism.

УДК 004.932.4

ОБЗОР АКТУАЛЬНОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ЦИФРОВОЙ СТАБИЛИЗАЦИИ

Горбуков А.Д., студент гр.067001 магистрант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Цветков В.Ю. – д-р тех. наук

Аннотация. В этой статье приводится обзор актуальных исследований по теме цифровой стабилизации. Выделены общие шаги и подходы алгоритмов стабилизации. Найдены наиболее актуальные и распространённые подходы. Проведен обзор методов оценки качества алгоритмов стабилизации и их сравнения между собой.

Ключевые слова. Цифровая стабилизация, обработка изображений, обзор, оценка качества стабилизации видео.

Несмотря на развитие фотоматриц, остается проблема исправления искажений, вызванных нежелательными движениями камеры. В частности, большой проблемой является съемка на движущихся платформах или с рук [1]. Дополнительные проблемы вызывают матрицы, снимающие по принципу сканирующего затвора [2]. В профессиональной съемке проблему обычно решают различными штативами или схожими приспособлениями [3]. Именно такое движение камеры считается наиболее приятным для восприятия человеком. Кроме цифровой стабилизации существует множество механических и механико-цифровых методов стабилизации при помощи гироскопов, акселерометров и других датчиков ориентации [4][5].

Большинство алгоритмов имеют схожие общие шаги. Сначала производится оценка движения камеры, затем сырые данные фильтруются от нежелательных искажений и выбросов. После чего из этих данных строится модель передвижения камеры. Полученный путь корректируется, а затем из исходных данных и скорректированного пути генерируется стабильное видео.

Основные подходы оценки движения основываются на сопоставлении отдельных пикселей [6][7], блоков пикселей [8][9] и признаков. В связи с развитием вычислений на видеопроцессорах становится популярными методы, основанные на оптическом потоке. Алгоритмы выделения признаков могут быть различными, но самыми популярными являются: SIFT [10][11], SURF [12][13] и KLT [2][14]. Оценка движения обычная является самой затратной частью алгоритма. Она выбирается в зависимости от располагаемых ресурсов и желаемого быстродействия.

Из оценки движения по отдельным точкам необходимо убрать различные помехи и искажения. В основном это делается анализом статистики по двум соседним кадрам [3][15] или по целому потоку кадров [2][16]. Основное отличие заключается в том, что в случае оценки целого потока мы можем работать с длительностью траектории. Это хороший способ отсеять ненадежные точки, но при этом ресурсозатратный.

Модель камеры — это геометрическая модель, описывающая процесс съемки кадра. Очевидно, что это лишь некое приближение к реальному процессу. Разделяют двухмерные, трехмерные [1][5] и психовизуальные [2][16] модели. В свою очередь двухмерные модели могут учитывать только аффинное преобразование [3][17] или проективное преобразование [10][18]. Выбор конкретной модели движения зависит от характера стабилизируемого видео и предполагаемых ситуаций использования.

Коррекция пути обычно происходит двумя путями: с помощью фильтра нижних частот [19][20] или подгонкой пути [10][2]. ФНЧ просто убирает высокочастотные нежелательные вибрации камеры. При подгонке алгоритм пытается приблизить траекторию к «кинематографичной». Обычно это выражается в том, что корректированный путь может быть описан только простыми полиномами до 2-3 степени.

Синтез стабильного видео разделяют на плотный [21][22] и разряженный [2][23]. Первый метод применяют если нам известно положение всех пикселей текущего кадра на восстановленном кадре, а второй, когда у нас есть лишь частичная информация о перемещении пикселей.

Большой проблемой является сравнение алгоритмов. Если сравнение по скорости возможно провести объективно, то качество алгоритмов стабилизации субъективно. Существуют некоторые исследования, которые пытаются, некоторым образом, сравнить качество алгоритмов стабилизации [24]. Однако ни одной предложенной метрике не удалось стать стандартной. Наиболее часто встречающиеся метрики — это наивные подходы на основе пикового отношения сигнала к шуму [18] и субъективные оценки [2].

В связи с появлением алгоритмов, основанных на применении машинного обучения, стали, появляется базы данных с большим количеством видео для их обучения [25]. Эти базы содержат как нестабилизированное видео, так и эталонное стабилизированное. Это позволяет тестировать и сравнивать алгоритмы на одном и том же наборе данных.

Таким образом мы можем сделать вывод, что за прошедшие годы было опубликовано множество статей о различных алгоритмах цифровой стабилизации. Большинство этих алгоритмов имеют схожую структуру и состоят из одинаковых шагов. Эти шаги могут быть реализованы различными алгоритмами. Несмотря на активные исследования до сих пор не существует общепринятого подхода для оценки качества алгоритмов стабилизации и их сравнения. В смежных областях, таких как слежение за объектом, существуют общепринятые бэнчмарки и соревнования. Однако с каждым годом увеличивается количество попыток решить задачу стабилизации с помощью нейронных сетей, что способствует появлению баз данных для тестирования и сравнения.

Список использованных источников:

1. Liang, Y. Video stabilization for a camcorder mounted on a moving vehicle / Y. Liang, H. Tyan, S. Chang, H.M. Liao, S. Chen // IEEE Transactions on Vehicular Technology – 2004. – Vol. 53. – P. 1636-1648.

2. Yeong, J. K. Video stabilization based on feature trajectory augmentation and selection and robust mesh grid warping. J. K. Yeong, L. Chulwoo, K. Chang-Su. // IEEE Transactions on Image Processing, – 2015. – Vol. 24, №12. – P. 5260–5273.

3. Grundmann, M. Auto-directed video stabilization with robust L1 optimal camera paths / M. Grundmann, V. Kwatra, I. Essa. // IEEE Conference on Computer Vision and Pattern Recognition (CVPR) – 2011. – P 225–232.

4. Sachs, D. Image stabilization technology overview / D. Sachs, S. Nasiri, D. Goehl // InvenSense Whitepaper – 2006.

5. Chao, J. Probabilistic 3-D motion estimation for rolling shutter video rectification from visual and inertial measurements / L E. Brian, J. Chao // IEEE International Workshop on Multimedia Signal Processing (MMSP) – 2012. – P. 203–208.

6. Chang, H. C. A robust real-time video stabilization algorithm / H. C. Chang, S. H. Lai, and K. R. Lu. // Journal of Visual Communication and Image Representation – 2006, – Vol. 17, №3 P. – 659–673.

7. Hany, F. Video stabilization and enhancement. Technical report, / F. Hany, B. J. Wodward // Dartmouth College, Computer Science – 2007.

8. Battiato, S. A robust video stabilization system by adaptive motion vectors filtering / S. Battiato, G. Puglisi, A. R. Bruna // IEEE International Conference on Multimedia and Expo (ICME) – 2008. – P. 373–376.

9. Narendra Babu, J. Block processing video stabilization / J. Narendra Babu, M. Nageswariah, S. Shajahan, A. Maheswari. // International Journal of Scientific and Research Publications (IJSRP) – 2013. – Vol. 3, №3.

10. Gleicher, M. L. Re-cinematography: improving the camera dynamics of casual video / M. L. Gleicher and F. Liu. // ACM International Conference on Multimedia – 2007. – P. 27–36.

11. Battiato, S. SIFT features tracking for video stabilization // S. Battiato, G. Gallo, G. Puglisi, and S. Scellato. / International Conference on Image Analysis and Processing (ICIAP) – 2007. – P. 825–830.

12. Zheng, X. Video stabilization system based on speeded-up robust features // X. Zheng, C. Shaohui, W. Gang, L. Jinlun. / International Industrial Informatics and Computer Engineering Conference (IIICEC) – 2015. – P 1996–1998.

13. Song, C. Robust video stabilization based on bounded path planning // C. Song, H. Zhao, W. Jing, and Y. Bi. / IEEE International Conference on Pattern Recognition (ICPR) – 2012. P. 3684–3687.

14. Ringaby, E. Efficient video rectification and stabilisation for cell-phones // E. Ringaby, P. Forssen / International Journal of Computer Vision – 2012. – Vol. 96, №3. – P. 335–352.

15. Liu, S. Steadyflow: Spatially smooth optical flow for video stabilization // S. Liu, L. Yuan, P. Tan, J. Sun / IEEE Conference on Computer Vision and Pattern Recognition (CVPR) – 2014. – P. 4209–4216.

16. Liu, F. Subspace video stabilization // F. Liu, M. Gleicher, J. Wang, H. Jin, and A. Agarwala / ACM Transactions on Graphics (TOG) – 2011. – Vol. 30, №1. – P. 1–10.

17. Zhang, F. L. Simultaneous camera path optimization and distraction removal for improving amateur video // F. L. Zhang, J. Wang, H. Zhao, R. R. Martin, S. M. Hu. / IEEE Transactions on Image Processing – 2015. – Vol. 24 №12. – P. 5982–5994.

18. Jeon, S. Robust video stabilization using particle keypoint update and L1-optimized camera path // S. Jeon, I. Yoon, J. Jang, S. Yang, J. Kim, and J. Paik. / Sensors – 2017. – Vol. 17, №2. – p. 337.

19. Litvin, A. Probabilistic video stabilization using kalman filtering and mosaicing // A. Litvin, J. Konrad, W. C. Karl / Image and Video Communications and Processing – 2003. – P. 663–674.

20. Battiato, S. A robust video stabilization system by adaptive motion vectors filtering // S. Battiato, G. Puglisi, A. R. Bruna / IEEE International Conference on Multimedia and Expo (ICME) – 2008. – P. 373–376.

21. Sánchez, J. Comparison of motion smoothing strategies for video stabilization using parametric models. // J. Sánchez / Image Processing Online –2017. – Vol. 7. – P. 309–346.

22. Zhang, G. Robust metric reconstruction from challenging video sequences // G. Zhang, X. Qin, W. Hua, T. T. Wong, P. A. Heng, H. Bao / IEEE Conference on Computer Vision and Pattern Recognition (CVPR) – 2007. – P. 1–8.

23. Lee, D. B. ROI-based video stabilization algorithm for hand-held cameras // D. B. Lee, I. H. Choi, B. C. Song, T. H. Lee / IEEE International Conference on Multimedia and Expo Workshops (ICMEW) – 2012. – P. 314–318.

24. Li, X. Spatiotemporal statistics for video quality assessment // X. Li, Q. Guo, X. Lu. / IEEE Transactions on Image Processing – 2016. – Vol. 25, №7. – P. 3329–3342.

25. Ito, M. S. A dataset and evaluation framework for deep learning based video stabilization systems // M. S. Ito, E. Izquierdo / IEEE Visual Communications and Image Processing (VCIP) – 2019. – P 1–4.

UDC 004.932.4

Overview of relevant studiesin IN digital stabilization

Harbukou A.D.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Tsviatkou V.Yu. – Doctor of Sciences in Technical Sciences

Annotation. Overview of relevant studies in digital stabilization. Common steps and approaches in digital stabilization algorithm are highlighted. The most popular and relevant approaches are found. Video Stabilization Quality Assessment (VSQA) and corporation methods in modern studies has been reviewed.

Keywords. Digital image stabilization, digital image processing, review, Video Stabilization Quality Assessment, VSQA.

УДК 621.39

ОСОБЕННОСТИ ЦИФРОВОЙ ФИЛЬТРАЦИИ ПО АЛГОРИТМУ КАЛМАНА

Старовойтова Е.Е., Козека А.И.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Данейко Т.М. – ст. преподаватель кафедры ИКТ

Многие области науки, техники и электроники нуждаются в простых и эффективных алгоритмах фильтрации. Одним из самый популярных алгоритмах фильтрации является Фильтр Калман принцип которого состоит в том, что при фильтрации используется информация о физике самого явления.

Фильтр Калмана описывается моделью пространства состояний, динамика которого в момент времени *n* кодируется вектором состояния x_n. Модель состояния определяется как выход линейной динамической системы, на вход которой поступает белый шум:

$$x_{n+1} = Ax_n + \xi_n$$

где A – переходная матрица состояния размером (*M*x*M*), ξ_n – белый шум с нулевым средним значением и корреляционной матрицей Q.

Состояние системы не наблюдается непосредственно, а через измерения, которые описываются уравнением:

$$y_n = Cx_n + v_n$$

где y_n – наблюдаемый вектор, значение которого зависит от матрицы измерений C , вектора состояний и v_n шума измерений, который представляет собой белый шум с нулевым средним значением и корреляционной матрицей R.

Начальное состояние x0, шумы ξ и v предполагаются гауссовскими и взаимно некоррелированными.

Задача фильтра Калмана может быть сформулирована следующим образом. Заданы известные матрицы A, C, Q, R, функция распределения вероятности (ФРВ) начального состояния $p(x_0)$, ряд наблюдений $y_{1..n}$.

Требуется получить оптимальную (по критерию минимума среднего квадрата) оценку состояния x_n.

Для решения задачи использованы функции распределения Гаусса и марковского процесса первого порядка:

$$p(x_0) = N(\hat{x}_0, P_0)|_{x_0}, p(x_n|x_{n-1}) = N(Ax_{n-1}, Q)|_{x_n}, p(y_n|x_{n-1}) = N(Cx_n, R)|_{y_n}$$

Напомним, что марковский процесс первого порядка определяется как процесс, в котором текущее состояние зависит только от предыдущего и текущее наблюдение зависит только от текущего состояния:

$$p(x_n|x_{0..n-1}, y_{1..n-1}) = p(x_n|x_{n-1}), p(y_n|x_{0..n-1}, y_{1..n-1}) = p(y_n|x_n)$$

Такое свойство позволяет получить рекурсивную зависимость для функции совместного распределения вероятностей:

$$p(x_{0..n}|y_{1..n}) = p(x_0)\prod_{i=1}^{n} p(x_i|x_{i-1})\prod_{j=1}^{n} p(y_j|x_j)$$

и реализовать операции предсказания, фильтрации и сглаживания.

Функция условного распределения вероятностей $p(x_n \mid y_{1...n-1})$ может быть определена рекурсивно за 2 шага (см. рисунок 1.1.)

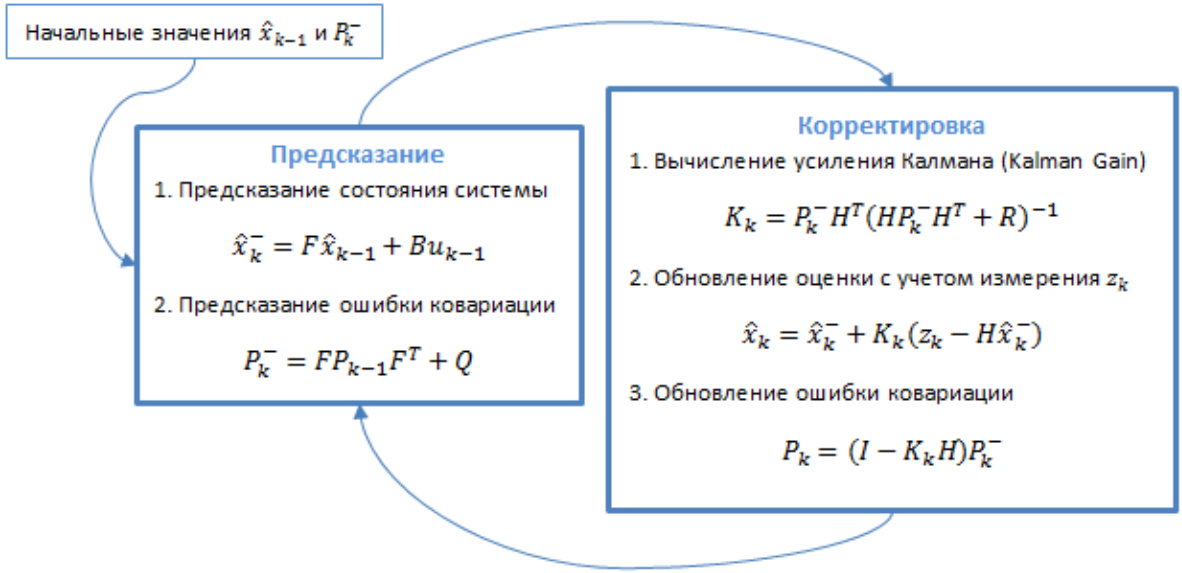


Рисунок 1.1 .– Алгоритм работы фильтра Калмана

Правило Байеса играет ключевую роль в фильтре Калмана, связывая Гауссовские переменные **y***n* линейной зависимостью с переменными x

$$p(x,y) = p(y|x)p(x) = N(Ax,Q)|_y\, N(\mu,\Sigma)|_x = p(x|y)p(y) = N(m,S)|_x N(A\mu, A\Sigma\Sigma\ + Q)|_y$$

Фильтр Калмана – один из самый популярный алгоритм фильтрации, используемый во многих областях науки и техники. Благодаря своей простоте и эффективности его можно встретить в GPS-приемниках, обработчиках показаний датчиков, при реализации систем управления и т.д.

Список использованных источников

1. Саломатин С.Б., Цифровые адаптивные методы защиты от помех, учеб.-метод. пособие С. Б. Саломатин, Д. Л. Ходыко. – Минск : БГУИР, 2007. – 84 с. : ил.
2. http://www.cs.unc.edu/~welch/kalman/media/pdf/Kalman1960.pdf.

UDC 621.39

FEATURES OF DIGITAL FILTERING ACCORDING TO THE KALMAN ALGORITHM

Starovoitova E.E., Kozeka A.I.

Belarusian State University of Informatics and Radioelectronics1, Minsk, Republic of Belarus

Daneiko T.M. – senior lecturer of department of ICT

Annotation. In the class of FIR filters, it is possible to synthesize filters that have a given frequency response and a strictly linear and therefore constant group delay (GDT), i.e. the initial phases of all frequency components of the signal receive a shift proportional to the frequency, so their phase relationships are not violated.

Keywords. FIR filters, linear phase response, impulse response, group delay.

УДК 004.01,004.02,004.4,004.6,004.7

СИСТЕМА МОНИТОРИНГА ЛОКАЛЬНЫХ И ОБЛАЧНЫХ СЕРВИСОВ

Желудкович В.В., магистрант гр.067041

Белорусский государственный университет информатики и радиоэлектроники, г.Минск Республика Беларусь

Бобов М.Н. – профессор , доцент технических наук

Аннотация. Предложен алгоритм перехода к системе мониторинга локальных и облачных сервисов. С помощью нижеописанного алгоритма перехода, становится возможным осуществлять мониторинг как локальных сетей, приложений, серверов, так и развёрнутых в облаке, с удалённого рабочего места, используя один инструмент, сохраняя безопасность, обеспеченную Microsoft Active Directory.

Ключевые слова: локальные сервисы, служба каталогов, службы авторизации, служба аутентификации, облачные сервисы.

ВведениеДля мониторинга локальный и облачных сервисов на базе операционных систем семейства Windows существует огромное количество, как стороннего, так и встроенного программного обеспечения. С переносом сервисов в облако появляется задача одностороннего мониторинга двух систем, как облачной, так и локальной с использованием общего инструмента с одинаковым набором метрик. Это необходимо для скорейшего выявления неполадок, сетевых атак. Кроме того, необходим такой инструмент, который может быть использован любым среднестатистическим специалистом, не обладающим специфическими знаниями. Также данное программное обеспечение должно соответствовать всем нормам сетевой безопасности. Для осуществления всего вышеописанного необходимо подключить все свои сервисы к системе мониторинга Microsoft Azure arc. Для этого необходима подготовка, обновление программного обеспечения, а также знание скриптового языка Microsoft PowerShell.

Подключение к общей системе мониторинга сетевых сервисов. Подготовка текущей системы заключается в обновлении систем каталогов Windows Active Directory до минимально необходимой версии 2016 года. Обновление привычным способами Microsoft приводит к потере данных, изменению схемы каталогов, некорректной работе службы групповых политик. Что в свою очередь часто приводит к нарушению безопасности. Уровень доступа пользователей может манятся. А отследить внесённые изменения не всегда представляется возможным. Identity сервисы являются наиболее важными сервисами в сегодняшнее время. Наиболее правильным путём будет добавление нового мастер сервера в существующий домен и передача ему роли мастера операций посредством PowerShell с параметрами. Сервер должен находится в одной подсети со старым для корректного ввода в домен. Также можно использовать средства виртуализации для создания сервера ADDS.

PowerShell код выполняемый в командной оболочке: Move-ADDirectoryServerOperation MasterRole -Identity "USER01-DC01" -OperationMasterRole PDCEmulator.

Предварительно необходима установка module Active Directory. Этот метод позволяет сохранить без изменений базу данных Active Directory.

Далее, чтобы проверить, перемещены ли роли, нужно перейти на новый сервер Windows. В Диспетчер сервера в разделе средства выбрать Active Directory модуль для Windows PowerShell Get-ADDomain. Командлет Get-ADForest для просмотра владельцев ролей FSMO. Далее после репликации контролёра домена можно выводить из работы старый сервер и проверить аутентификацию на любом пользователе.

После осуществления обновления необходимо синхронизировать Azure Active Directory с Active Directory Domain Services. В облачном портале появляется функция SSO - Single Sign-On. Другими словами, появляется возможность авторизации и аутентификации при помощи логина и пароля пользователя, созданного на локальном сервере. Но вместе с тем у этого пользователя отсутствует доступ к управлению локальной сетью. Для этого системным администратором необходимо настраивать VPN-тоннель для установки взаимоотношений двух сетей облачной и локальной. У пользователя в облачном портале есть доступ только к мониторингу сервисов.

Далее необходима настройка системы мониторинга на стороне облака. В портале Azure, в строке поиска ресурсов устанавливаем все необходимое (рис. 1).

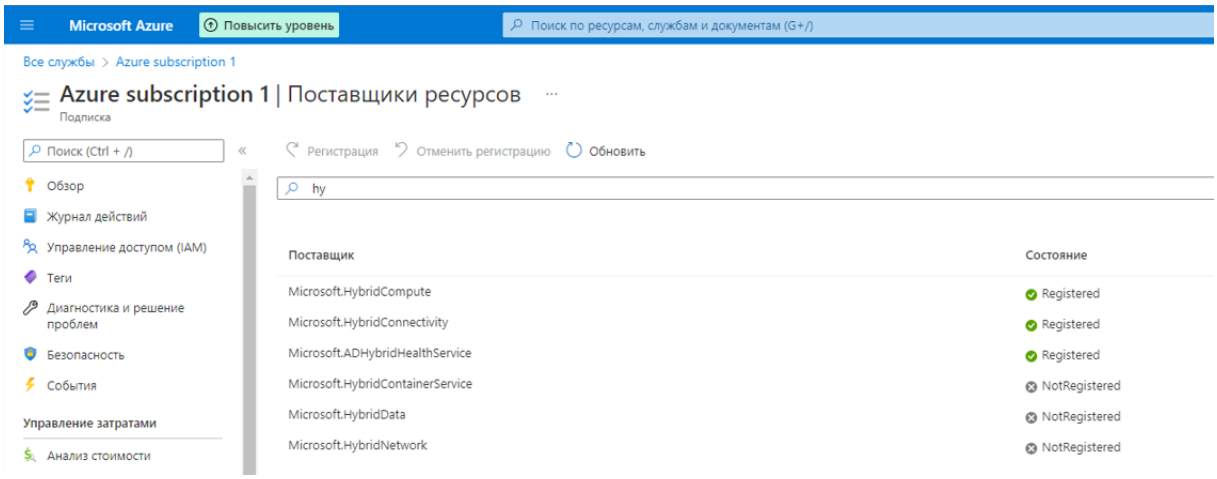


Рис. 1. Ресурсы системы мониторинга

Hybrid Compute, Hybrid Connectivity – отвечают за подключение гибридных серверов (локальных, облачных).
Hybrid HealthCare – панель мониторинга гибридной системы.
После установки ресурсов необходимо осуществить подключение серверов. Подключение осуществляется при помощи скриптового языка PowerShell, на стороне сервера, который необходимо подключить. Пример скрипта описан на рис. 2.

C: > Users > zhalu > OneDrive > Рабочий стол > ExitTask > ip.ps1

```
# Скачивание и установка пакетов
Invoke-WebRequest -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\install_windows_azcmagent.ps1"
# Установка гибридного агента
& "$env:TEMP\install_windows_azcmagent.ps1"
if($LASTEXITCODE -ne 0) {
throw "Failed to install the hybrid agent"
}
# Запуск подключённой программы
& "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "ADDS" --tenant-id "f6ce8ba2-89a1-4442-b939-1ddbbb7c2e47" --`
location "eastus" --subscription-id "d8272f6f-327a-4dd9-9754-f2a0fa035a2b" --cloud "AzureCloud" --correlation-id "c8a00abe-747a-4d22-919a-c2609c4b5001"`
if($LastExitCode -eq 0){Write-Host -ForegroundColor yellow "To view your onboarded server(s), navigate to`
https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType /Microsoft.HybridCompute%2Fmachines"}
```

Рис. 2. Пример кода для подключения к системе мониторинга Azure

В данном коде осуществляется запрос на удалённый сервер, для скачивания сгенерированного скриптового файла под определённый сервер, его дальнейшая установка и запуск. Всё это происходит в командной оболочке.
После выполнения скриптового кода на сервере должны отобразиться сообщения о успешном выполнении этапов установки и запуска (рис.3). При неверном исполнении будут выводиться ошибки со всей необходимой информацией. Это описано в коде для устранения проблем установки.

```
PS C:\Users\Administrator> # Download the installation package
PS C:\Users\Administrator> Invoke-WebRequest -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\instal
l_windows_azcmagent.ps1"
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Install the hybrid agent
PS C:\Users\Administrator> & "$env:TEMP\install_windows_azcmagent.ps1"
VERBOSE: Installing Azure Connected Machine Agent
VERBOSE: Downloading agent package
VERBOSE: Installing agent package
Installation of azcmagent completed successfully
PS C:\Users\Administrator> if($LASTEXITCODE -ne 0) {
>>     throw "Failed to install the hybrid agent"
>> }
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Run connect command
PS C:\Users\Administrator> & "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "Arc" --ten
ant-id "f6ce8ba2-89a1-4442-b939-1ddbbb7c2e47" --location "westeurope" --subscription-id "d8272f6f-327a-4dd9-9754-f2a0fa035a2b"
 --cloud "AzureCloud" --correlation-id "87d902f2-b789-46ba-ab1a-1deb9c02f00b"
time="2022-02-15T09:09:26-08:00" level=info msg="Loading AgentConfig file from: C:\\ProgramData\\AzureConnectedMachineAgent\\C
onfig\\agentconfig.json"
time="2022-02-15T09:09:26-08:00" level=info msg="Onboarding Machine. It usually takes a few minutes to complete. Sometimes it
may take longer depending on network and server load status."
time="2022-02-15T09:09:26-08:00" level=info msg="Check network connectivity to all endpoints..."
time="2022-02-15T09:09:27-08:00" level=info msg="All endpoints are available... continue onboarding"
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code CSWLJDMS6 to authenticate.
time="2022-02-15T09:10:26-08:00" level=info msg="Successfully Onboarded Resource to Azure" VM Id=dc4e026d-e60e-45c0-99c2-4db3c
d1c89e2
PS C:\Users\Administrator>
PS C:\Users\Administrator> if($LastExitCode -eq 0){Write-Host -ForegroundColor yellow "To view your onboarded server(s), navig
ate to https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.HybridCompute%2Fmachines"}
To view your onboarded server(s), navigate to https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Micros
oft.HybridCompute%2Fmachines
PS C:\Users\Administrator>
```

Рис. 3. Успешное добавление сервера в систему мониторинга

В панели Azure в облачном портале появится добавленный сервер (рис.4).

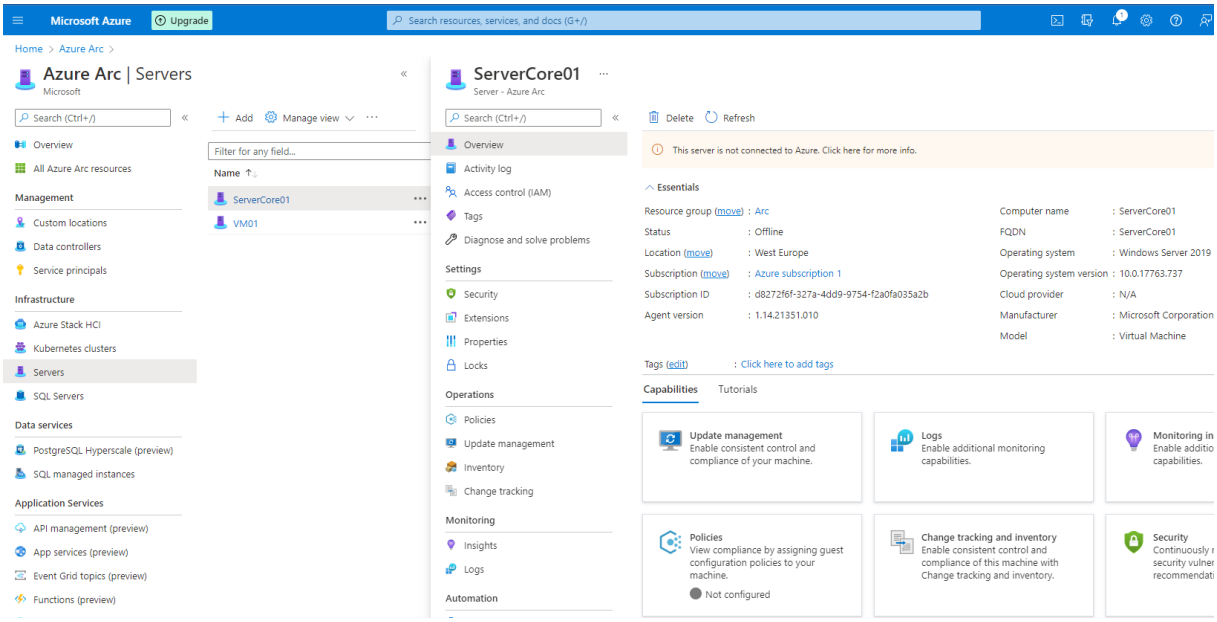


Рис. 4. Панель мониторинга Azure

Дополнительные возможности системы общего мониторинга и управления: централизованное управление широким спектром ресурсов, включая серверы Windows и Linux, SQL Server, кластеры Kubernetes; обеспечение управлением жизненным циклом виртуальных машин для своих сред Azure Stack HCI и VMware из централизованного расположения; создание ориентированных на облако приложений в большом масштабе.

Заключение. Переход на вышеописанную систему мониторинга открывает совершенно новые возможности. Нет необходимости отказываться от существующей локальной сетевой структуры, мониторинг осуществляется удалённо из любой точки планеты, аутентификация и авторизация осуществляется при помощи Active Directory, что в свою очередь обеспечивает безопасность. Существует перспектива роста и переход к новой системе управления. Всё выше описанное позволяет с уверенность сказать, что любую старую сетевую структуру можно безболезненно переносить в облако имея при этом современный доступ к мониторингу всех сервисов. Не нужно иметь несколько инструментов мониторинга для каждой из сетей будь то облако или локальный сервер.

Список литературы

1. Mastering Active Directory 2021. Dishan Francis. // Domen Controllers. 2021. Vol. 3. P. 31–37.
2. PowerShell for system administrators. Adam Bertram //Active Directory. 2021. Vol. 51. P. 100–125.
3. Computer Networking James F.Kurose //. 2008. Vol. 9. P. 35–79.
4. Microsoft Azure Security Center, First Edition. // . 2018. Vol. 48. P. 130–159.

УДК 003.26

MATHEMATICAL SIMULATION OF DIGITAL FILTERS WITH FINITE PULSE CHARACTERISTICS

Pesetskaya A.A., Sosna I.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

Daneiko T.M. – Senior Lecturer

Abstract. The article discusses the methodology for optimizing the structure of decimation filters using mathematical modeling. This can significantly reduce the requirements for FPGA resources. The study of the architecture of the FIR resampling filter with a buffer is divided into stages.A finite impulse response (FIR) digital resampling filter is a filter which impulse response (response to any finite length input) has a finite duration, since it ends to zero in a finite time.
An FIR filter can be used to implement almost every kind of frequency response in digital form and is itself implemented with help of using multipliers, adders and delay elements [1].

When implementing FIR filters in field-programmable gate arrays (FPGA), their capabilities are significantly limited by some FPGA resources. The most "deficient" resource usually turns out to be a resource, such as multipliers.

Due to the lack of multipliers, developers have to use more expensive FPGAs, reduce the filter order, and reduce the number of available digital strip values. As a result, this negatively affects the technical characteristics of the final product.

The methodology for optimizing the structure of FIR decimation filters consists in performing the following actions:

– Calculate the corresponding coefficients of the FIR filter and the order of the digital filter.

The characteristic of a classical FIR filter can be represented as:

$$y(n) = \sum_{i=0}^{n} b_i x(n - \mathrm{i}) \qquad (1)$$

where n is the order of the filter,

b_i is filter coefficient.

The block diagram of a non-recursive FIR filter is shown in Figure 1.

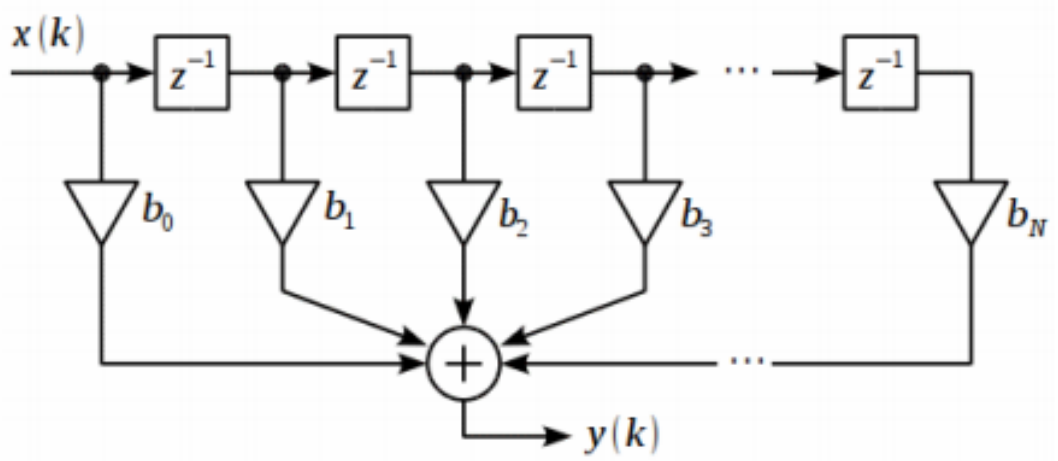


Fig. 1 – Block diagram of a non-recursive FIR filter

An order n FIR filter contains **n** delay lines and **n + 1** coefficients. If the coefficient **b0 = 1**, then we have an FIR filter of order **n**, for which multiplication by **b0 = 1** will be trivial.

The impulse response of an FIR filter is always finite and exactly matches the filter coefficients. The array of such filters allows us to implement **m** different nominal values of digital bands, where **m** is any integer.

– Estimate the need for resources (such as multipliers) for this filter array:

$$M = (n + 1) \times m \qquad (2)$$

– Consider as an alternative solution the architecture of the buffer FIR decimation filter shown in Figure 2.

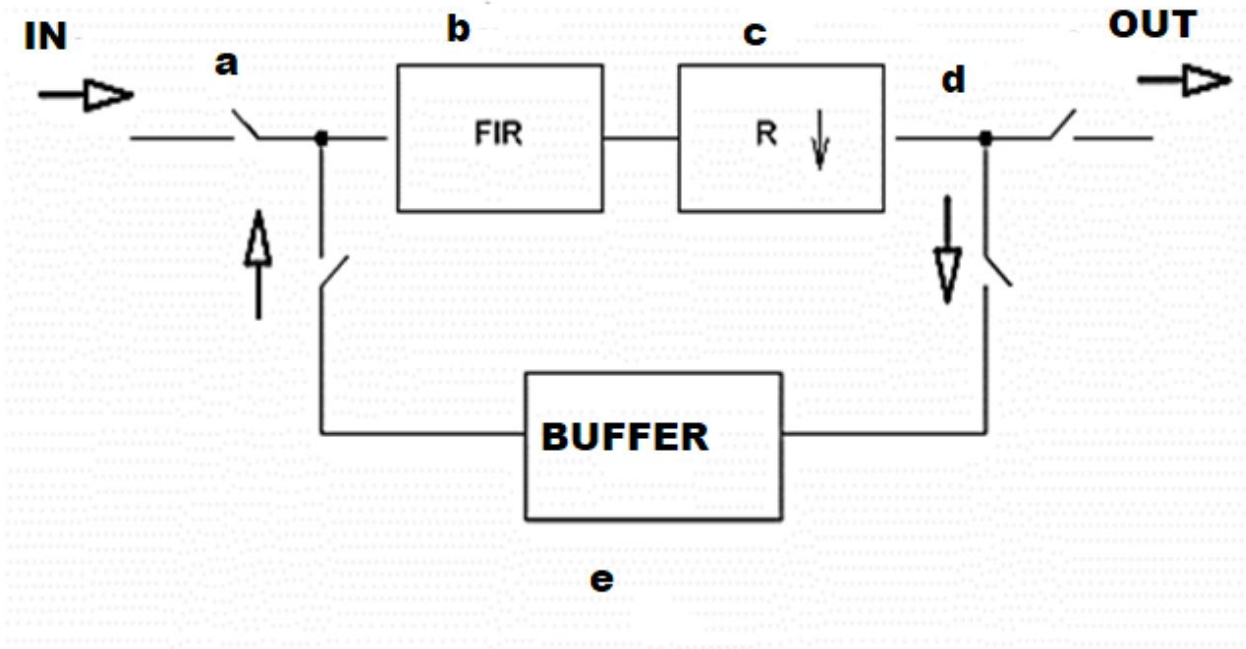


Fig. 2 – Block diagram of the buffer FIR filter:

a - input logic switch;

b - halfband FIR filter;

c - decimation block with a coefficient R = 2;

d - output logic switch;

e - buffer.

The input for this filter are samples of a digital signal, pre-converted to 0 Hz.

- Evaluate the data processing scheme with this filter.

1. Data enters the input logic switch a) and is redirected to the input of the FIR filter b), which is designed primarily to remove aliasing in the input signal during decimation.

2. After filtering, the clock frequency of the signal is halved using the decimator c).

3. After decimation, the data goes to the output switch d). If the required signal bandwidth is not reached, the data is redirected to the buffer e).

4. After being filled, the buffer returns the data block through the input switch a) for the next iteration to narrow the bandwidth.

5. Steps 2-4 are repeated until the required signal bandwidth is reached. It is obvious that for block data, that due to the cyclic structure of signal processing, it is possible to implement any decimation coefficients on one filter, if they are multiples of **2k**, where **k** = 1, 2, 3, ...

This filter allows you to process streaming (continuous) data with decimation by half and block data (data blocks with a fixed number of samples) with any decimation factor divisible by **2k**, i.e. it allows you to create unlimited digital signal bands.

For streaming data, the specified filter can be applied with a decimation factor of 2. In this case, the filter passes the data through itself once without using a buffer. The use of a filter with decimation coefficients of more than 2 is possible, but not so effective due to a significant reduction in suppression in the attenuation band.

- Consider additional possibilities for optimizing the FIR filter requirements for the number of multipliers required for its implementation in modern field-programmable gate arrays.

For the analysis, it is necessary to introduce the following restrictions into the filter structure: let us assume that every second filter coefficient is equal to zero and the filter coefficients are symmetric about the central coefficient. This filter requires only one multiplier for every four orders of magnitude for implementation, in contrast to the classical FIR filter.

- Take into account when designing the filter that a necessary and sufficient condition for the equality of every second coefficient to zero is that the filter should be half-band, or in other words, cutoff frequency (**Wpass**) and stop frequency (**Wstop**) should be symmetric about the half the sampling frequency (**Fs / 2**) [2].

The converse is also true. For a half-band filter with cutoff frequencies symmetric about the frequency **Fs / 2**, every second coefficient is equal to zero. It should be noted, however, that the cutoff and stop frequencies should be as close as possible to the half of the sampling rate as possible. Otherwise, the equality of every second sample to zero can significantly distort the filter characteristics.

- When implementing a filter buffer, it is necessary to take into account that an FIR filter is a non-recursive filter or a convolution filter. FIR filters convolve their coefficients with a sequence of input data samples, while the resulting data volume increases according to the formula:

$$\mathrm{K} = \mathrm{K}_d + \mathrm{K}_f - 1 \qquad (3)$$

where **K** is the number of elements in the output sequence;

$\mathbf{K_d}$ is the number of input data samples;

$\mathbf{K_f}$ is the number of filter coefficients.

In this case, the first $\mathbf{K_f - 1}$ samples of the output sequence are not valid.

The fact of an increase in the number of samples at the output can be explained as follows: the FIR filter is designed as a delay line, the outputs of which are multiplied by coefficients and summed up. The length of the delay line is equal to the order of the filter. Therefore, until the entire delay line is full, the output data is not valid.

In order for all output data to be valid and constant in size, the first $\mathbf{K_f - 1}$ samples must be discarded. It must be done also when data is returning to the next iteration.

One of the important properties of the filter is the linearity of its phase-frequency characteristic (PFC). The non-linear PFC of the filter distorts the signal, i.e. different frequencies acquire different phase shifts and, accordingly, different time delays at the filter output. This should be taken into account, since, for

example, in coherent processing, phase distortion is unacceptable. Therefore, the more linear the PFC – the better the filter.

The proposed architecture has some restrictions on its application, namely: the filter can be effectively applied with a decimation factor of more than 2 only with block data; decimation coefficients can only be multiples of **2k**; the filter has a relatively "rigid" structure, namely, every second coefficient is equal to zero, and the coefficients must be symmetric about the central coefficient [3]. However, this structure is easily implemented by using standard mathematical modeling tools.

Thus, completing of an independent computational study for optimizing the structure of FIR decimation filters, according to the proposed method, will allow students to effectively master the material.

Sources

1. Karbushov, Ch.S. Development of an FIR filter using a distributed arithmetic architecture // Technical sciences: problems and prospects: materials of the V International scientific conference. - 2017.

2. Steven W. Smith, The Scientist and Engineer's Guideto Digital Signal Processing, Second Edition, 1999, California Technical Publishing, P.O. Box 502407, San Diego, CA 92150.

3. Theory and practice of digital signal processing [Digital resource]: Structures of digital filters and their characteristics. –Access mode: http://www.dsplib.ru/content/filters/ch10/ch10.html

УДК 003.26

ПРИМЕНЕНИЕ ТЕОРИИ ВЕРОЯТНОСТЕЙ В ЗАДАЧАХ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

Старовойтова Е.Е.

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – ст. преподаватель каф. ИКТ

Теория вероятностей представляет собой раздел математики, изучающий случайные события, случайные величины, их свойства и операции над ними. Случайное событие есть любой факт в опыте со случайным исходом, который может произойти или не произойти. Случайный процесс в теории вероятностей — семейство случайных величин, индексированных некоторым параметром, чаще всего играющим роль времени или координаты. Случайными величинами называют величины, которые принимают в зависимости от случая те или иные значения с определенными вероятностями.

К случайным процессам относится большинство процессов, протекающих в радиотехнических устройствах.

На практике все сигналы, которые предназначены для передачи информации, носят случайный характер. Именно в случайности изменения сигналов заложена информация, которую необходимо передать получателю. Помимо этого, при передаче сигналов действуют помехи, которые также носят случайный характер.

Случайным сигналом называют функцию времени, значения которой заранее неизвестны и могут быть предсказаны лишь с некоторой вероятностью. К основным характеристикам случайных сигналов относятся: закон распределения (относительное время пребывания значения сигнала в определенном интервале), спектральное распределение мощности сигнала.

В задачах цифровой обработки сигналов случайные сигналы делятся на два класса: шумы (беспорядочные колебания, состоящие из набора разных частот и амплитуд), сигналы (несущие информацию, для обработки которых требуется прибегать к вероятностным методам).

С помощью случайных величин можно моделировать воздействие реальной среды на прохождение сигнала от источника к приёмнику данных. При прохождении сигнала через какое-то шумящее звено, к сигналу добавляется так называемый белый шум. Как правило, спектральная плотность такого шума равномерно распределена на всех частотах, а значения шума во временной области распределены нормально (Гауссовский закон распределения).

Функцией распределения случайной величины X называется вероятность того, что она примет значение меньшее, чем аргумент x функции F(x):

$$F(x) = p(X < x) \tag{1.1}$$

Примем во внимание, что сигнал распространяется во времени, и тогда, функция распределения примет следующий вид:

$$F(x,t) = p(X(t) < x) \tag{1.2}$$

Функция распределения любой дискретной случайной величины есть разрывная ступенчатая функция, скачки которой происходят в точках, соответствующих возможным значениям случайной величины, и равны вероятностям этих значений.

Зная, что плотность вероятности, есть производная функции вероятности, и характеризует плотность вероятности в окрестности точки x, можем записать:

$$f(x,t) = \frac{dF(x.t)}{dx} \tag{1.3}$$

Для изучения распределения случайных величин используют ряд числовых характеристик, самыми важными из которых являются математическое ожидание, имеющее смысл среднего

значения, и дисперсия, характеризующая разброс значений случайной величины относительно ее математического ожидания.

$$m_X = \int_{-\infty}^{\infty} x \cdot f(x)dx \tag{1.4}$$

$$D_x = \int_{-\infty}^{\infty} (x - m_X)^2 f(x)dx = \int_{-\infty}^{\infty} x^2 f(x)dx - m_x^2 \tag{1.5}$$

где x – значение случайной величины.

Для цифровой обработки сигналов данные характеристики являются необходимыми и обязательными для описания случайного сигнала, развивающегося во времени. Выражения (1.4) и (1.5) примут вид:

$$m_X(t) = \int_{-\infty}^{\infty} x \cdot f(x,t)dx \tag{1.6}$$

$$\begin{aligned} D_x(t) = \int_{-\infty}^{\infty} (x - m_X(t))^2 f(x,t)dx \\ = \int_{-\infty}^{\infty} x^2 f(x,t)dx - m_x(t)^2 \end{aligned} \tag{1.7}$$

Следует отметить, что данные характеристики имеют различные формы записи исходя из типа случайной величины, а также данные параметры широко применяются в теории сигналов, т.к. математическими моделями случайных сигналов и помех являются случайные процессы. При достаточном знании случайных величин, хорошо описанная случайная функция поможет решить задачу нелинейной обработки цифровых сигналов.

УДК 003.26

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА НА ОСНОВЕ ДАННЫХ, ПОЛУЧЕННЫХ С АКСЕЛЕРОМЕТРА ТЕЛЕФОНА

Яцевич К. А., Анциферова Е. И., Сайко Р.И.

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Данейко Т.М. – ст. преподаватель каф. ИКТ

Аннотация. В данной работе описывается процесс получения данных с акселерометра телефона, а также их дальнейший анализ и их использование в качестве доказательной базы. После получения, данные необходимо отфильтровать, отбросив значения, которые имеют высокую погрешность, и, затем, разделив данные на группы, приступить к их обработке.

Ключевые слова: акселерометр, анализ данных, датчики телефона.

В каждом смартфоне существует набор датчиков, которые служат для различных целей. Датчиками называются различные устройства, считывающие дополнительную информацию. Они делают работу с телефоном, планшетом или другим гаджетом удобнее, а также добавляют больший функционал.

Примерами таких датчиков являются: гироскоп, акселерометр, магнитометр, шагомер, датчик освещенности, дактилоскопический сенсор и многие другие. Этот набор может варьироваться для различных моделей телефонов, однако практически во всех есть акселерометр. Он является самым простым и служит для регистрации поворота смартфона из портретной ориентации в ландшафтную. Если точнее, акселерометр регистрирует разницу ускорения объекта и гравитационного ускорения по трём осям. Затем электроника вычисляет разницу, делает выводы и отправляет сигнал программному обеспечению - когда и в какую сторону повернуть экран. Отсюда вытекает главный недостаток акселерометра – если нет ускорения или оно не велико, то акселерометр перестает регистрировать положение устройства в пространстве или делает это с большой погрешностью.

Для реализации получения данных необходимо написать программный код, который регистрирует значения по трем осям и предоставляет их для дальнейшей обработки. Для этого используется среда разработки Android Studio. В данную среду разработки встроен эмулятор, который помогает отследить изменение данных, в зависимости от изменения положения смартфона, выбранного для исследования (см.рис.1).

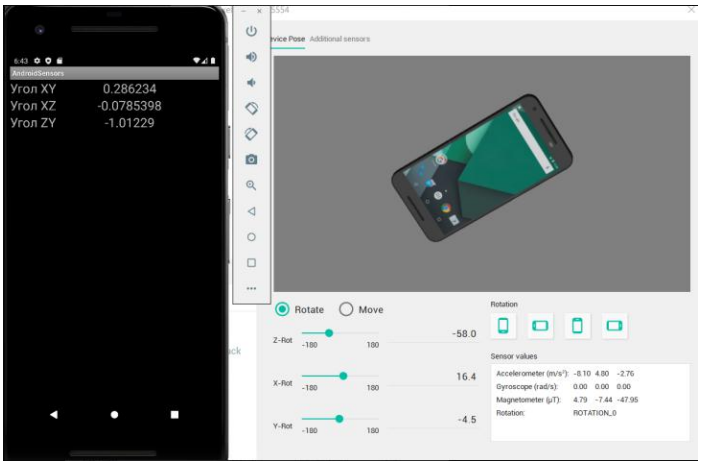


Рисунок 1 – Процесс изменения данных, в зависимости от положения смартфона

Для анализа, полученные данные необходимо не только зафиксировать, но еще и сохранить. Это можно сделать локально либо поместить в удаленное хранилище. Так как в результате получается достаточно большой объем данных, можно реализовать удаление значений, которые использовались ранее, однако при последующих исследованиях уже не нужны.

Чтобы разбить значения на группы для более удобного анализа, можно воспользоваться программной реализацией записи определенного количества данных.

Вся программная реализация происходит на языке программирования Java, так как он является наиболее удобным и распространенным для приложений на Android.

Список использованных источников:

1. Собираем показания датчиков Android смартфона [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/137678/

2. SkillFactory blog [Электронный ресурс]. – Режим доступа: https://blog.skillfactory.ru/kak-polzovatsya-android-studio/

ИНФОКОММУНИКАЦИИ

Сборник материалов 58-ой научной конференции аспирантов, магистрантов и студентов

Ответственный за выпуск *Т.М. Данейко*

Компьютерная верстка *Коробкина Е.А.*

Дизайн обложки *Коробкина Е.А.*


ФАКУЛЬТЕТ
ИНФОКОММУНИКАЦИЙ