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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СБОРНИК МАТЕРИАЛОВ
59-я научной конференции
аспирантов, магистрантов и студентов
17–21 апреля 2023 года

Минск, БГУИР

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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

Сборник материалов

17–21 апреля 2023 года
Минск, БГУИР

УДК 621.391

59- я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 17-23 апреля 2023 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2023. – 190 с.; ил.

В сборнике опубликованы материалы докладов, представленных на 59-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»

Статистика по 59-ой научной конференции аспирантов, магистрантов и студентов УО «Белорусский государственный университет информатики и радиоэлектроники»

НАПРАВЛЕНИЕ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рисунок 1 – Диаграмма «Количество статей по секциям»

Рисунок 2 – Учреждения образования, принявшие участие в конференции

Рисунок 3 – Участники конференции

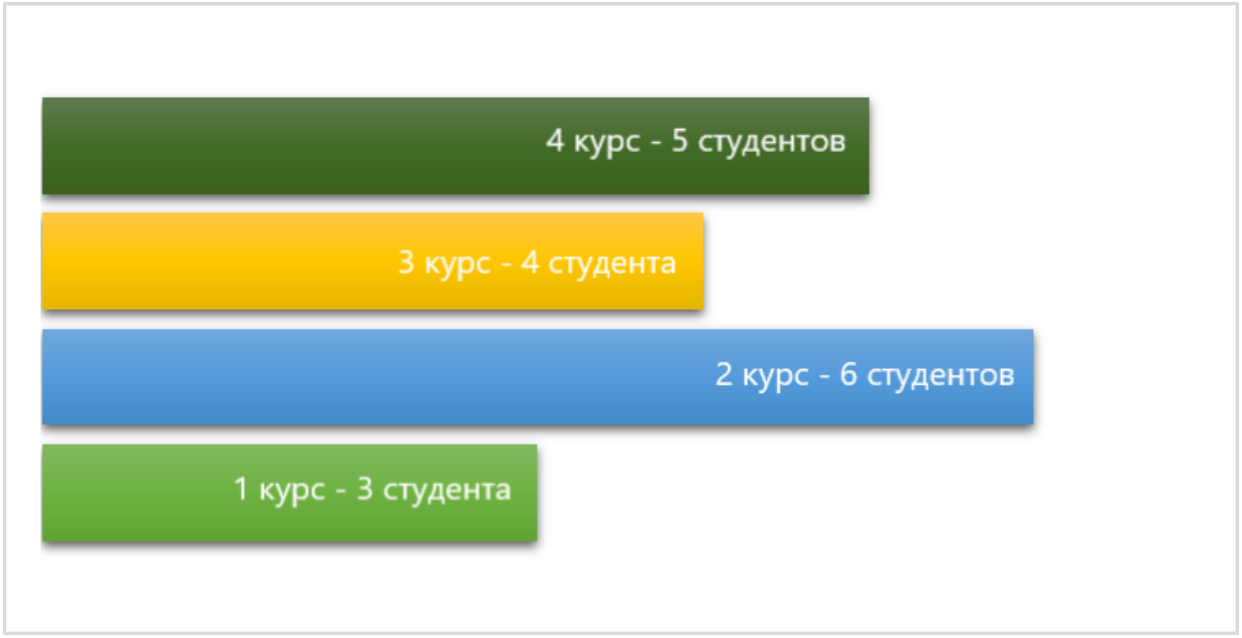


Рисунок 4 – Студенты-участники конференции

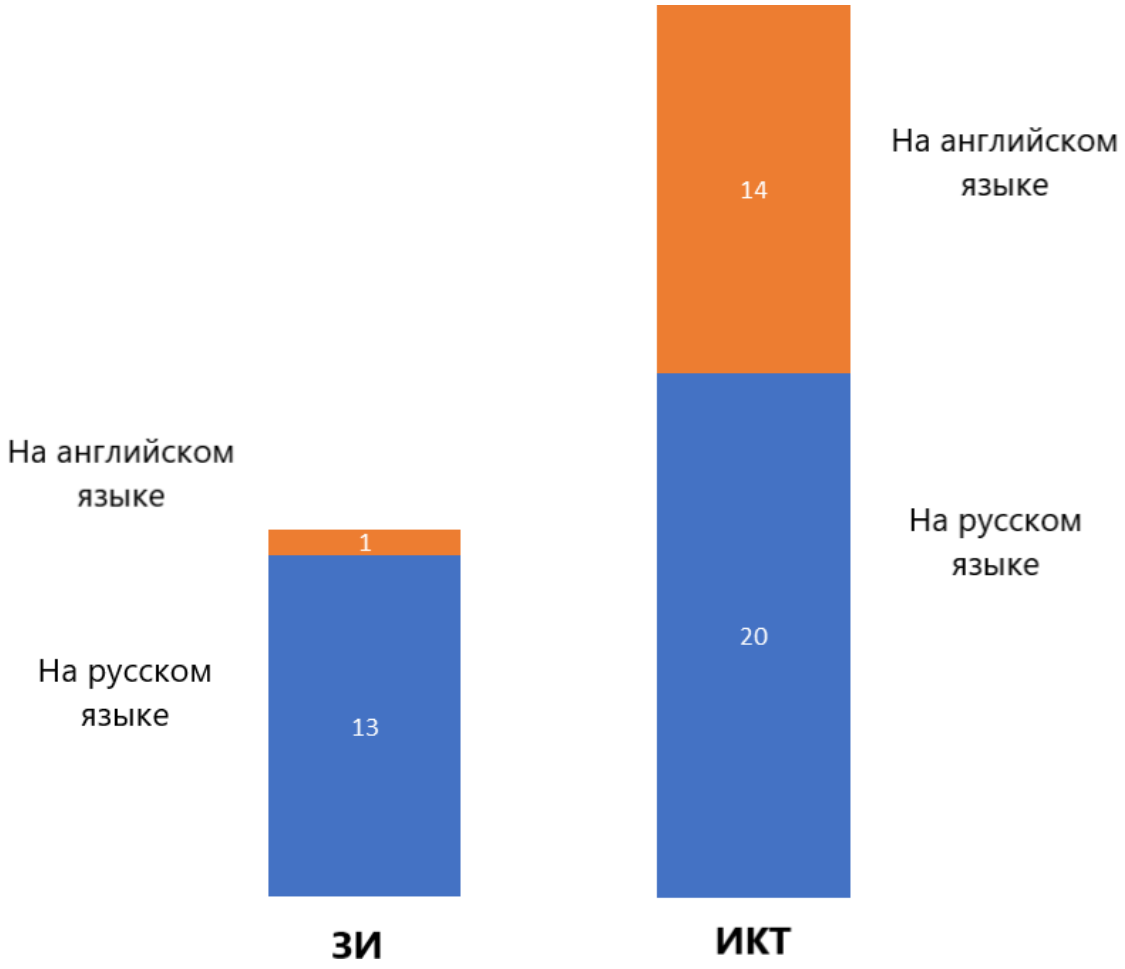


Рисунок 5 – Диаграмма «Материалы конференции на русском и английском языках»

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ» СТАТЬИ

УДК 004.056.5:34

АНАЛИЗ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Дорожкин И.В., ст. гр. 173602; Шарафанович Я.О., ст. гр. 173602

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук

Аннотация. Использование компьютерных и информационных технологий в различных сферах жизни общества становится обязательным атрибутом для достижения максимальной эффективности данной сферы. В связи с этим сфера информационных технологий становится всё более популярной для различного рода мошенников и преступников. Через информационные технологии проходит значительный поток финансов и различной личной информации. Мошенники пользуются этим, пытаясь различными способами выкрасть деньги или же личную информацию пользователя, чтобы в дальнейшем использовать её в своих целях. В данной статье рассмотрены различные источники угроз и виды преступлений в сфере информационных технологий. Основными выводами являются меры предосторожности, способные уберечь пользователя от потенциальных опасностей деятельности правонарушителей.

Ключевые слова: информационные технологии, киберпреступность, фишинг, кардинг, информатизация, компьютерная информация, вирус, уголовный кодекс.

Одним из самых распространенных видов правонарушений в сфере информационных технологий являются разного рода мошеннические схемы. Разделить такие преступления на отдельные категории довольно сложно, так как встречается довольно много пересечений. Однако в целом можно выделить следующие виды киберпреступлений:

– финансово-ориентированные преступления;

– киберпреступления, связанные со вторжением в личную жизнь;

– социальные и политически мотивированные киберпреступления.

Существует множество способов и схем, с помощью которых мошенники получают доступ к персональным данным пользователя, такими как пароли, данные банковских карт и многое другое. Наиболее часто встречающимися являются:

— фишинг;

— кардинг;

— "нигерийские" письма;

— кибервымогательство;

— взлом аккаунтов социальных сетей.

Рассмотрим каждый вид мошенничества подробнее.

Фишинг — вид интернет-мошенничества, который заключается в "выуживании" конфиденциальных данных у пользователя. Спецификой данного метода является то, что жертва мошенничества предоставляет свои данные добровольно. Для этого преступники используют специальные фишинговые сайты, email-рассылку, нацеленную рекламу. Как правило, мошенники маскируются под известные компании, социальные сети или сервисы электронной почты.

Примерами фишинга могут быть:

– рассылка поддельных сообщений с просьбой подтвердить логин или пароль;

– фишинговые схемы при проведении интернет-аукционов, при этом товары выставляются на продажу на легальном сайте, однако средства перечисляются через поддельный web-узел;

– фиктивные благотворительные организации, обращающиеся с просьбой о пожертвовании денежных средств на спасение больного ребёнка или вымирающего вида животного;

– создание фишинговых интернет-магазинов, где товары продаются по очень низким ценам либо с большими скидками, что привлекает посетителей, и они предоставляют данные своих банковский карт не подозревая, что становятся жертвами мошенничества[3].

Самым известным случаем, когда знаменитый человек стал жертвой фишинга, стал взлом хаккерами почты главы избирательного штаба предвыборной компании Хилари Клинтон Джона Подесты. Злоумышленники прислали ему письмо, что его пароль от почтового ящика Google был взломан и его стоит сменить. Политик перешёл по указанной ссылке на поддельный сайт и сменил там пароль, и, таким образом, передал данные своей почты хаккерам. Как результат, в интернет попали сотни его личных писем, многие из которых оказались компрометирующими. Из-за данного инцидента рейтинг Клинтон упал, и она проиграла выборы Дональду Трампу.

Кардинг — сфера киберпреступности, которая напрямую взаимодействует с деньгами обычных законопослушных граждан. При данном виде мошенничества производится операция с использованием платёжной карты, не инициированная её держателем[4]. Кража денежных средств — одна из самых страшных опасностей для любого человека, но есть факторы, из-за которых на сферу кардинга стоит обращать особое внимание.

В основном "кардеры" осуществляют свою деятельность на территории США или Европы. Это обусловлено тем, что уголовные сроки за такие преступления в Америке или Европе находятся в пределах 2-5 лет тюремного заключения, в то время как в странах СНГ этот срок может доходить и до десяти лет заключения. Также работа с русскоязычными счетами сопряжена с множествами проблем, ведь данные системы защиты сильно опережают западные. Однако не стоит отметать эту угрозу, ведь хоть для большинства кардеров присуща работа не в нашей стране, некоторые всё таки продолжают работать в СНГ. А если речь идёт о более мелких преступниках, то и подавно, ведь внимания к своей персоне они привлекают куда меньше.

Кардеры используют ряд методов для кражи платёжных средств:

фишинг, как и описывалось ранее, создаётся поддельный сайт, на котором пользователь должен ввести свои платёжные данные;

взлом баз данных мелких предприятий, например магазинов, сервера которых плохо защищены, а иногда и самовольная продажа банковских данных самой компанией или её сотрудниками;

После получения данных карты, злоумышленники либо просто снимают с неё все сбережения, либо же продают карту на специальных магазинах, называемых "кардер-шопами".

Но опасность кардинга состоит еще и в том, что обычный пользователь может быть привлечён к уголовной ответственности. Так от кардеров вам может прийти сообщение, где будет предлагаться с помощью некоторого сервиса оплачивать такси или заказывать еду по очень выгодной цене, нужно лишь сбросить дельцу указанную сумму и пользоваться услугами такси или доставки через данный сервис. Выполнив такие действия, вы вполне можете получить повестку в суд по уголовной статье в роли соучастника, ведь деньги, которые вы выслали мошенникам были положены на украденную карту и именно с неё оплачивались все счета данного сервиса. Подобные схемы возможны и при оплате перелётов, туров и других дорогостоящих услуг.

"Нигерийские" письма — вид мошенничества, основанный на массовой рассылке электронных писем. Своё название письма получили из-за того, что данный вид мошенничества получил наибольшее распространение в Нигерии, причём ещё до распространения интернета, когда письма распространялись по обычной почте. Однако такого рода письма могут приходить и из других стран, но всё же в основном из стран Африки, например, Анголы, Того, Гамбии, Сомали и других.

Схема подобного рода мошенничества заключается в следующем:

В сети рассылается тысячи электронных писем с разного рода предложениями и услугами.

В случае, если мошенники получают от адресата ответное письмо, выражающее некоторую заинтересованность, преступники вступают в диалог с адресатом, пытаясь получить от него необходимые данные: счета, пароли, непосредственно деньги и тому подобное.

Переписка продолжается до тех пор, пока жертва не будет сама готова перечислить деньги мошенникам.

После перечисления денег возможны два сценария развития событий: если мошенники понимают, что их "клиент" безусловно верит им, то под каким-либо предлогом сообщают ему, что перечисленных им средств недостаточно, и необходимо выслать ещё; либо же переписка мошенников с их жертвой резко обрывается, а счёт, на который были переведены нужные средства моментально закрывается.

В настоящее время наиболее распространенными являются следующие сценарии мошеннических схем:

Адресату посылается письмо будто бы от представителя погибшего очень дальнего родственника жертвы. По заверению адресанта, жертве полагается крупное наследство, а для его перевода просят у него либо рассказать всю информацию о его банковском счёте, либо отправить некоторую сумму, чтобы разморозить счёт с наследством.

Жертве сообщается о выигрыше в лотерею или каком-нибудь проводимом розыгрыше. Например, адресату может сообщаться о выигранном новом смартфоне, могут даже высылаться

фотографии выигранного товара, что ещё больше подогревает интерес жертвы. Но для пересылки выигрыша требуется либо заплатить налог, либо произвести оплату посылки в город жертвы.

Высылаются письма об очень выгодной вакансии где-нибудь за рубежом, но для трудоустройства первоначально необходимо оплатить счета за визу, разрешения на проживание и работу.

В социальных сетях могут приходить письма, где якобы африканская девушка или парень, в зависимости от пола жертвы, которая представляется принцессой небольшого государства или наследницей крупного состояния. Она сообщает, что находится в лагере беженцев в другой африканской стране, из-за того, что на её родине произошел переворот. Девушка предлагает на ней жениться и унаследовать всё её состояние, но для этого ей нужны деньги, чтобы вернуться на родину, когда обстановка в стране стабилизируется.

Стоит отметить, что некоторые пользователи, понимая, что их хотят обмануть, отвечают мошенникам из любопытства, интересуясь, что им могут предложить и как будут пытаться обманывать. Однако, этого делать не стоит. Причиной этого является то, что когда адресат отвечает на такое сообщение, то автоматически заносит себя в базу данных мошенников. Это может обернуться, как минимум, засоренной почтой, а, как максимум, на компьютер жертвы может выслаться опасный вирус, после чего не составит труда получить доступ к личным данным пользователя[5].

Кибервымогательство — вымогательство с использованием интернета. Как правило, при таком способе вымогательства пользователь получает сообщение, в котором говорится, что злоумышленники получили личную информацию и угрожают выложить её в открытый доступ.

Хаккеры могут проводить кибератаки на различные серверы и компании, при этом условием неразглашения украденной ими информации является перевод денежных средств на указанный счёт.

Кибервымогательство связано с наличием прямых или косвенных угроз вторжения в личную жизнь, кражи личных данных, которые могут содержать информацию о переписке в социальных сетях, голосовых сообщений, данных используемых приложений, историю браузера и поисковых запросов, а также удалённый доступ к рабочему столу персонального компьютера и многое другое. Все эти действия способны нанести существенный моральный вред потенциальной жертве.

В случае с несогласием выдвинутых требований, злоумышленники угрожают распространением личных фотографий дискредитирующего характера и других данных, относящихся к частной жизни, что может привести к разрушению прав человека, нарушению деловой репутации, а также привести к эмоциональному стрессу и другим видам морального вреда.

Преступники используют ряд различных схем и программ с целью вымогательства. Также злоумышленники могут использовать шифрование данных с целью вымогательства денег за выдачу ключей расшифровки. Вирусы, запущенные вымогателем, шифруют данные на компьютере пользователя, из-за чего эти данные перестают быть доступными для пользователя, и требуют выкуп за возможность восстановить доступ к ним. Проникнув в корпоративную сеть, вымогатели способны блокировать сразу большое количество компьютеров пользователей данной компании. При отказе от уплаты выкупа, зашифрованные данные могут остаться недоступными для пострадавшего навсегда[6].

Взлом социальных сетей и дальнейшее вымогательство денег — один из самых распространенных и часто встречающихся способов мошенничества. Такая популярность данного метода вытекает из ненадёжности большинства социальных сетей — их очень легко взломать. При этом, необязательно быть специалистом в области информационных технологий. На просторах интернета есть куча информации, как взломать ту или иную социальную сеть, поэтому справиться с этой задачей может даже абсолютно неподготовленный человек, никак не связанный с хакерством.

Войдя в чужой аккаунт, злоумышленник для разных целей, например, кража личной информации, переписок и дальнейший шантаж жертвы. Однако наиболее популярным преступлением является рассылка “друзьям” пользователя сообщений с просьбой о долге.

Злоумышленник, зайдя в чужой профиль, пишет друзьям жертвы, якобы у него закончились деньги, и просит одолжить некоторою сумму денежных средств до определенного срока. Если жертва соглашается помочь, то мошенник либо просит предоставить данные банковских реквизитов, либо присылает номер счёта, на который нужно перевести необходимую денежную сумму.

При пользовании новейшими информационными технологиями необходимо осознавать риски, которые могут возникать при их эксплуатации. Прежде всего это угроза утечки конфиденциальных данных, а также заражение устройства вредоносными программами. Чаще всего это происходит из-за установки на устройство вредоносного программного обеспечения,

целенаправленных действий злоумышленника или неосторожности и несоблюдении правил безопасности личных данных.

В наши дни люди часто хранят всю свою личную информацию на компьютерах и телефонах. Если пользователь устанавливает на своё устройство вредоносное ПО, это может привести к обширной утечке данных и многим другим последствиям, например, краже персональных данных.

Кража персональных данных зачастую происходит с целью дальнейшей подмены личности или же кражи финансовой личности. При данном виде кражи преступник выдаёт чужую личность за свою в финансовых целях. Это может быть взятие кредита на чужое имя, осуществление покупок в интернет-магазинах или же получение информации о медицинском и финансовом положении жертвы.

Другой формой вторжения в личную жизнь с помощью информационных технологий может стать шпионаж. Шпионаж может проявляться по-разному: от взлома устройств пользователя и прочтению его личных данных и переписок, вплоть до полноценной слежки и нелегального отслеживания всей жизни жертвы.

Преступники используют различные методы хищения данных, наиболее популярные методы представлены ниже:

Отслеживание нажатия клавиш. За отслеживание отвечают специальные программы, которые определяют, какие комбинации клавиш пользователь использует чаще всего. Данный способ обычно используется для выявления паролей от банковских счетов и других сервисов.

Подбор паролей. Если преступникам известна некоторая личная информация о пользователе, например имя, фамилия, год рождения и тому подобное, то они могут попытаться подобрать пароль исходя из этих знаний, используя разные комбинации таких данных в качестве пароля. Данный способ является наиболее простым и лёгким, но при этом срабатывает крайне редко, так как очень малое количество людей используют личную информацию в качестве пароля от чего-либо. Тем не менее, такие люди встречаются, и мошенники могут использовать этот факт.

Backdoor программы — программы, позволяющие преступникам входить в систему компьютера пользователя или выходить из нее. Такие программы помогают злоумышленникам удаленно контролировать деятельность пользователя, а также просматривать личную информацию, в том числе пароли.

Обман сети. Злоумышленники могут создавать ложные сети, например Wi-Fi. Правонарушитель может ждать свою жертву в общественном месте, где создаст сеть с названием этого места. Когда пользователь подключится к такой сети, то преступник сможет отслеживать его действия в интернете, а также просматривать файлы вашего устройства или даже установить на него вирус или другую зловредную программу.

Сейчас абсолютно любой человек может стать жертвой киберпреступников, хотя многим до сих пор сложно представить, что кто-то может всерьёз интересоваться их личными данными, кому-то может быть интересно и важно всё знать об их личности и даже шпионить за ними. Из-за этого многие люди могут не использовать все меры предосторожности при использовании современных информационных технологий[7].

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей. Преступления на почве ненависти по отношению к личности или группе людей обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности сексуальной ориентации и других признаков.

Примерами таких киберпреступлений являются домогательства и рассылка оскорбительных сообщений, и распространение ложных новостей, касающихся определенной группы лиц. Анонимность и легкодоступность интернета серьезно затрудняют борьбу с преступлениями на почве ненависти.

Группировки экстремистской и террористической направленности все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесенияя вреда IT-инфраструктурам.

Зачастую объектами таких киберпреступлений могут стать крупные корпорации или даже целые государства.

Примером атаки на крупную корпорацию может стать взлом одной из самой популярной социальной сети мира Facebook в 2020 году. В результате хакерской атаки, в сеть утекли данные более чем 260 миллионов пользователей. После таких утечек суд обязал компании выплатить штраф в размере 5 миллиардов долларов, что является крупнейшим штрафом за утечки данных в истории.

Если говорить о преступлениях в отношении целого государства, то примером является взлом и получение доступа к 269 Гб секретных данных правоохранительных органов и спецслужб Соединенных Штатов Америки группировкой хакеров Anonymous. Среди этих данных содержались

видеоролики, электронные письма, документы по планированию и разведке за последние 5 лет. Из-за произошедшего в стране разразился громкий скандал. Репутация власти США и, в частности, американских спецслужб сильно пошатнулась[8].

Стоит отметить, что любая размещённая пользователем информация в интернете является публичным высказыванием, даже если информация, размещённая пользователем, не является популярной и её почти никто не просматривает. И при пользовании интернетом обязательно стоит знать и руководствоваться правилами и законами страны, в которой пользователь проживает.

Наиболее часто встречаемым правонарушением в интернате является популяризирование запрещенной информации. При этом не обязательно размещать информацию о чём-то наиболее радикальном. Человека могут привлечь к административной ответственности и за банальные "смешные картинки". Важно, что пользователь может и не быть автором данной статьи в интернете, достаточно просто "оценить" данную статью или оставить свой комментарий под запрещенным материалом. Также необходимо учитывать, что существует понятие как длящееся правонарушение, то есть если пользователь распространял любой запрещённый материал много лет назад, но он до сих пор доступен в сети, то такой пользователь всё равно считается правонарушителем. При этом удаление ранее размещенного контента не всегда помогает, ведь при дальнейшем разбирательстве правоохранители могут руководствоваться обычными скриншотами. Так что единственным способом быть защищённым от данного правонарушения — это хорошо знать, какие темы находятся под запретом и по возможности их избегать.

Далее перечислены темы, за распространение которых предусмотрена уголовная и административная ответственность, согласно уголовному кодексу Республики Беларусь:

– умышленные действия, направленные на возбуждение расовой, национальной, религиозной либо иной социальной вражды или розни по признаку расовой, национальной, религиозной, языковой или иной социальной принадлежности;

– публичные призывы к организации или проведению незаконных собрания, митинга, уличного шествия, демонстрации либо пикетирования, либо привлечение лиц к участию в таких массовых мероприятиях;

– публичные призывы к захвату государственной власти, или насильственному изменению конституционного строя Республики Беларусь, или измене государству, или совершению акта терроризма или диверсии, или осуществлению действий, направленных на нарушение территориальной целостности Республики Беларусь, или совершению иных действий, направленных на причинение вреда национальной безопасности Республики Беларусь, в том числе на применение мер ограничительного характера (санкций) в отношении Республики Беларусь, физических и юридических лиц Республики Беларусь, либо распространение материалов, содержащих такие призывы, при отсутствии признаков более тяжкого преступления;

– умышленное унижение чести и достоинства личности, выраженное в неприличной форме (оскорбление), в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, распространенной в глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования;

– пропаганда или публичное демонстрирование, в том числе с использованием глобальной компьютерной сети Интернет либо иной информационной сети, изготовление, распространение нацистской символики или атрибутики, а равно хранение или приобретение такой символики или атрибутики[9].

Другим правонарушением со стороны обычного пользователя может стать спам — рассылка писем без согласия получателя. Конечно, чаще всего спам — это дело мошенников, которые могут предлагать обычным пользователям различные махинационные схемы или предложения выгодной покупки или заработка, однако спам могут распространять и обычные люди, не видящие ничего противозаконного в своих действиях. Например, если человек устроился работником в какую-нибудь организацию, и посредством массовой рассылки рекламы своим друзьям и знакомым о данной организации пытается повысить её узнаваемость на рынке, то его действия также будут считаться нелегитимными и могут быть осуждены в соответствии с законодотельством путём наложения денежного штрафа.

Очень частым правонарушением с использованием информационных технологий является нарушение авторских прав. В наше время любой человек ежедневно сталкивается с объектами авторского права. Это может быть прослушивание музыки, просмотр фильмов и фотографий, поиск и скачивание файлов в интернете. В таких условиях очень сложно не пересечь ту грань, где использование чужих объектов собственности становится преступлением.

Нарушение авторских прав — это использование, копирование, распространение чужого произведения, либо несоблюдения условий договора по использованию данного объекта. Причём даже такая мелочь, как играющая на фоне музыка в салоне красоты или ресторане может стать нарушением, в случае ее использования без согласия правообладателя. Пользователь может

использовать чужие материалы лишь после получения исключительного права на произведение — право использовать чужие произведения в любой форме. При этом необходимо чётко обговаривать с автором назначение использования. Например, если было получено разрешение публиковать фото в интернете, пользователь не может напечатать его на афише. Если пользователь хочет законно использовать чужие материалы, ему необходимо получить разрешение у автора и указать при этом его имя, так будут соблюдены и права на использование, и личные неимущественные права автора[10].

Как уже стало понятно из описания методов правонарушений в области информационных технологий, данные действия могут нести серьёзную опасность для финансов, конфиденциальности пользователя. Тем очевиднее факт, что необходимо знать способы защиты от киберпреступлений и их предостережения.

Защита от фишинга включает в себя соблюдение нескольких элементарных правил безопасности в интернете.

Необходимо помнить, что ни в коем случае нельзя передавать такие конфиденциальные данные как пин-код банковской карты, пароль электронной почты или аккаунтов в социальных сетях. Ни банк, ни соцсеть никогда не станут запрашивать такого рода данные используя электронную почту.

Если пользователь зашёл на зловредный сайт, на его компьютер может быть выслан опасный вирус. Вирус — это специальная программа, способная самопроизвольно присоединяться к другим программам при запуске последних и выполнять различные нежелательные действия.

Наличие вируса может проявляться следующими способами:

– некоторые программы перестают работать или начинают работать некорректно;

– на экран выводятся посторонние сообщения, сигналы и другие эффекты;

– работа компьютера существенно замедляется;

– структура некоторых файлов оказывается испорченной.

По способу заражения вирусы классифицируют на следующие виды:

– троянские программы, назначением которых, по аналогии с троянским конём, является имитация каких-либо полезных программ, после активации которых программа активируется и выполняет определенные нежелательные действия;

– утилиты скрытого администрирования по интерфейсу и функционалу во многом напоминают системы администрирования компьютера в сети, при инсталяции которых происходит установка на компьютер скрытой системы удаленного управления;

Intended-вирусы — вирусы, которые не могут размножаться или размножаются только один раз, то есть вирусы, которые заразив какой-либо файл, утрачивают способность к дальнейшему размножению.

По деструктивным возможностям выделяют такие виды вирусов:

– неопасные вирусы, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическими или звуковыми эффектами;

– опасные вирусы, которые потенциально могут привести к нарушениям в структуре файлов и сбоям работы компьютера;

– очень опасные вирусы, в алгоритм которого специально заложены процедуры уничтожения данных и возможности обеспечивать быстрый износ движущихся частей механизма компьютера.

Для защиты от вирусов рекомендуется установить на компьютер надёжный антивирус — программы, препятствующей распространению вируса на компьютере пользователя.

Антивирусы разделяют на пять основных групп:

1 Мониторы. Программы мониторы располагаются в оперативной памяти компьютера, перехватывают и сообщают пользователю об обращениях операционной системы, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить и запретить такие обращения. Такие антивирусы могут выявлять даже неизвестные вирусы на ранней стадии заражения.

2 Детекторы — программы, которые проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При её обнаружении выводится соответствующее сообщение.

3 Доктора — программы, восстанавливающие зараженные файлы путём удаления из них тела вируса. Обычно такие программы рассчитаны на конкретные виды вирусов. Такие программы необходимо часто обновлять для получения версий, способных обнаружить новые виды вирусов.

4 Ревизоры анализируют изменение состояния файлов, проверяют состояние загрузочного сектора, а также время атрибуты и время создания файлов. При обнаружении несоответствий, пользователю сообщается об этом.

5 Вакцины модифицируют программы так, что это не отражается на их работе, но вирусы, от которых происходит вакцинация, считаю такие программы уже зараженными.

Также для защиты от фишинга необходимо обращать внимание на дизайн сайтов, на которые переходит пользователь. Если он кажется странным, недоработанным, сделанным на скорую руку, то вполне возможно, что это фишинговый сайт.

Всегда нужно обращать внимание на адресную строку в ссылке перехода — незначительное изменение в электронном адресе может привести абсолютно на другой сайт. Существует возможность дешифровать ссылку с помощью специальных сервисов и посмотреть, на какой сайт она ведет.

При посещении сайтов нужно следить, чтобы было установлено защищенное соединение https://. В адресной строке должен отображаться специальный символ — замок.

Письма с незнакомых номеров, имеющие экстренный характер должны в первую очередь вызывать подозрение. Письма, в которых говориться, что аккаунт пользователя взломан или был получен крупный выигрыш, почти всегда является мошенническим.

Стоит остерегаться заходить в банковские аккаунты через точки доступа общественного интернета, ведь с помощью их преступники могут установить доступ к личным данным пользователя. Безопаснее пользоваться мобильным интернетом или защищенным соединением.

Не стоит игнорировать предупреждения от браузера или социальной сети о переходе на подозрительный сайт. Если браузер советует пользователю не переходить по данной ссылке, то стоит прислушаться.

Чтобы обезопасить себя от утечки платежных данных пользователь должен предпринять следующие действия:

1 Не вводить данные о банковской карте в непроверенных магазинах и вообще постараться предостеречься от любых онлайн-покупок. Оставлять данные о финансовой карте лучше либо на максимально проверенных сервисах, либо вообще нигде.

2 Не пытаться сэкономить деньги там, где это попросту невозможно. Конечно, ситуация, где пользователя могут привлечь как соучастника по делу об отмыве "скарженных" средств, хоть и с довольно малой вероятностью, но все же может стать реальностью. Поэтому лучше отказываться от быстрых и простых способов сэкономить.

3 Необходимо подключить услугу о снятии денежных средств с банковской карты от мобильных банков. Пользователь будет получать уведомления о снятии денежных после каждой проведенной транзакции в интернете. Чем быстрее обнаружится взлом и несанкционированное снятие денег, тем больше будет шансов их вернуть.

4 Всегда нужно оставаться бдительными и не позволять панике или эмоциям влиять на принятые решения. Кардеры, как и прочие киберпреступники, умело пользуются общественной паникой[11].

Чтобы обезопасить себя от того, чтобы быть обманутыми нигерийскими письмами можно порекомендовать следующее:

– не высылать персональные данные или копии каких-либо документов и номера банковских счетов по запросу организаций, в которые пользователь не обращался, или людям, которых до этого никогда не знал;

– если пользователь является участником интернет-форумов, то следует завести для этого отдельную почту с другим паролем;

– пользоваться программами-фильтрами, которые фильтруют информацию, поступающую на почту пользователя, и при получении нигерийских писем рекомендуют владельцу почты такие письма удалять.

Существует несколько способов, чтобы пользователь мог обезопасить себя от шифрования важных данных и дальнейшего шантажа.

В первую очередь, нужно быть осторожным с сообщениями, приходящими на почту или в социальные сети. Чаще всего троянские вирусы с шифровальными программами находятся во вложениях писем или на зараженных сайтах. Поэтому стоит относиться к каждому письму от незнакомого источника как к потенциально опасному.

В связи с тем, что опасность может находиться на каком-либо сайте, то стоит остерегаться незнакомых и подозрительных сайтов. Так, если после клика на баннер появляется совсем не тот ресурс, который ожидался, или сайт выдает предложение загрузить что-нибудь на устройство пользователя, то его с большой вероятностью пытаются заразить.

В процессе использовании какой-либо программы в ней часто находятся уязвимости, которыми пользуются мошенники. Но, как правило, разработчики со временем выпускают обновления, в которых существующие неполадки исправляются. Поэтому люди, которые не обновляют своё программное обеспечение или другие программы рискуют больше тех, кто эти программы регулярно обновляет.

Стоит использовать современные защитные программы, которые способны распознавать и оперативно блокировать программы-шифровальщики. Антивирус анализирует действия запущенных файлов и блокирует попытки шифра какой-либо программы.

Одним из самых действенных решений является резервное копирование данных. Стоит регулярно сохранять важные файлы и документы в облачное хранилище типа диска Google или на внешний жёсткий диск. Стоит отметить, что при копировании информации на резервный жёсткий диск стоит только тогда, когда пользователь что-то копирует или считывает с него. Если он окажется соединен с компьютером во время нападения, то его также зашифруют. Также, при хранении данных на жёстком диске нужно защитить его надёжным паролем, желательно с двухэтапной аутентификацией, это существенно снизит вероятность взлома облачного хранилища пользователя[12].

Список использованных источников:

[1] Информатизация - [Электронный ресурс]. – Режим доступа: http://multilang.pravo.by.

[2] Правонарушения в сфере информационных технологий - [Электронный ресурс]. – Режим доступа: https://www.elibrary. ru/download/elibrary_ 37130233_76877572.pdf.

[3] Фишинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3.

[4] Кардинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D0%B4%D0%B8%D0%BD%D0%B3.

[5] Нигерийские письма - [Электронный ресурс]. – Режим доступа: https://nigeria.mfa.gov.by/ru/letters/.

[6] Кибервымогательство — это вымогательство в интрнете - [Электронный ресурс]. – Режим доступа: https://news.ykt.ru/.

[7] Виды киберпреступлений - [Электронный ресурс]. – Режим доступа: https://internetpolicy.kg/literacymodule/course_2/module1/glava1_2.html.

[8] Десять самых громких атак XXI века - [Электронный ресурс]. – Режим доступа: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

[9] Уголовный кодекс Республики Беларусь - [Электронный ресурс]. – Режим доступа: https://kodeksy-by.com/ugolovnyj_kodeks_rb.

[10] Инструкция: как не нарушить авторские права - [Электронный ресурс]. – Режим доступа: https://www.asi.org.ru/2020/04/23/instruktsiya-avtorskie-prava/.

[11] Что такое кардинг, и как защитишься от взлома, покупая в интернете - [Электронный ресурс]. – Режим доступа: https://trends.rbc. ru/trends/industry/60ae051f9a7947c4dc22101b.

[12] Как защититься от шифровальщиков-вымогателей: 5 советов - [Электронный ресурс]. – Режим доступа: https://www.kaspersky. ru/blog/ransomware-five-tips/31352/.

UDC 004.056.5:34

OFFENSES IN THE SPHERE OF INFORMATION TECHNOLOGIES

Dorozhkin I.V., Sharafanovich Ya.O.

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

Pulko T.A. – PhD in Technical sciences

Annotation

The use of computer and information technologies in various spheres of society is becoming a mandatory attribute to achieve maximum efficiency in this area. In this regard, the field of information technology is becoming increasingly popular for various kinds of scammers and criminals. A significant flow of finance and various personal information passes through information technology. Fraudsters take advantage of this by trying to steal money or personal information of the user in various ways in order to further use it for their own purposes.

This article discusses various sources of threats and types of crimes in the field of information technology. The main conclusions are the precautions that can protect the user from the potential dangers of the activities of offenders.

Keywords

Information technologies, cybercrime, phishing, carding, informatization, computer information, virus, criminal code.

УДК 004.056.53

РИСКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ БГУИР

Матюшкин С.И., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

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

Аннотация. Рассмотрены различные аспекты, связанные с рисками безопасности информационных систем, имеющие место в информационной системе БГУИР. Также приведены возможные варианты снижения рисков информационной безопасности, в частности риска нарушения доступности сетевых ресурсов БГУИР.

Ключевые слова. Информационная безопасность, интегрированная информационная система БГУИР, уязвимости, доступность информационного ресурса.

Обеспечение информационной безопасности информационной системы включает в себя комплекс мер для обеспечения бесперебойной работы и целостности обрабатываемой информации.

Безопасность определяется слабейшим звеном в системе защите. Можно ставить различные антивирусы, закрыть все порты на сервере, но если при этом пользовали ставят пароли типа 123456 или пишут их на бумажке на рабочем столе на ПК, то риски быть взломанным очень высоки. Поэтому фокус внимания всегда должен быть на наиболее слабых на данный момент звеньях.

Экономическое обоснование взлома. Зачем взламывают какую-либо систему? Для получения некой выгоды. И эта выгода может быть не только материальная. Если взлом стоит дешевле этой выгоды, то игра стоит свеч. Задача защиты сделать взлом невыгодным. Необходимо повысить стоимость взлома до такого уровня, чтобы он стал не привлекателен.

Риски взлома информационной системы:

– Утечка данных — будет потеряна конфиденциальность информации;
– Данные могут быть повреждены — информация потеряет целостность;
– Информация может стать недоступна пользователю — потеряна доступность;
– Ресурсы системы могут быть использованы для взлома других систем.

Все меры по безопасности так или иначе направлены на обеспечение конфиденциальности, целостности и доступности информации.

Человеческий фактор в информационной безопасности является самый важным моментом. У человека есть множество соблазнов и уязвимых мест. Кого-то можно подкупить, кого-то запугать, а кто-то может делать, не понимая к каким результатам могут привести его действия.

Более опасен для системы внутренний человек (сотрудник), а не человек с улицы. У него может быть много причин для помощи злоумышленнику: обидели на работе, не дают повышения, «подработка», компромат на него, некомпетентность, банальная глупость и т.д. Имея доступ во внутреннюю часть системы человек становится точкой входа для злоумышленника или сам становится им.

Защита должна соответствовать уровню угроз и модели злоумышленника. Важно представлять себе примерный портрет злоумышленника и его возможности.

Это позволит понять, что может сделать злоумышленник, какие цели преследует (что он сможет получить в случае успешного взлома) и какие варианты атаки он может реализовать.

Непрерывность состояния защищенности. Система безопасности должна работать непрерывно во времени. Необходимо предусмотреть факторы, которые могут прервать непрерывность состояния защищенности: выключили свет, уволился системный администратор, необходимо обновить какое-то программное обеспечение или ключ шифрования.

Подход риск менеджмента — риски информационной безопасности сайта. Информационная безопасность подразумевает работу с рисками, представляющими собой комбинацию вероятности реализации угрозы и критичность актива для бизнеса.

Угрозы информационной безопасности и меры противодействия угрозам безопасности

Первый вопрос — кто злоумышленник, и зачем ему нужно взламывать систему?

Что он получит? Какие возможности для взлома у него есть? Какой бюджет на взлом он может выделить? Понимая эти вопросы, можно адекватно выработать ряд мер защиты.

Основные меры защиты по угрозам для конфиденциальности, целостности и доступности информации на сайте информационной системы БГУИР.

Меры по обеспечению конфиденциальности

Протокол SSL (HTTPS). HTTPS соединение шифрует трафик между браузером и сервером. Это усложняет для злоумышленника получение данных в промежуточных узлах (например, извлечение пароля пользователя при входе). Также SSL дает некую гарантию пользователю, что он взаимодействует именно с нужным сайтом (в браузере отображается принадлежность сертификата).

Защита от разных атак на веб-приложение (XSS, SQL инъекции). Пользователь может ввести некий код через поля форм и этот код может негативно сказаться на работе системе. Например, XSS атака подразумевает ввод JS кода, который сохранится в базе сайта (например, при подаче заявки в систему единой технической поддержки), затем другой пользователь запросит эти данные из базы и этот вредоносный код JS выполнится от имени этого пользователя.

Атака SQL Injection — вводится код SQL, который видоизменяет SQL выполняемый на сервере. Это позволяет вводить прямые команды в БД (например, удалять данные или считывать данные из таблиц). Защита от SQL инъекций — весь код SQL выполнять в хранимых процедурах с параметрами без использования динамически генерируемых процедур.

Обновление программного обеспечения (ПО). Периодически разработчики находят уязвимости в ПО и выпускают обновления. Если не делать обновления, то есть риск, что этой уязвимостью воспользуются злоумышленники. Необходимо проводить профилактику сервера и ПО на нем.

Организационные меры и обучение сотрудников. Можно так построить бизнес-процесс, чтобы снизить вероятность утечки конфиденциальности и целостности.

Второе направление это обучение. Люди должны хорошо знать свой участок и роль в процессах. Что они могут, а что делать нельзя. Знать, какие бывают ситуации и как они должны реагировать на них.

Контроль целостности данных можно реализовывать через скрипты. Данные в системе нужно периодически проверять. Код сайта может содержать ошибки, которые будут приводить к нарушению целостности. В этом случае необходимо создать ряд скриптов, которые будут проверять по бизнес-логике целостность данных в таблицах. Можно запускать подобные скрипты ежедневно для нахождения коллизий в данных, после чего выдавать отчет на почту.

Правильная структура данных в базе данных. Если структура базы данных имеет проблемы, то при частичном обновлении данных может нарушиться целостность данных. Необходимо использовать нормализацию базы данных достаточного уровня, вводить ограничения, устанавливать внешние ключи и т.д.

Так как сайт информационной системы разрабатывался, а не просто был сделан из готовых блоков, то в нем могут быть ошибки. Они могут проявиться в ходе эксплуатации. Необходимо проводить профилактику приложения: анализировать системный журнал и быстродействие, искать проблемные точки. Это сказывается как на качестве системы, так и на состоянии защищенности. В ходе таких обзоров могут быть обнаружены бреши, которые на стадии разработки сайта никак себя не проявляли.

Защита от DOS. DOS атака это организация множества запросов на сайт с целью его перегрузки. Происходит отказ в обслуживании — сервер просто начинает не справляться с возникшей нагрузкой. Следует блокировать подозрительные IP адреса, и сервер просто не будет обрабатывать некоторые запросы. Тут главное не перестараться, т.к. таким образом, можно отсеять реальных пользователей вместе с ботами (программы, заходящие на сайт).

Нагрузочное тестирование. Проводите нагрузочные тесты, находите проблемные места в своем сайте про производительности. То, что хорошо работает на малом объеме, может очень тормозить на больших оборотах.

Резервный сервер. Если основной сервер выйдет из строя, надо иметь возможность быстро восстановить работу приложения на резервном сервере. В идеале сделать работу несколько серверов в связке, чтобы при выходе из строя одного сервера, запросы шли на другой сервер.

Мониторинг доступности и оповещения. Если возникла остановка работы сайта, то необходимо узнать об этом как можно раньше, чтобы сразу принять все меры по восстановлению сайта. Для этого используются средства мониторинга, которые опрашивают сайт. В случае падения они сообщают через e-mail или SMS о проблеме.

Рекомендации по обеспечению информационной безопасности

Для повышения безопасности, рекомендуется использовать сложные пароли, однако такие, которые можно запомнить. Это позволит избежать записывания паролей на бумаге. Например, "Para001medic+" – пароль, состоящий из специальных символов, цифр, символов в верхнем регистре, содержащий более 8 символов. Такой пароль трудно подобрать, но легко запомнить пользователю.

Минимальный доступ и убрать все ненужные элементы. У каждого пользователя должен быть минимальный уровень доступа, достаточный для его работы. Не нужно давать больше, чем ему нужно для выполнения служебных обязанностей. Атаке извне может быть подвергнут любой элемент вашей системы, и чем меньше возможностей у этого элемента, тем лучше.

Закрыть доступ через неиспользуемые порты на сервере. Каждый порт это потенциальная точка входа для злоумышленника.

Обновления. Ставьте обновления своевременно. Заведите регламент работ по обновлению основного ПО.

Инсайдеры. Инсайдер гораздо опаснее внешнего злоумышленника. У него уже есть доступ в системе. К нему есть некоторое доверие со стороны других людей в системе. Он может долгое время незаметно пакостить в системе. Создайте условия для максимальной удовлетворенности людей в системе, со всеми расставайтесь полюбовно, не оставляя долгов перед другими (особенно перед программистами и системными администраторами).

Используйте основы риск менеджмента. Проводите пересмотр рисков и мер по уменьшению критичности и вероятности возникновения риска.

Не публикуйте в общий доступ лишней информации. Внешний злоумышленник собирает информацию сначала из открытых источников. По крупицам ищет уязвимости системы, изучает структуру системы и возможные точки входа в него.

Не публикуйте в общий доступ информацию, чувствительную ко взлому. Тем самым вы уменьшите вероятность взлома внешним злоумышленником.

На рабочих станциях, тем более на серверах, не должно быть ненужного ПО. Любое дополнительное ПО приносит потенциальную возможность получить вирус или другую вредоносную программу.

Уязвимости в ПО также могут быть точкой входа в систему. Поэтому ставьте приложения только из проверенных источников и давайте этим приложениям минимум необходимых прав. Не следует доверять введенным пользовательским данным. Когда сайт обрабатывает запрос от браузера, нельзя доверять введенным данным от пользователя.

Ежедневно должны создаваться резервные копии. Их нужно копировать на удаленное хранилище.

Нет смысла описывать угрозы, считать риски без проведения работ по повышению уровня защищенности. Реализовывать эти работы можно в виде регламентов обслуживания системы — т.е. это совокупность неких периодических действий, направленных на реализацию мер по обеспечению безопасности.

Регламент обслуживания сервера. Выполняет системный администратор, проверяет критичные параметры сервера (память, место на диске, процессор), изучает системные журналы, проводит обновление ПО, смотрит за резервными копиями.

Плановое обновление паролей. Вы можете проводить процедуру изменения пароля для важных точек входа — соединение с базой данных, доступ к хостинг-панелям, доступ к серверу и т.д.

Регламент пересмотра состава угроз и соответствующих мер (риск менеджмент). Хотя бы раз в полгода имеет смысл возвращаться к рискам информационной безопасности и заново проводить анализ рисков,

Интегрированная информационная система (ИИС) «БГУИР: Университет» ориентирована на автоматизацию учебных процессов и облегчение взаимодействия сотрудников и студентов БГУИР. Использование ИИС позволяет упростить учет информации о студентах, учебных группах, учебных планах специальностей. При обеспечении работоспособности и защищенности ИИС БГУИР необходимо учитывать все описанные выше меры безопасности. Однако, наиболее частыми проблемами, с которыми приходится иметь дело при эксплуатации интегрированной информационной системы БГУИР это перебои электропитания и попытки взлома из сети Интернет, что вызывает нарушение доступности информационных сервисов БГУИР.

Предложен способ повышения доступности за счет обеспечения бесперебойности электропитания серверного и сетевого оборудования.

Серверное оборудование предусматривает возможность установки двойного питания (2 блока питания в сервере). Установив по два блока питания в серверы, можно обеспечить подачу электропитания из двух источников. Так как здания запитываются от трехфазной сети, то подача питания с двух разных фаз через источники бесперебойного питания обеспечит:

1. Устойчивость к перебоям электропитания по любой из используемых фаз, что является наиболее частым случаем.

2. Увеличит вдвое время работы от источников электропитания.

3. Создаст запас времени для развертывания, запуска и переключения питания на дизель-генератор вместо одной из линий питания при отключении электроэнергии на всех линиях, сохраняя возможность автоматического переключения на вторую линию при восстановлении снабжения.

Сетевое оборудование имеет свои источники бесперебойного питания, но не имеет возможности двойного питания и запитывается от местных линий энергоснабжения. Для обеспечения возможности переключения сетевого оборудования на резервный дизель-генератор или другую линию энергоснабжения, необходимо сделать для них отдельную сеть электропроводки, которая будет запитываться в серверной комнате.

Список использованных источников:

1. Как защитить сайт? Обеспечение информационной безопасности сайта / Р.Ш. Раянов // https://falconspace.ru/blog/kak-zashchitit-sayt--obespechenie-informacionnoy-bezopasnosti-sayta

2. Обзор методов защиты корпоративной информации / Алексей Парфентьев // https://lib.itsec.ru/articles2/Inf_security/obzor-metodov-zaschity-korporativnoy-informatsii

3. Кейсы, реальные истории из практики клиентов / searchinform // https://searchinform.ru/cases/

4. Как обезопасить свой веб-сайт? / VDSina.ru // https://habr.com/ru/companies/vdsina/articles/503772/

5. Анализ и оценка информационной безопасности / Региональные системы // https://www.ec-rs.ru/blog/informacionnaja-bezopasnost/analiz-i-otsenka-informatsionnoy-bezopasnosti/?ysclid=lgc8qpmgur833212051

UDC 004.056.53

SECURITY RISKS OF THE BSUIR INFORMATION SYSTEM

Matyushkin S.I.

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

Petrov S.N. – PhD, associate professor

Annotation. Various aspects related to the security risks of information systems that take place in the BSUIR information system are considered. Possible options for reducing information security risks, in particular the risk of disruption of the availability of BSUIR network resources, are also presented.

Keywords. Information security, integrated BSUIR information system, vulnerabilities, availability of an information resource.

УДК 004.056.5

ШАБЛОНЫ ДЕТЕКТИРОВАНИЯ И КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПРАКТИК MITRE ATT&CK

Солонович Т.И., студентка гр.961402

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Петров С.Н. – доцент кафедры ЗИ

Аннотация. Обеспечение информационной безопасности – одна из главных целей крупных организаций, осуществляющих хранение и обработку персональных данных. Для реализации перед сотрудниками стоят задачи проведения комплекса мероприятий по защите информации и IT-инфраструктуры предприятия. Существует большой спектр программных комплексов, которые предоставляют оптимальные инструменты для управления информационной безопасностью. Для корректного использования необходимо понимать принципы реализаций атак, пути их распространения, техники и тактики, используемые злоумышленниками. Методология MITRE ATT&CK содержит вышеперечисленную информацию, опираясь на которую, можно формировать и обрабатывать инциденты информационной безопасности. Их грамотная аналитика позволит снизить риски утечки информации, проникновения вредоносного программного обеспечения в корпоративную сеть или компрометации учетных данных сотрудников организации.

Ключевые слова. Информационная безопасность, SOC, риск, уязвимость, ERP, SGRC, IRP, SOAR, SIEM, ядро, коллектор, коррелятор, хранилище, инцидент, реагирование, анализ, правило корреляции, MITRE ATT&CK, тактика, техника, событие информационной безопасности, аутентификация.

В настоящее время наиболее актуальной практикой в сфере обеспечения информационной безопасности является организация Security Operation Center (далее SOC) [1].

SOC, или центр мониторинга информационной безопасности, – это команда квалифицированных специалистов в направлении кибербезопасности, которая занимается круглосуточным мониторингом состояния IT-инфраструктуры организации. Анализ событий и инцидентов позволяет снизить риски сбоев функционирования систем обеспечения безопасности, предотвратить угрозы и различного рода мошеннические действия (например, мошеннические действия в каналах дистанционного банковского обслуживания).

Для корректной аналитики нотификаций о потенциальных уязвимостях и фильтрации ложных инцидентов, а также реализации прочих задач, SOC должен включать множество программных решений.

Сюда можно отнести EDR (Endpoint Detection & Response) – класс решений для обнаружения и изучения вредоносной активности на оконечных устройствах: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее.

Системы SOAR (Security Orchestration, Automation and Response) предназначены для оркестровки систем безопасности, их координации и управления ими. Threat Intelligence предоставляет информацию об актуальных угрозах, что позволяет организациям изучить цели, тактики, векторы атак и инструменты злоумышленников для выстраивания эффективной стратегии защиты.

SGRC (Security Governance, Risk Management and Compliance) обеспечивает управление информационной безопасностью на основе рассмотрения вопроса информационной безопасности на высшем уровне руководства организации (Governance), управления рисками (Risk), а также в соответствии с требованиями различных нормативных документов (Compliance).

IRP (Incident Response Platform, «платформа реагирования на инциденты») является программным продуктом, предназначенным для автоматизации реагирования на киберинциденты. Данная функция реализуется посредством составления сценариев (плейбуков) с последовательностью стандартных действия при возникновении угрозы информационной безопасности для дальнейшего автоматического выполнения, что позволяет оптимизировать процесс реагирования.

Однако, одним из главных программных решений, используемых для построения SOC, является система обработки логов Security Information and Event Management (далее SIEM).

SIEM система [2] позволяет получать события из различных источников с помощью агентов, отправлять их в хранилище, обрабатывать через шаблоны детектирования и корреляции, также анализировать инциденты в режиме реального времени и обеспечивать оперативное реагирование.

Примерами таких решений являются системы MaxPatrol SIEM (Positive Technologies), Argsight SIEM (Micro Focus), Kaspersky Unified Monitoring and Analisys (Kaspersky).

Архитектурно программа имеет ядро (для управления настройками компонентов системы), коллекторы (для получения событий из источников, парсинг, нормализацию, фильтрацию, агрегацию), хранилище (для регистрации нормализованных событий и оповещений) и корреляторы (для анализа нормализованных событий и создания оповещений в соответствии с правилами корреляции). Архитектура SIEM системы представлена на рисунке 1.

Рисунок 1 – Архитектурное представление SIEM системы

SIEM система ежедневно генерирует большое количество уведомлений и чем больше организация, тем больше этот поток. В данном случае, колоссальный переизбыток информации может привести к тому, что многие из них могут игнорироваться. Во избежание этого информация должна корректно обработана и передана аналитикам для детального разбора.

Правила корреляции позволяют коррелировать события и формировать оповещения аналитикам SOC для анализа и оперативного принятия мер по предотвращению развития угрозы. Они составляются на основе методологий и тактик MITRE ATT&CK [3]. Данная база знаний содержит техники, которыми зачастую пользуются злоумышленники, описание и категоризацию их действий, а также ряд вредоносного инструментария, тем самым позволяя решать ряд задач информационной безопасности, в том числе расследовать киберинциденты.

Необходимо понимать, какие тактики и техники используются хакерами при выполнении атак и как они могут быть обнаружены. На основе базы знаний MITRE ATT&CK можно составить список типичных событий, которые могут указывать на наличие атаки или нарушения безопасности в системе. После того, как определены типичные события, необходимо определить, какие из них могут быть коррелированы друг с другом. Например, возможно, что событие блокировки учетной записи пользователя может быть связано с другим событием, указывающим на подозрительную активность в этой учетной записи.

Угрозы описаны принципом набора TTP, который расшифровывается как Tactics-Technique-Procedure (или Тактика-Техника-Процедура). Под тактикой понимается то, как злоумышленник действует на разных этапах своей операции, какая цель или задача злоумышленника на определенным шаге. Техника включает информацию о том, как злоумышленник достигает цели или поставленной задачи, какие использует инструменты, технологии, код, эксплоиты, утилиты. Процедура – действия, по выполнению этой техники выполняется и ее целевое назначение.

Каждая из матриц отражает техники определенного этапа атаки и ее нацеленность:

1 PRE-ATT&CK – TTP, отражённые в данной матрице, используются злоумышленниками непосредственно на стадии подготовки к атаке, например, сканирование, инвентаризация сети или социальная инженерия;

2 Enterprise – данная матрица отражает TTP, которые используются для атак на организации;

3 Mobile – TTP, связанные с переносными устройствами;

4 ATT&CK for ICS – включает в себя TTP, направленные на индустриальные системы.

Так, аномалии аутентификации можно отследить по правилам корреляции, опираясь на тактику TA0008 Lateral Movement. На основании техники T1078 Valid Accounts и анализа риска M1026 Privileged Account Management, можно составить правило реагирования на интерактивный вход под привилегированной учётной записью для операционной системы Windows, механизм которого позволит обнаружить вход как с использованием клавиатуры, так удаленные подключения по протоколу RDP. Для этого необходимо настроить фильтр на события типа 4624, со значениями типа входа Logon Type 2 (пользователь успешно вошел в систему на данном компьютере), 10 (пользователь выполнил вход в систему на этом компьютере через службы терминалов или удаленного рабочего стола.) и 11 (пользователь выполнил вход в систему на этом компьютере с сетевыми учетными данными, которые хранились локально на компьютере. Контроллер домена не использовался для проверки учетных данных.). Для корректной работы правила должен быть привязан список привилегированных учетных записей и признак, по которому их можно распознать. Одним из таких признаков может быть значения поля имени пользователя, которое содержит, например, символы “svc” (от “service”), “sa” (от “service account”), “adm” (от “admin”).

Таким образом, опираясь на конкретную тактику TA0008 Lateral Movement было смоделировано правило, которое генерирует оповещения в SIEM системе при наличии событий формата, отраженного на рисунке 2. Оперативный анализ оповещений и реагирование позволит предупредить намеренные вредоносные действия, произведенные под привилегированными учетными данными.

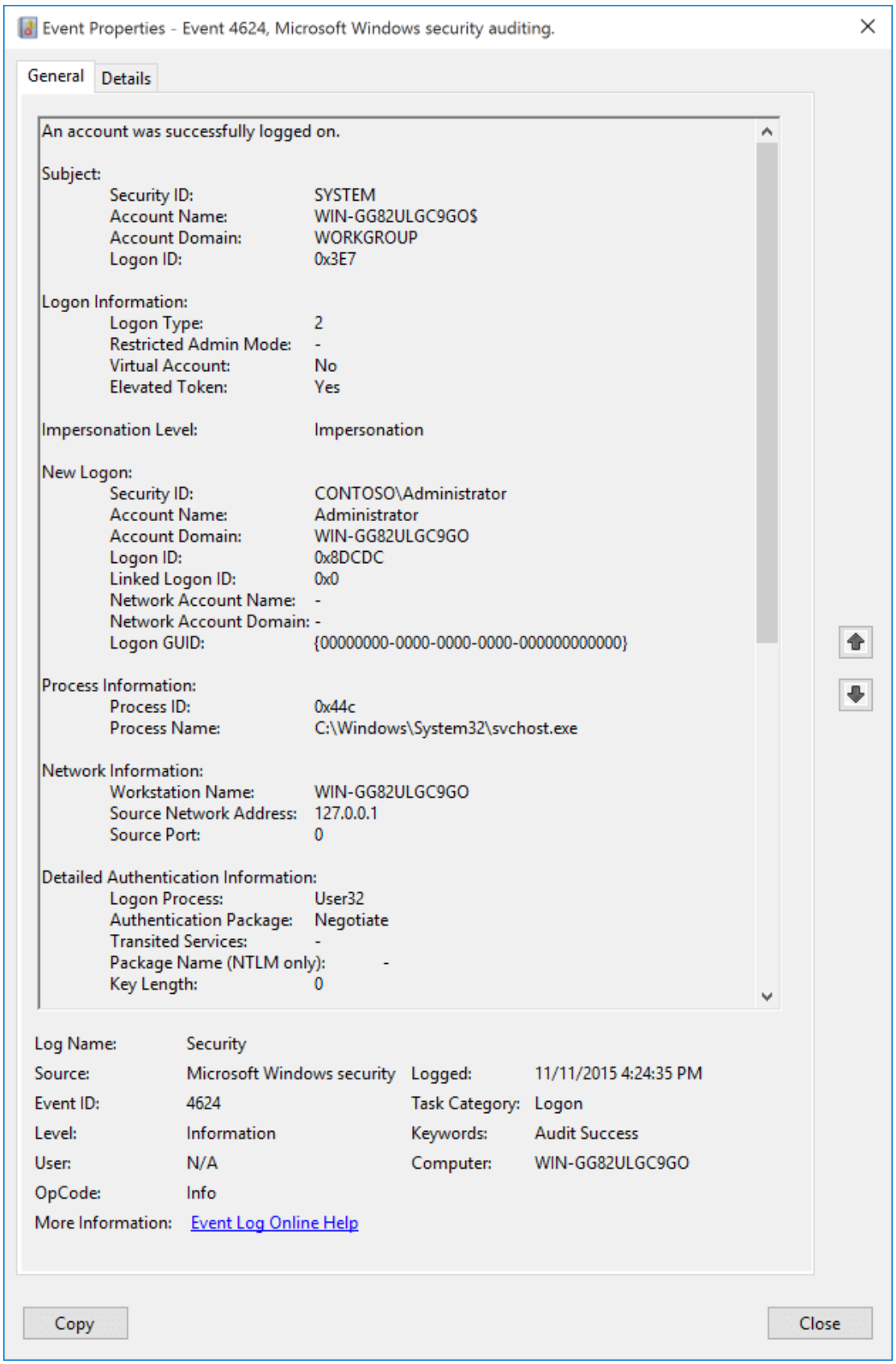


Рисунок 2 – Событие интерактивного входа под привилегированной учетной записью

Методология MITRE ATT&CK позволяет формировать пути реализации и вектор атаки, использовать наборы TTP при моделировании угроз и на основании этого формировать правила

обработки логов, связанных с доступом к учетным записям, обходом защитных мер, повышением привилегий, запуском исполняемых файлов и скриптов, сканированием и сбором данных сети.

Созданные шаблоны мониторинга на основе MITRE ATT&CK могут быть дополнены, тестированы и обновлены со временем, учитывая новые тактики, техники и IOC, появляющиеся в киберугрозах. Регулярное тестирование эффективности шаблонов и их обновление может помочь. Мониторинг реального времени может помочь определить, какие события коррелируются, и какие могут потенциально приводить к ложным срабатываниям.

Список использованных источников:

1. Security Operation Center [Электронный ресурс]. – https://www.securityvision.ru/blog/soc-chto-eto/. – Дата доступа: 0104.2023
2. SIEM система [Электронный ресурс]. – https://encyclopedia.kaspersky.ru/glossary/siem/. – Дата доступа: 01.04.2023
3. MITTRE ATT&CK [Электронный ресурс]. – https://attack.mitre.org/. – Дата доступа: 01.04.2023

UDC 004.056.5

PATTERNS OF DETECTION AND CORRELATION OF INFORMATION SECURITY EVENTS BASED ON MITRE ATT&CK PRACTICES

Solonovich T.I., student gr.961402

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

Petrov S.N. – PhD, associate professor

Annotation. Ensuring information security is one of the main goals of large organizations that store and process personal data. For implementation, employees are faced with the task of carrying out a set of measures to protect information and IT infrastructure of the enterprise. There is a wide range of software systems that provide optimal tools for information security management. For correct use, it is necessary to understand the principles of attack implementations, ways of their distribution, techniques and tactics used by attackers. The MITRE ATT&CK methodology contains the above information, based on which it is possible to generate and process information security incidents. Their competent analytics will reduce the risks of information leakage, penetration of malicious software into the corporate network or compromising the credentials of employees of the organization.

Keywords. Information security, SOC, Risk, Vulnerability, ERP, SRC, IP, STAR, SIM, Core, Collector, Correlator, Storage, Incident, response, analysis, correlation rule, MITRE ATT&CK, Tactics, Technique, Information security event, authentication.

УДК 004.056.53

ВОЗМОЖНОСТИ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ DDOS АТАК

Шаронова Е. И., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Петров С. Н.. – канд. техн. наук

Аннотация. Показаны возможности методов машинного обучения для обнаружения признаков атак типа DDoS.

Ключевые слова. Машинное обучение, ботнет, DDoS-атака, нейронные сети, сетевой поток, датасет, библиотеки машинного обучения.

DDos-атаки нацелены на сайты и онлайн-сервисы. Смысл такой атаки заключается в том, чтобы заблокировать сеть или сервер чрезмерным трафиком. Эффективность достигается за счет использования нескольких скомпрометированных систем в качестве источников атакующего трафика. DDoS-атаки делятся на различные подкатегории в зависимости от уровня сетевого подключения, которое они пытаются атаковать (согласно модели OSI). Выделяют следующие категории: SYN Flood, UDP Flood, MSSQL, LDAP, Portmap и т.п.

Использование нейронных сетей для детектирования DDoS-атак (атак распределенного отказа в обслуживании) является одним из подходов в области кибербезопасности, который может помочь в выявлении подозрительной активности, связанной с DDoS-атаками. Ниже приведены основные шаги, связанные с использованием нейронных сетей для детектирования DDoS-атак [1].

Подготовка данных: Для тренировки нейронной сети необходимо иметь подготовленный набор данных, содержащий размеченные примеры DDoS-атак и нормальной сетевой активности. Этот набор данных будет использоваться для обучения нейронной сети, чтобы она могла "научиться" распознавать характерные признаки DDoS-атак [2].

Выбор архитектуры нейронной сети: В зависимости от конкретной задачи и объема данных можно выбрать подходящую архитектуру нейронной сети. Например, сверточные нейронные сети (Convolutional Neural Networks, CNN) могут быть эффективны для анализа сетевого трафика, а рекуррентные нейронные сети (Recurrent Neural Networks, RNN) могут быть полезны для анализа последовательностей событий.

Обучение нейронной сети: Набор данных с размеченными примерами DDoS-атак и нормальной сетевой активности используется для обучения нейронной сети. Нейронная сеть "изучает" характерные признаки DDoS-атак на основе предоставленных данных.

Тестирование и настройка нейронной сети: После обучения нейронной сети необходимо протестировать ее на отдельном наборе данных, который не был использован в процессе обучения. Это поможет оценить точность и эффективность нейронной сети и внести дополнительные настройки при необходимости [3].

Интеграция в систему обнаружения атак: После успешного тестирования и настройки нейронной сети ее можно интегрировать в систему обнаружения атак, такую как система SIEM (Security Information and Event Management), для автоматического обнаружения DDoS-атак в реальном времени [4].

Рассмотрим более подробно некоторые пункты этого списка.

Для обучения нейронных сетей на обнаружение DDoS-атак необходимо использовать подготовленные датасеты, содержащие размеченные примеры DDoS-атак и нормальной сетевой активности. Ниже приведены некоторые из популярных датасетов, которые можно использовать для этой цели:

DARPA Intrusion Detection Data Sets: Датасеты, предоставленные DARPA (Defense Advanced Research Projects Agency), включают большой объем данных с размеченными примерами различных типов атак, включая DDoS-атаки. Эти датасеты широко используются в исследованиях в области кибербезопасности и могут быть полезны для обучения нейронных сетей на обнаружение DDoS-атак.

CICDDoS2019: Датасет CICDDoS2019, разработанный в Канадском институте компьютерных исследований (Canadian Institute for Cybersecurity), содержит данные о сетевом трафике, сгенерированном DDoS-атаками разных типов, а также нормальной сетевой активности.

UNSW-NB15: Датасет UNSW-NB15, разработанный в Университете Нового Южного Уэльса (University of New South Wales), включает данные о сетевом трафике с размеченными примерами атак, включая DDoS-атаки.

А также UNSW_NB15 [5], Kitsune Network Attack, Network Intrusion Detection [6].

Это лишь некоторые из возможных датасетов, которые можно использовать для обучения нейронных сетей на обнаружение DDoS-атак. Важно выбирать подходящий датасет в зависимости от конкретных требований и целей исследования.

Выбор архитектуры нейронной сети для обнаружения DDoS-атак зависит от множества факторов, таких как доступность данных, требования к производительности, предполагаемые типы DDoS-атак и другие особенности конкретной задачи. Вот несколько распространенных архитектур нейронных сетей, которые могут быть использованы для обнаружения DDoS-атак:

Сверточные нейронные сети (Convolutional Neural Networks, CNNs) широко применяются в обработке изображений, но также могут быть использованы для обработки сетевого трафика, включая обнаружение DDoS-атак. Они могут автоматически извлекать важные признаки из входных данных, таких как пакеты или сетевые потоки, и использовать их для классификации на атаки или нормальную активность.

Рекуррентные нейронные сети (Recurrent Neural Networks, RNNs) подходят для анализа последовательных данных, таких как сетевой трафик, и могут быть использованы для обнаружения DDoS-атак, учитывая последовательную природу сетевого трафика. Например, LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit) – это популярные типы RNN, которые могут быть использованы для обработки временных рядов, включая сетевой трафик.

Автоэнкодеры (Autoencoders) это нейронные сети, которые могут быть использованы для извлечения важных признаков из входных данных и их реконструкции. Они могут быть использованы для обнаружения аномалий, включая DDoS-атаки, путем обучения на нормальной активности и выявления отклонений от нее.

Сочетание различных архитектур: В ряде случаев, комбинирование нескольких типов нейронных сетей может привести к лучшим результатам. Например, сочетание CNN и RNN может учитывать как пространственные, так и временные признаки сетевого трафика.

Также используются глубокие ансамбли (Deep Ensembles): Это архитектуры, состоящие из нескольких нейронных сетей, которые обучаются вместе. Они могут использоваться для повышения точности и устойчивости модели на обнаружение атак.

Важно проводить эксперименты с различными архитектурами и настраивать их параметры для конкретной задачи обнаружения DDoS-атак, чтобы достичь наилучших результатов.

Обнаружение IoT-трафика, используемого для DDoS-атак, является важной задачей в области кибербезопасности. Для решения этой задачи можно использовать различные методы, включая машинное обучение и анализ трафика. Один из подходов заключается в использовании алгоритмов машинного обучения, таких как классификация на основе дерева решений или нейронные сети, для обнаружения аномалий в трафике. Для этого необходимо собрать достаточное количество данных о трафике IoT-устройств и обучить модель на этом наборе данных. Другой подход заключается в анализе самого трафика с использованием методов, таких как анализ частоты и длительности пакетов, анализ наборов данных, таких как размер пакета, время задержки и количество пакетов в секунду, и другие методы. Эти методы могут быть использованы для определения аномалий в трафике IoT-устройств. Также можно использовать комбинацию методов машинного обучения и анализа трафика для обнаружения DDoS-атак, использующих IoT-устройства.

Для обнаружения IoT DDoS-трафика можно использовать различные датасеты, содержащие записи трафика, собранные в реальных условиях. Некоторые из популярных датасетов для обнаружения IoT DDoS-трафика включают:

IoT-23 – датасет, разработанный на основе DDoS-атак на устройства Интернета вещей (IoT) в реальных сетях. Он содержит записи трафика с 23 различных устройств IoT, включая камеры видеонаблюдения, медиаплееры, маршрутизаторы, принтеры и другие, и включает различные типы DDoS-атак [7].

Android Mischief Dataset – набор данных сетевого трафика с мобильных телефонов, зараженных троянами удаленного доступа Android [8].

Для обучения моделей распознавать DDoS атаки можно использовать различные языки программирования и фреймворки, в зависимости от предпочтений и требований проекта. Некоторые из популярных языков программирования и фреймворков для обучения моделей на обнаружение DDoS атак включают:

Python – является одним из наиболее популярных языков программирования для машинного обучения и имеет множество библиотек и фреймворков, таких как TensorFlow, Keras, PyTorch, scikit-learn, которые предоставляют мощные инструменты для создания и обучения моделей машинного обучения для обнаружения DDoS атак.

R – язык программирования и окружение для статистической обработки данных, который также может быть использован для обучения моделей машинного обучения. R предоставляет богатый набор библиотек, таких как caret, randomForest, xgboost и другие, которые могут быть использованы для создания моделей обнаружения DDoS атак.

TensorFlow – открытая библиотека машинного обучения, разработанная Google, которая предоставляет мощные инструменты для создания и обучения моделей машинного обучения, включая обнаружение DDoS атак. TensorFlow имеет широкий выбор предварительно обученных моделей и также позволяет создавать собственные модели с использованием глубоких нейронных сетей.

Scikit-learn – библиотека машинного обучения для языка программирования Python, которая предоставляет множество алгоритмов машинного обучения, таких как Decision Trees, Random Forest, SVM, и другие, которые могут быть использованы для создания моделей обнаружения DDoS атак.

Keras – высокоуровневый фреймворк машинного обучения для Python, который предоставляет простой и интуитивно понятный интерфейс для созд

PyTorch – фреймворк машинного обучения, разработанный Facebook, и также имеет множество инструментов и библиотек для обучения моделей на данных о DDoS атаках.

Машинное обучение используется для обнаружения DDoS атак во многих продуктах, включая:

– SIEM системы (Security Information and Event Management)
– Системы обнаружения вторжений (Intrusion Detection Systems)
– Системы защиты от DDoS атак (DDoS Protection Systems)
– Брандмауэры и системы безопасности сети
– Кластеры веб-серверов
– CDN (Content Delivery Network)

В этих продуктах используются различные методы машинного обучения, включая классические алгоритмы, такие как машины опорных векторов (SVM) и наивные байесовские классификаторы, а также более сложные алгоритмы, такие как глубокие нейронные сети и алгоритмы кластеризации данных.

Системы обнаружения вторжений (Intrusion Detection Systems, IDS) могут использовать машинное обучение для обнаружения DDoS атак, анализируя сетевой трафик или лог-файлы на наличие аномального поведения или характеристик, связанных с DDoS атаками. Системы облачной безопасности (Cloud Security) могут использовать машинное обучение для обнаружения DDoS атак, анализируя сетевой трафик и активность в облачной среде на предмет аномалий и признаков DDoS атак. Системы анализа журналов и лог-файлов (Log Analysis Systems) могут использовать машинное обучение для обнаружения DDoS атак, анализируя лог-файлы на наличие аномальных событий, включая признаки DDoS атак. Специализированные продукты для обнаружения DDoS атак разработанные специально для обнаружения DDoS атак с использованием машинного обучения, такие как Radware DefensePro, Arbor Networks APS, F5 Networks Silverline.

Сделаем краткое обобщение изложенных выше фактов.

Машинное обучение широко используется для обнаружения DDoS атак в различных продуктах и системах. Наиболее распространенными языками программирования и фреймворками для обучения моделей являются Python, TensorFlow, Keras, PyTorch и scikit-learn. В качестве датасетов используются как синтетические данные, так и данные с реальных атак. Для обнаружения IoT-сетей, используемых для DDoS атак, могут быть использованы датасеты, содержащие данные трафика с устройств IoT. Архитектуры нейронных сетей для обнаружения DDoS атак могут быть различными, включая сверточные нейронные сети, рекуррентные нейронные сети и комбинации из них. В качестве входных данных для моделей могут использоваться параметры сетевого трафика, такие как размер пакетов, частота запросов, распределение IP-адресов и протоколов. Продукты, использующие машинное обучение для обнаружения DDoS атак, включают в себя коммерческие решения от компаний, а также открытые проекты.

В целом, машинное обучение дает новые возможности для обнаружения DDoS атак, позволяя автоматически анализировать и выявлять необычное поведение в сети, что может быть связано с атакой. Однако, необходимо помнить, что машинное обучение не является универсальным решением для всех сценариев обнаружения DDoS атак и может требовать дополнительной настройки и адаптации для каждого конкретного случая.

Список использованных источников:

1. DDoS-атаки и электронная коммерция: современные подходы к защите [Электронный ресурс] / 1-С Битрикс / / Сайт Хабрахабр. - Режим доступа: https://habrahabr.ru/ company/bitrix/blog/267947

2. Шелухин О.И., Ванюшина А.В., Габисова М.Е. Фильтрация нежелательных приложений интернет трафика с использованием алгоритма классификации Random Forest. Вопросы кибербезопасности, № 2 (26), 2018 г., стр. 44-51

3. Artifcial intelligence and machine learning) / Niklas Kühl, Max Schemmer, Marc Goutier, Gerhard Satzger.] // Electronic Marketsи, https://link.springer.com/article/10.1007/s12525-022-00598-0 .

4. Котов, В. Д. Современное состояние проблемы обнаружения сетевых вторжений / В.Д. Котов, В.И. Васильев / / Вестник УГАТУ. - 2012. - Т. 16, № 3. - С. 198-204.

5. UNSW_NB15 – Kaggle [Электронный ресурс] – Режим доступа: https://www.kaggle.com/mrwellsdavid/unsw-nb15/. – Дата доступа: 02.04.2023

6. Network Intrusion Detection – Kaggle [Электронный ресурс] – Режим доступа: https://www.kaggle.com/sampadab17/network-intrusion-detection/. – Дата доступа: 02.04.2023

7. Aposemat IoT-23 – Stratosphereips [Электронный ресурс] – Режим доступа: https://www.stratosphereips.org/datasets-iot23. – Дата доступа: 02.04.2023

8. Android-mischief-dataset – Stratosphereips [Электронный ресурс] – Режим доступа: https://www.stratosphereips.org/android-mischief-dataset. – Дата доступа: 02.04.2023

UDC 004.056.53

MACHINE LEARNING CAPABILITIES FOR DETECTING DDOS ATTACKS

Sharonava E.I.

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

Petrov S.N. – PhD in Technical Sciences

Annotation. The possibilities of machine learning methods for detecting signs of DDoS attacks are shown.

Keywords. Machine learning, botnet, DDoS attack, neural networks, network flow, dataset, machine learning libraries.

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ» ТЕЗИСЫ

УГЛЕРОДОСОДЕРЖАЩИЕ ПОГЛОТИТЕЛИ ДЛЯ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТ ПОМЕХ

Бордиловская Д.В., студент гр.961401

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Белоусова Е.С., Бойправ О.В. – канд. тех. наук

Аннотация. В данной статье представлен сравнительный анализ результатов измерения коэффициентов отражения и передачи в диапазоне частот 2–17 ГГц для поглотителей электромагнитного излучения, изготовленных на основе углеродосодержащих компонентов, для защиты средств вычислительной техники от помех.

Ключевые слова. Коэффициент отражения, коэффициент передачи, поглотители электромагнитного излучения, активированный уголь.

Проблеме влияния электромагнитных помех на средства вычислительной технике долгое время не уделялось внимание, пока не были зарегистрированы сбои в информационных системах различных организаций электроэнергетики, промышленности и др. Сегодня производственные процессы настолько зависит от используемой электро- и радиотехники, что проблема обеспечения электромагнитной совместимости и защиты от помех стала актуальной.

Электромагнитная помеха – электромагнитное явление или процесс естественного, или искусственного происхождения, которые снижают или могут снизить качество функционирования технического средства [1].

Электромагнитная совместимость (ЭМС) – способность технических средств (ТС) функционировать с заданным качеством в определенной электромагнитной обстановке, не создавая при этом недопустимых электромагнитных помех другим техническим средствам и недопустимых электромагнитных воздействий на биологические объекты [1].

Обеспечение ЭМС, т.е. достижение такого состояния, когда электротехнические, электронные и радиоэлектронные аппараты, системы и установки будут пригодны к выполнению функций по назначению при воздействии помех, создаваемых электротехническими изделиями и вызываемых природными явлениями, стало необходимым условием научно-технического прогресса

К основным используемым методам при помощи, которых можно устранить или, уменьшить влияние помех при разработке отдельных узлов аппаратуры относятся следующие: экранирование, заземление, фильтрация, балансировка, изоляция, разнесение и ориентация проводников в пространстве, регулировка величины полного сопротивления схемы [2].

В данной работе представлены результаты измерений коэффициентов отражения и передачи поглотителей электромагнитного излучения изготовленных с помощью углеродосодержащих компонентов.

На рисунке 1 представлен внешний вид полученных поглотителей электромагнитного излучения, изготовленных по методике, изложенной в [3]. В смесь двухкомпонентной полиуретановой маски (70 масс. %) добавляллся порошкообразный активированный уголь двух видов: кокосовый (образец 1), березовый (образец 2).

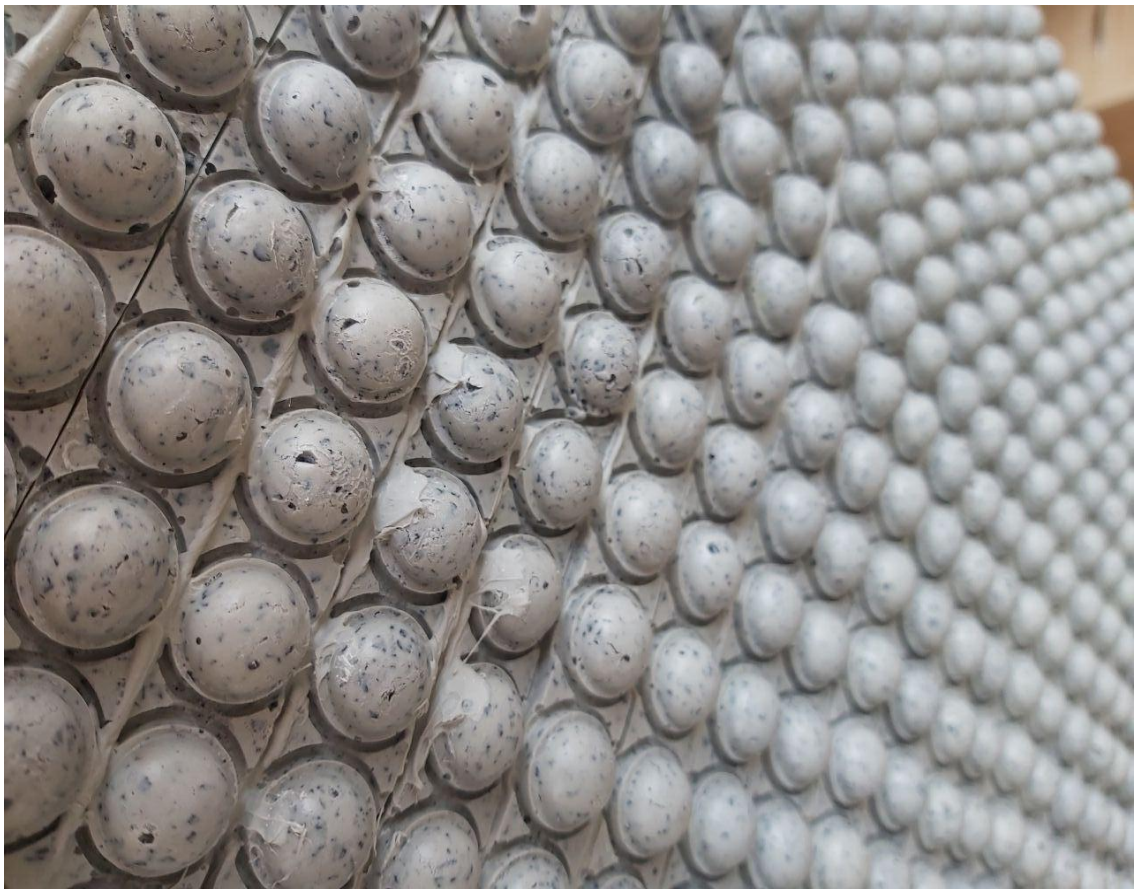
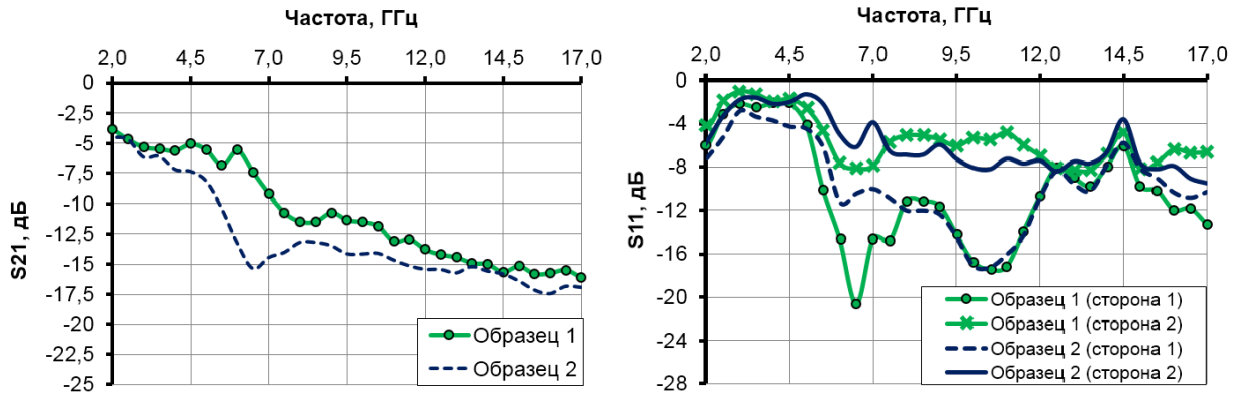


Рисунок 1 – Вид сверху и в перспективе поглотителя электромагнитного излучения (образец 1)

Для измерения коэффициентов передачи и отражения конструкций экранов ЭМИ использовался панорамный измеритель коэффициентов передачи и отражения SNA 0,01–18, работающий по принципу раздельного выделения и непосредственного детектирования уровней падающей и отраженной волн в диапазоне частот 2–17 ГГц. Измерения проводились с расположением плоского металлического листа за исследуемым поглотителем. Изначально проводились измерения коэффициента отражения при расположении поглотителей стороной с геометрическими неоднородностями (сторона 1) к излучаемой антенне, на следующем этапе измерения проводились при расположении поглотителей обратной (плоской) стороной (сторона 2) к излучаемой антенне. На рисунке 2 представлены частотные характеристики коэффициентов отражения и передачи в диапазоне частот 2–17 ГГц для образцов поглотителей электромагнитного излучения.



а б

Рисунок 2 – Частотные характеристики коэффициентов передачи и отражения в диапазоне частот 2–17 ГГц для образцов поглотителей электромагнитного излучения

Установлено, что коэффициент передачи для образца 1 (с порошкообразным активированным кокосовым углем) составляет менее –10 дБ на частотах выше 7 ГГц, для образца 2 – менее 12,5 дБ. Коэффициенты отражения незначительно отличаются при расположении обоих образцов плоской стороной (сторона 2) к излучаемой антенне. Минимальное значение коэффициента отражения (–21 дБ на частотах 6–7 ГГц) получено для образца 1 при его расположении стороной с геометрическими неоднородностями (сторона 1) к излучаемой антенне. Как видно на рисунке 2, значения коэффициентов отражения для обоих образцов на частотах свыше 8 ГГц коррелируют между собой.

На основе проведенного сравнительного анализа результатов измерений коэффициентов отражения и передачи в диапазоне частот 2–17 ГГц выявлено, что добавление порошкообразного активированного кокосового угля при изготовлении поглотителей электромагнитного излучения способствует уменьшению коэффициента отражения до значения –21 дБ на частотах 6–7 ГГц, что позволяет рекомендовать их использования для защиты средств вычислительной техники от помех.

Список использованных источников:

1. Малков, Н.А. Электромагнитная совместимость радиоэлектронных средств : учеб. пособие / Н.А. Малков, А.П. Пудовкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2007. – 88 с.

2. Кереселидзе, Е. В. Электромагнитная совместимость радиоэлектронных средств: учебно-методическое пособие / Е. В. Кереселидзе – Мн.: БГУИР, 2005. – 102 с.

3. Способ изготовления углесодержащего поглотителя электромагнитного излучения с геометрически неоднородной поверхностью и углесодержащий поглотитель электромагнитного излучения с геометрически неоднородной поверхностью, изготовленный этим способом : заявка на изобрет. № 20220116 / С.Э. Саванович, Е.С. Белоусова, О.В Бойправ. – Заявл. 29.04.2022.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ РЕЧЕПОДОБНЫХ ПОМЕХ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Валиев Е.А., учащийся направления «Информационная безопасность»;
Макареня Е.А., учащаяся направления «Информационная безопасность»

Национальный детский технопарк г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Аннотация. В рамках разработки устройства защиты речевой информации предложено формирование двух маскирующих речеподобных сигналов, одного с мощностью равной мощности информационного сигнала и формируемого без учета статистических особенностей языка, второго со значительно большей мощностью и формируемого с учетом статистических особенностей языка, что позволит повысить стойкость защиты к методам статистического анализа и анализа мощности сигнала.

Одним из методов защиты речевой информации является ее маскирование помеховыми сигналами [1, 2]. В качестве маскируемых сигналов широко применяются речеподобные помехи [3]. Таким образом, был разработан модуль синтеза речеподобных сигналов для активной защиты речевой информации [4]. Предложенный модуль синтеза речеподобных сигналов позволяет сформировать речеподобную помеху из голоса диктора-непосредственного участника конфиденциального разговора, не несущую никакой смысловой информации, и по своим статистическим особенностям полностью соответствующую русской речи. Поскольку уровень данной помехи значительно превышает уровень скрываемого информационного сигнала предлагается формировать дополнительный речеподобный сигнал также из речи данного диктора, уровень которого будет равен уровню скрываемого сигнала, но без учета статистических закономерностей языка. В результате смешения информативного сигнала с дополнительным речеподобным сигналом произойдет нарушение статистических закономерностей, в результате чего смешанный сигнал может быть классифицирован как не несущий смысловой нагрузки. В тоже время более мощный речеподобный сигнал, соответствующий статистическим закономерностям, может быть классифицирован как смысловой.

Для формирования речеподобной помехи были изучены статистические особенности русского языка с помощью разработанного на языке программирования C++ программного средства. Данное программное средство способно производить расчет частоты используемых в заданном тексте букв с целью проведения статистического анализа текста. Для этого в программу загружается текстовый файл с заданным именем, в котором рассчитывается частота встречаемости каждого символа, результаты сохраняются в другой текстовый файл с заданным именем. Внешний вид интерфейса программы представлен на рисунке 1.

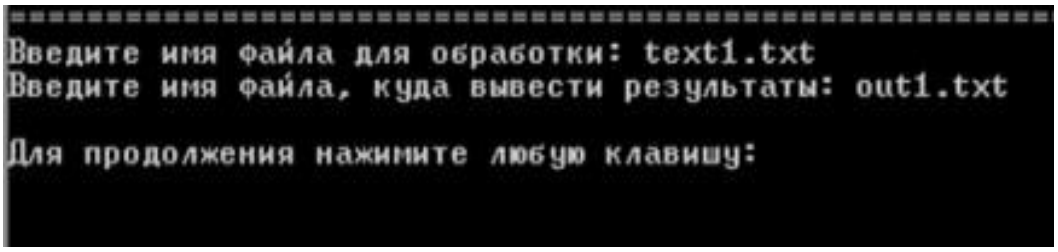


Рисунок 1 – Внешний вид интерфейса разработанного программного средства

С помощью API, размещенного на портале text.ru, производится подсчет слоговой частотной характеристики. Частотная характеристика абзацев и предложений рассчитывается с помощью API, размещенного на портале planetacalc.ru. Для анализа были использованы тексты художественного, публицистического и научного стилей объемом более 80 тысяч символов каждый. С целью изучения статистики русского языка были выбраны следующие тексты: роман «Мастер и Маргарита», журнал «Цифровая трансформация», газета «СБ. Беларусь сегодня». В результате анализа полученных статистических закономерностей русского языка в основу модуля формирования речеподобных помех было положено распределение вероятностей, соответствующее публицистическому стилю, поскольку оно представляет собой среднее между художественной и технической литературой и в большей степени соответствует стилю делового общения.

Список использованных источников:

1. Основы защиты информации: учеб.-метод. комплекс для слушателей ИПК спец. 1-40 01 73 «Программное обеспечение информационных систем» / Р. П. Богуш, А. В. Курилович. – Новополоцк: ПГУ, 2009. – 96 с.

2. Бузов Г.А., Калини С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. М., 2005.

3. Бурлаков М.Е., Осипов М.Н. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум. Самара 2021.

4. Валиев, Е. А. Устройство защиты информации от утечки по акустическим и вибрационным каналам/ Е. А. Валиев, Е. А. Макареня// Наука и образование в современном мире: вызовы XXI века: материалы XII Международной научно-практической конференции, Астана, 10-15 февраля 2023г. / Общенациональное движение «Бобек»; редкол.: Е. Абиев (гл. ред.) [и др.]. – Астана, 2023. – С. 25-28.

ОБОСНОВАНИЕ ВЫБОРА ЭМУЛЯТОРА GNS3 ДЛЯ ИЗУЧЕНИЯ ПРИНЦИПОВ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ С МЕЖСЕТЕВЫМ ЭКРАНИРОВАНИЕМ

До М.К., ст. гр. 961402

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В статье представлены результаты сравнения и обоснования выбора среды моделирования для изучения принципов конфигурации межсетевых экранов и их внедрения в локальные сети. Показаны преимущества использования GNS3 VM и межсетевой экрана FortiGate-VM. Составлены рекомендации по использованию GNS3 в образовательном процессе.

Ключевые слова. Моделирование локальных сетей, межсетевой экран, GNS3, Fortinet, FortiGate.

GNS3 (Graphical Network Simulator 3) – это программный эмулятор сетевого оборудования, который позволяет создавать модели виртуальных сетей [1-2]. Его главным отличием от известного симулятора локальных сетей Cisco Packet Tracer является полная эмуляция сетевых устройств без ограничения их функциональности. GNS3 поддерживается различными операционными системами (Microsoft Windows, MacOS, Linux), его использование является бесплатным и требует лицензии. GNS3 включает в себя два вида программного обеспечения: GNS3-all-in-one software (GUI), GNS3 virtual machine (VM). В GNS3 есть поддержка эмуляции сетевых устройств разных производителей (Fortinet, Juniper и др.), а также серверов и оконечных устройств с разными операционными системами (Windows, Ubuntu). Работа GNS3 основана на использовании среды виртуализации, VirtualBox или VMWare.

Использование эмуляторов сетевого оборудования упрощает настройку, управление и мониторинг смоделированной виртуальной сети благодаря удобному графическому интерфейсу, который предназначен для опытных специалистов, имеющих опыт работы с технологиями виртуализации. Графические инструменты GNS3 позволят более быстро и легко осуществлять проектирование виртуальной сети.

Таким образом, можно выделить следующие основные достоинства использования программного эмулятора сетевых устройств GNS3 для изучения принципов построения локальных сетей:

– возможность полной эмуляции сетевых устройств без ограничения их функционала;

– проектирование гетерогенных сетей, которые будут включать в себя устройства разных производителей;

– внедрение в спроектированную виртуальную сеть полноценных рабочих станций и серверов под управлением разных операционных систем.

При создании топологии в GNS3 созданные устройства должно быть размещены и запущены серверным процессом. Существует несколько вариантов серверной части ПО: локальный сервер GNS3, локальная виртуальная машина Если устройство пользователя использует виртуальную машину GNS3, ее запуск осуществляется на ПК с помощью программного обеспечения для виртуализации, также возможен запуск виртуальной машины GNS3 удаленно на сервере с помощью VMWare ESXi или в облаке. Возможно использование GNS3 без виртуальной машины GNS3, но при этом функционал будет ограничен. При необходимости создания сложной топологии GNS3 с использованием таких устройств как Cisco VIRL, для которого требуется Qemu, требуется запуск виртуальной машины GNS3. Таким образом, GNS3 поддерживает как эмулированные, так и смоделированные устройства.

При установке необходимо совпадение версий программного обеспечения GNS3 и GNS3 VM, в данной работе использовалась версия 2.2.32, реализованная на платформе VMware Workstation версии 14.0. Для построения топологии сети в VMware Workstation были добавлены виртуальные машины GNS3 в качестве удаленного сервера и Window 10 в качестве клиента.

Установка GNS3 VM начинается с запуска VWware Workstation Player14, выбора пункт Open a Virtual Machine и добавления вирутальной машины, скачанной с сайта GNS3. В открывшемся окне вводится имя GNS3 VMware. Образ будет импортирован в хранилище виртуальных машин vmware.

Для настройки программного обеспечения GNS3 и его синхронизации с виртуальной машиной GNS3 VM в VMware необходимо перейти в раздел Edit → Preferences → GNS3 и активировать «Enable the GNS3 VM», выбрать имя добавленной в VMware виртуальной машиной GNS3 VM.

Межсетевые экраны являются аппаратно-программными устройствами или программами, которые регулируют поток сетевого трафика между сетями. Большинство межсетевых экранов расположено на границы сетевого периметра, и в первую очередь они предназначены для защиты внутренних устройств от внешних атак.

На рисунке 1 показан пример получения доступа и настройки IP-адреса межсетевого экрана FortiGate-VM посредством CLI (Command Line Interface), на рисунке 2 – результат подключения с помощью GUI (Graphic User Interface).

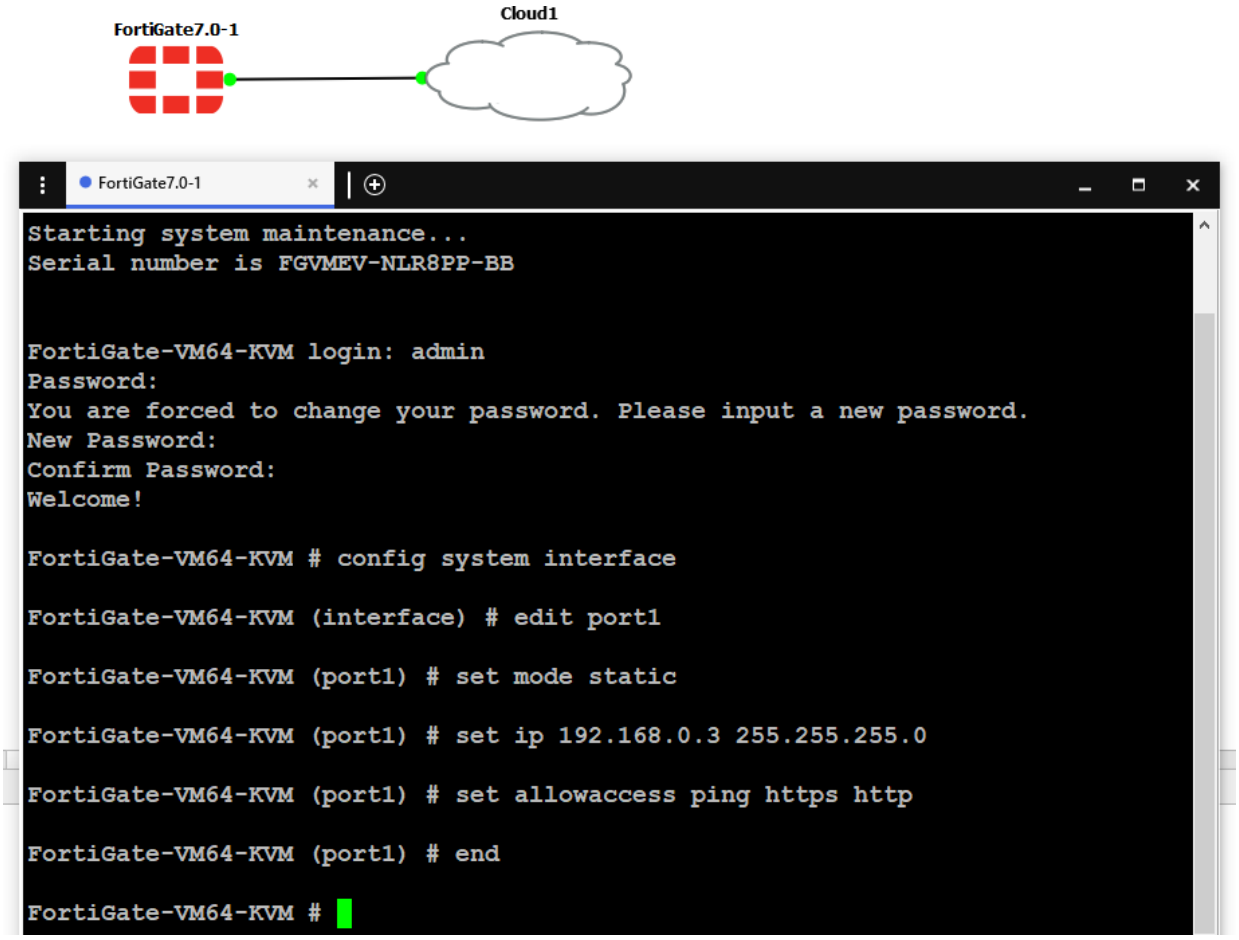


Рисунок 1 – Результат добавления FortiGate-VM в рабочую область GNS3 и получения доступа по CLI

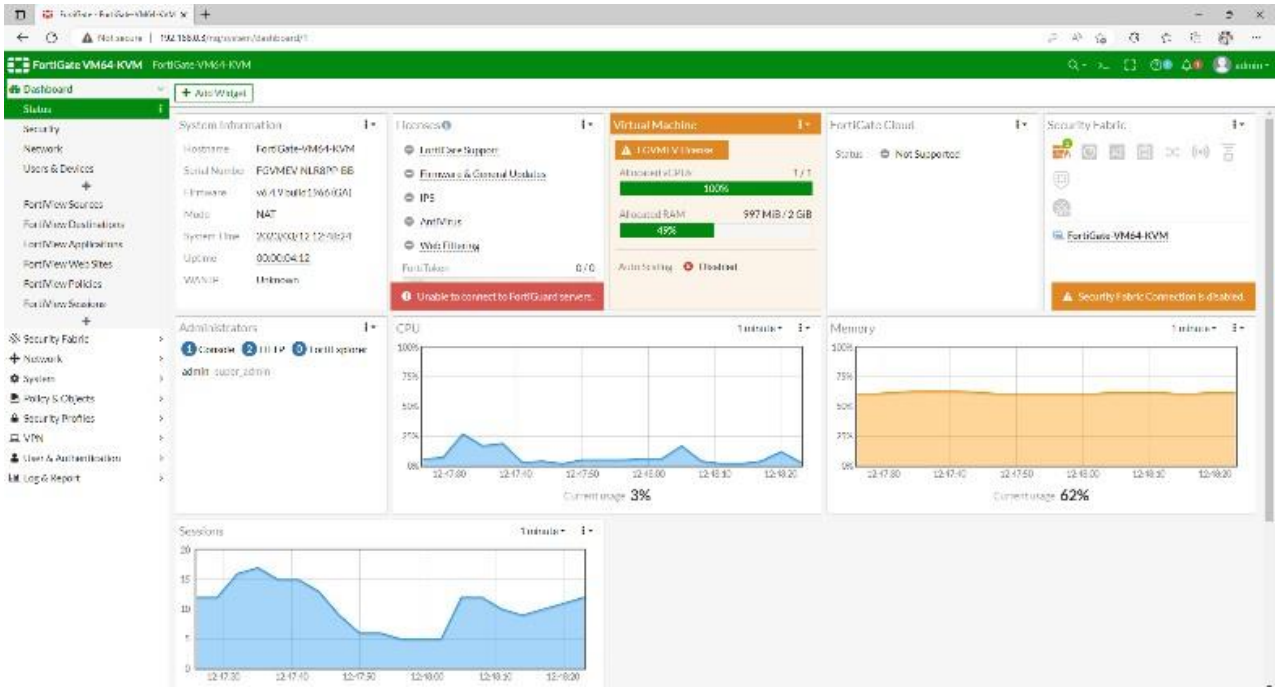


Рисунок 2 – Результат подключения к FortiGate-VM посредством GUI

FortiGate-VM – это полнофункциональный межсетевой экран FortiGate в виде виртуального устройства [3], которое подходит для мониторинга и управления виртуальным трафиком на платформах виртуализации, облаках и SDN, включая VMware vSphere, Hyper-V, Xen, KVM и AWS. FortiGate-VM можно организовать в программно-определяемой среде для предоставления гибких и эластичных услуг сетевой безопасности для виртуальных рабочих нагрузок.

Для скачивания FortiGate-VM на сайте Fortinet [4] необходимо в разделе Support → VM images выбрать платформу KVM. Далее в консоли GNS3 после подключения к виртуальной машине GNS3 необходимо добавить FortiGate в разделе Browse all appliances → New template → Install an appliance from the GNS3 server → Next → Firewalls → FortiGate → Install → Install the appliance on the GNS3 → Next.

Как только образ FortiGate-VM будет установлен на виртуальной машине GNS3, его можно добавить на рабочую область и осуществить конфигурацию (рисунок 1).

Таким образом, GNS3 – это одна из самых популярных программ эмуляции сети, которая позволяет не только изучать взаимодействие сетевых устройств в различных топологиях сетей, но и осуществлять их конфигурацию. В GNS3 эмулируются все основные компоненты устройств, в том числе процессор, память, устройства ввода/вывода, имитируется поведение системы и ее интерфейсов. Описанные достоинства и удобства использования GNS3 на примере добавления и конфигурации FortiGate-VM позволяют рекомендовать его для изучения принципов построения локальных сетей с межсетевым экранированием.

Список использованных источников:

1 Getting Started with GNS3 [Электронный ресурс]. – Режим доступа: https://docs.gns3.com/docs/.

2. Основы GNS3. Обзор [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/266503/.

3. Fortinet FortiGate VM Series [Электронный ресурс] – Режим доступа: https://www.avfirewalls.com/Fortigate-VM-Series.asp.

4. How to add a FortiGate VM into the GNS3 [Электронный ресурс] – Режим доступа: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-add-a-FortiGate-VM-into-the-GNS3/ta-p/242132

ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Дорожкин И.В., ст. гр. 173602; Шарафанович Я.О., ст. гр. 173602

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук

Аннотация. Использование компьютерных и информационных технологий в различных сферах жизни общества становится обязательным атрибутом для достижения максимальной эффективности данной сферы. В связи с этим сфера информационных технологий становится всё более популярной для различного рода мошенников и преступников. Через информационные технологии проходит значительный поток финансов и различной личной информации. Мошенники пользуются этим, пытаясь различными способами выкрасть деньги или же личную информацию пользователя, чтобы в дальнейшем использовать её в своих целях. В данной статье рассмотрены различные источники угроз и виды преступлений в сфере информационных технологий. Основными выводами являются меры предосторожности, способные уберечь пользователя от потенциальных опасностей деятельности правонарушителей.

Существует множество способов и схем, с помощью которых мошенники получают доступ к персональным данным пользователя, такими как пароли, данные банковских карт и многое другое.

Фишинг — вид интернет-мошенничества, который заключается в "выуживании" конфиденциальных данных у пользователя. Спецификой данного метода является то, что жертва мошенничества предоставляет свои данные добровольно. Для этого преступники используют специальные фишинговые сайты, email-рассылку, нацеленную рекламу. Как правило, мошенники маскируются под известные компании, социальные сети или сервисы электронной почты.

Кардинг — сфера киберпреступности, которая напрямую взаимодействует с деньгами обычных законопослушных граждан. При данном виде мошенничества производится операция с использованием платёжной карты, не инициированная её держателем. Кража денежных средств — одна из самых страшных опасностей для любого человека, но есть факторы, из-за которых на сферу кардинга стоит обращать особое внимание.

"Нигерийские" письма — вид мошенничества, основанный на массовой рассылке электронных писем. Своё название письма получили из-за того, что данный вид мошенничества получил наибольшее распространение в Нигерии, причём ещё до распространения интернета, когда письма распространялись по обычной почте. Однако такого рода письма могут приходить и из других стран, но всё же в основном из стран Африки, например, Анголы, Того, Гамбии, Сомали и других.

Кибервымогательство — вымогательство с использованием интернета. Как правило, при таком способе вымогательства пользователь получает сообщение, в котором говорится, что злоумышленники получили личную информацию и угрожают выложить её в открытый доступ.

Взлом социальных сетей и дальнейшее вымогательство денег — один из самых распространенных и часто встречающихся способов мошенничества. Такая популярность данного метода вытекает из ненадёжности большинства социальных сетей — их очень легко взломать. При этом, необязательно быть специалистом в области информационных технологий. На просторах интернета есть куча информации, как взломать ту или иную социальную сеть, поэтому справиться с этой задачей может даже абсолютно неподготовленный человек, никак не связанный с хакерством.

Преступники используют различные методы хищения данных, наиболее популярные методы представлены ниже:

Отслеживание нажатия клавиш. За отслеживание отвечают специальные программы, которые определяют, какие комбинации клавиш пользователь использует чаще всего. Данный способ обычно используется для выявления паролей от банковских счетов и других сервисов.

Подбор паролей. Если преступникам известна некоторая личная информация о пользователе, например имя, фамилия, год рождения и тому подобное, то они могут попытаться подобрать пароль исходя из этих знаний, используя разные комбинации таких данных в качестве пароля. Данный способ является наиболее простым и лёгким, но при этом срабатывает крайне редко, так как очень малое количество людей используют личную информацию в качестве пароля от чего-либо. Тем не менее, такие люди встречаются, и мошенники могут использовать этот факт.

Backdoor программы — программы, позволяющие преступникам входить в систему компьютера пользователя или выходить из нее. Такие программы помогают злоумышленникам удаленно контролировать деятельность пользователя, а также просматривать личную информацию, в том числе пароли.

Обман сети. Злоумышленники могут создавать ложные сети, например Wi-Fi. Правонарушитель может ждать свою жертву в общественном месте, где создаст сеть с названием

этого места. Когда пользователь подключится к такой сети, то преступник сможет отслеживать его действия в интернете, а также просматривать файлы вашего устройства или даже установить на него вирус или другую зловредную программу.

Как уже стало понятно из описания методов правонарушений в области информационных технологий, данные действия могут нести серьёзную опасность для финансов, конфиденциальности пользователя. Тем очевиднее факт, что необходимо знать способы защиты от киберпреступлений и их предостережения.

Необходимо помнить, что ни в коем случае нельзя передавать такие конфиденциальные данные как пин-код банковской карты, пароль электронной почты или аккаунтов в социальных сетях. Ни банк, ни соцсеть никогда не станут запрашивать такого рода данные используя электронную почту. Это самый простой способ защиты от фишинга.

Для защиты от вирусов рекомендуется установить на компьютер надёжный антивирус — программы, препятствующей распространению вируса на компьютере пользователя.

Нельзя вводить данные о банковской карте в непроверенных магазинах и вообще постараться предостеречься от любых онлайн-покупок. Оставлять данные о финансовой карте лучше либо на максимально проверенных сервисах, либо вообще нигде.

Для защиты от «нигерийских писем» не стоит высылать персональные данные или копии каких-либо документов и номера банковских счетов по запросу организаций, в которые пользователь не обращался, или людям, которых до этого никогда не знал.

Одним из самых действенных решений для защиты от блокировки персональных данных является резервное копирование данных. Стоит регулярно сохранять важные файлы и документы в облачное хранилище типа диска Google или на внешний жёсткий диск. Стоит отметить, что при копировании информации на резервный жёсткий диск стоит только тогда, когда пользователь что-то копирует или считывает с него. Если он окажется соединен с компьютером во время нападения, то его также зашифруют. Также, при хранении данных на жёстком диске нужно защитить его надёжным паролем, желательно с двухэтапной аутентификацией, это существенно снизит вероятность взлома облачного хранилища пользователя.

Список использованных источников:

[1] Информатизация - [Электронный ресурс]. – Режим доступа: http://multilang.pravo.by.

[2] Правонарушения в сфере информационных технологий - [Электронный ресурс]. – Режим доступа: https://www.elibrary. ru/download/elibrary_ 37130233_76877572.pdf.

[3] Фишинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3.

[4] Кардинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D0%B4%D0%B8%D0%BD%D0%B3.

[5] Нигерийские письма - [Электронный ресурс]. – Режим доступа: https://nigeria.mfa.gov.by/ru/letters/.

[6] Кибервымогательство — это вымогательство в интрнете - [Электронный ресурс]. – Режим доступа: https://news.ykt.ru/.

[7] Виды киберпреступлений - [Электронный ресурс]. – Режим доступа: https://internetpolicy.kg/literacymodule/course_2/module1/glava1_2.html.

[8] Десять самых громких атак XXI века - [Электронный ресурс]. – Режим доступа: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

[9] Уголовный кодекс Республики Беларусь - [Электронный ресурс]. – Режим доступа: https://kodeksy-by.com/ugolovnyj_kodeks_rb.

[10] Инструкция: как не нарушить авторские права - [Электронный ресурс]. – Режим доступа: https://www.asi.org.ru/2020/04/23/instruktsiya-avtorskie-prava/.

[11] Что такое кардинг, и как защитишься от взлома, покупая в интернете - [Электронный ресурс]. – Режим доступа: https://trends.rbc. ru/trends/industry/60ae051f9a7947c4dc22101b.

[12] Как защититься от шифровальщиков-вымогателей: 5 советов - [Электронный ресурс]. – Режим доступа: https://www.kaspersky. ru/blog/ransomware-five-tips/31352/.

МЕТОДИКА ПОИСКА И АНАЛИЗА УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Нгуен К.А., ст. гр. 961402

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Бойправ О.В. – канд. техн. наук

Аннотация. В докладе представлены результаты обоснования и разработки методики и анализа уязвимостей в информационных системах. Эта методики основана на использовании сканера уязвимостей OpenVAS.

Уязвимость – это недостаток программно-технического средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации. Иными словами, уязвимость – это слабое место актива или средства контроля и управления, которое может быть использовано злоумышленниками. Сведения об известных уязвимостях систематизированы в базе CVE (Common Vulnerabilities and Exposures). Для оценки уязвимостей используется система CVSS (от англ. Common Vulnerability Scoring System).

Сканеры уязвимостей – это, как правило, программные средства, предназначенные для выявления проблем безопасности на узлах вычислительной сети. Позволяют исследовать систему с целью обнаружения уязвимостей.

Известными коммерческими сканерами являются Nessus, GFI LANguard, XSpider (MAxPatrol). Nessus. Они предназначены для автоматического поиска известных уязвимостей и организации защиты информационных систем. В отлчиие от перечисленных сканеров OpenVAS является сканером уязвимостей и средство управления ими с открытым исходным кодом. Проект OpenVAS поддерживается организацией Software in the Public Interest. База уязвимостей OpenVAS включает в себя около 35000 проверок, так называемых Network Vulnerability Tests (NVTs), а также подключение к базе CVE, описывающей известные уязвимости. В отличии от прочих, OpenVAS бесплатен, работает без каких-либо ограничений и может пригодится как сетевым администраторам, так и специалистам ИБ для выявления актуальных проблем своей инфраструктуры. В связи с указанными преимуществами OpenVAS по сравнению с другими сканерами уязвимостей, это программное средство было выбрано в качестве инструмента для разработки методики.

Сканер уязвимостей OpenVAS может быть установлен с помощью VirtualBox в виде виртуальной машины. Для этого енобходимо выполнить следующие шаги.

1. Задать в VirtualBox следующие параметры устанавливаемой виртуальной машины: операционная система – Other Linux, оперативная память – 5120 Мб, процессоры – 2, видеопамять – 9 Мб, носители – загружаемый файл OVA, сеть – сетевой мост.

2. Выполнить процесс установки виртуальной машины.

3. Получить доступ к ресурсам установленной виртуальной машины при использовании следующих учетных данных: логин – admin, пароль – admin.

4. Создать новую учетную запись веб-администратора.

Сканер уязвимостей OpenVAS также может быть установлен в дистрибутив операционной системы Kali Linux. Для этого необходимо выполнить следующие шаги.

1. Полностью обновить систему Kali Linux путем применения команды apt update && apt upgrade -y.

2. Выполнить следующую команду, чтобы загрузить OpenVAS: apt install openvas.

3. Запустить программу установки OpenVAS путем применения следующей команды: gvm-setup.

4. Сгенерировать пароль для первого входа в систему.

5. Проверить настройки OpenVAS путем использования следующей команды: gvm-check-setup.

6. Сгенерировать новый пароль администратора.

Управление OpenVAS выполняется через веб-интерфейс. Доступ к веб-интерфейсу OpenVAS, установленного в виде виртуальной машины, необходимо получать следующим образом.

1. Ввести IP-адрес веб-интерфейса устройства.

2. Войти в систему под учетной записью веб-администратора, созданной во время установки виртуальной машины.

Доступ к веб-интерфейсу OpenVAS, установленного в дистрибутив операционной системы Kali Linux, необходимо получать следующим образом.

1. Открыть веб-интерфейс: http://localhost:9293.

2. Войти в систему при использовании следующих учетных данных: имя пользователя – admin, пароль – новый пароль администратора, сгенерированный при установке.

В ходе апробации разработанной методики были обнаружены 4 уязвимости: 2 уязвимости высокого уровня риска: SMB логины (имя и пароль совпадают), SMB сервер (ms17–010) с портом 445/TCP; 1 уязвимость среднего уровня риска (причина – DCE/RPC сервис с портом 135/TCP); 1 уязвимость низкого уровня риска (причина – временные метки пакетов, передаваемых по протоколу TCP). Следует отметить, что в OpenVAS предусмотрена возможность генерирования отчетов по результатам выполненного сканирования.

Разработанная методика может быть использована для поиска и анализа уязвимостей информационных систем различного масштаба.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРОЦЕССОВ В СИСТЕМЕ ОБРАЗОВАНИЯ

Нестерович Ю.Н., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Листопад Н.И. – д.т.н, профессор

В ходе цифровой трансформации процессов в системе образования создается Республиканская информационно-образовательная среда, с использованием которой будет формироваться новая цифровая реальность системы образования, включающая информационно-телекоммуникационную инфраструктуру, регламенты, нормативно-правовое обеспечение, доверенные образовательные сервисы и платформы, информационные системы и ресурсы, обеспечивающие требуемый уровень информационной безопасности.

В эпоху формирования и развития экономики знаний, основанной на производстве, распределении и использовании информации, система образования должна трансформироваться, отвечая на вызовы настоящего и будущего. Цифровая трансформация всех областей деятельности человека предъявляет новые требования к образованию людей, которые будут участвовать в модернизации процессов во всех видах своей деятельности: на производстве, в общественной и личной жизни, создавая, внедряя и используя в повседневной практике цифровые технологии. Изменяется заказ на образование со стороны социума, семьи, самого обучаемого. Образование становится непрерывным, мобильным, открытым.

Министерством образования разработана и утверждены Концепция развития системы образования Республики Беларусь до 2030 года [1], Концепция цифровой трансформации процессов в системе образования Республики Беларусь на 2019-2025 годы [2], определяющая основные цели, задачи, направления и границы цифровой трансформации процессов в системе образования Республики Беларусь до 2025 года.

Согласно Концепции, цифровая трансформация процессов в системе образования включает следующие основные направления: развитие и модернизация информационно-коммуникационной инфраструктуры системы образования; формирование современного электронного образовательного контента; автоматизация процессов управления.

В 2019 году в рамках научно-исследовательской работы «Разработка программно-методического обеспечения Республиканской информационно-образовательной среды», выполнявшейся Белорусским государственным университетом в рамках мероприятия 20 «Создание информационно-образовательного пространства для формирования личности, адаптированной к жизни в информационном обществе (проект «Электронная школа»)» подпрограммы 3 «Цифровая трансформация» Государственной программы развития цифровой экономики и информационного общества на 2016-2020 годы разработана Концепция создания Республиканской информационно-образовательной среды (далее - РИОС) [3].

В ходе цифровой трансформации процессов в системе образования будет создана РИОС. В рамках РИОС будет формироваться новая цифровая реальность системы образования, включающая информационно-телекоммуникационную инфраструктуру, регламенты, нормативно-правовое обеспечение, доверенные образовательные сервисы и платформы, информационные системы и ресурсы, обеспечивающие требуемый уровень информационной безопасности.

С целью обеспечения информационной безопасности будет осуществлено построение комплексной модели информационной безопасности на примере учреждения общего среднего образования, а именно:

a. построение инфраструктуры информационной безопасности;
b. административно-организационные методы построения информационной безопасности;
c. нормативно-правовые методы построения информационной безопасности.

Практическая реализация предложенной модели будет способствовать повышению эффективности построения информационной безопасности в учреждениях общего среднего образования.

Список использованных источников:

1. Концепция развития системы образования Республики Беларусь до 2030 года [Электронный ресурс] // Официальный сайт Министерства образования Республики Беларусь. Режим доступа: https://edu.gov.by/kontseptsiya-do-2030-goda/%D0%BA%D0%BE%D0%BD% D1%86%D0%B5% D0%BF%D1%86%D0%B8%D1%8F.pdf. – Дата доступа: 10.03.2023.

2. Концепция цифровой трансформации процессов в системе образования Республики Беларусь на 2019-2025 годы [Электронный ресурс] // Официальный сайт Государственного учреждения образования «Минский городской институт развития образования». Режим доступа: https://drive.google.com/file/d/1T0v7iQqQ9ZoxO2IIwR_OlhqZ3rjKVqY-/view?usp=sharing. – Дата доступа: 10.03.2023.

3. Разработка программно-методического обеспечения республиканской информационно-образовательной среды : отчет о научно-исследовательской работе (заключительный) / БГУ ; научный руководитель Ю. И. Воротницкий. Режим доступа: https://elib.bsu.by/handle/123456789/236401. – Дата доступа: 24.03.2023.

МЕТОДИКА РАЗРАБОТКИ МНОГОСЛОЙНЫХ ГИБКИХ ПОГЛОТИТЕЛЕЙ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ СВЧ-ДИАПАЗОНА НА ОСНОВЕ АЛЮМИНИЕВОЙ ФОЛЬГИ

Павлёнок М.В., ст. гр. 961401

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Бойправ О.В. – канд. техн. наук

В докладе представлены результаты обоснования методики разработки многослойных гибких поглотителей электромагнитного излучения на основе алюминиевой фольги, а также результаты исследования характеристик отражения и передачи электромагнитного излучения таких поглотителей.

Поглотители электромагнитного излучения СВЧ-диапазона в настоящее время широко применяются для защиты средств обработки информации от воздействия электромагнитных помех. Такая защита направлена на обеспечение целостности и доступности информации, обрабатываемой с применением указанных средств. Преимущество поглотителей электромагнитного излучения СВЧ-диапазона по сравнению с отражателями электромагнитного излучения СВЧ-диапазона состоит в том, что они не являются причиной возникновения пассивных помех. Поэтому в настоящее время поглотители электромагнитного излучения СВЧ-диапазона чаще, чем отражатели электромагнитного излучения СВЧ-диапазона, являются объектами исследований в области создания новых материалов [1].

Предложена новая методика разработки многослойных поглотителей электромагнитного излучения. По сравнению с аналогами эти поглотители характеризуются пониженными массой и стоимостью, а также гибкостью, что обусловлено соответствующими свойствами материалов, на основе которых они изготовлены (алюминиевая фольга и нетканый волокнистый синтетический материал). Предложенная методика включает в себя следующие этапы.

Этап 1. Откраивание от рулона нетканого волокнистого синтетического материала двух фрагментов одинаковых форм и размеров.

Этап 2. Проделывание несквозных отверстий во фрагментах, полученных в результате реализации этапа 1, с учетом следующих условий:

– проделанные отверстия должны располагаться с шагом, не превышающим половину длины волны на средней частоте рабочего диапазона частот изготавливаемого поглотителя;

– отверстия, проделанные в первом из фрагментов, полученных в результате реализации этапа 1, должны быть смешены относительно отверстий, проделанных во втором из фрагментов, полученных в результате реализации этапа 1 (при условии расположения этих фрагментов друг на друге таким образом, чтобы их края совпадали).

Этап 3. Изготовление на основе алюминиевой фольги элементов кольцевидной формы для расположения в отверстиях первого из фрагментов, полученных в результате реализации этапа 1, с учетом того, что диаметр этих элементов не должен превышать половину длины волны на средней частоте рабочего диапазона частот изготавливаемого поглотителя.

Этап 4. Изготовление на основе алюминиевой фольги элементов сферической формы для расположения в отверстиях второго из фрагментов, полученных в результате реализации этапа 1, с учетом того, что диаметр этих элементов не должен превышать половину длины волны на средней частоте рабочего диапазона частот изготавливаемого поглотителя.

Этап 5. Расположение элементов, полученных в результате реализации этапа 3, в отверстиях первого из фрагментов, полученных в результате реализации этапа 1.

Этап 6. Расположение элементов, полученных в результате реализации этапа 4, в отверстиях второго из фрагментов, полученных в результате реализации этапа 1.

Этап 7. Расположение фрагмента, полученного в результате реализации этапа 5, поверх фрагмента, полученного в результате реализации этапа 6, таким образом, чтобы края этих фрагментов совпадали, и ниточное соединение указанных фрагментов по их краям.

Этап 8. Откраивание от рулона полимерного фольгированного материала одного фрагмента, форма и размер которого совпадают с формой и размерами фрагментов, полученных в результате реализации этапа 1.

Этап 10. Расположение конструкции, полученной в результате реализации этапа 7, поверх фрагмента полимерного фольгированного материала, полученного в результате реализации этапа 8, таким образом, чтобы конструкция, полученная в результате реализации этапа 8, была

ориентирована вверх слоем в виде фрагмента нетканого волокнистого синтетического материала, в отверствия которого вставлены элементы кольцевидной формы.

Этап 11. Ниточное соединение по краям конструкции, полученной в результате реализации этапа 7, и фрагмента полимерного фольгированного материала, полученного в результате реализации этапа 8.

В соответствии с предложенной методикой изготовлены два типа экспериментальных образцов поглотителей электромагнитного излучения СВЧ-диапазона. Экспериментальный образец каждого из типов отличался шагом расположения в его объеме элементов кольцевидной и сферической форм. Экспериментальному образцу первого типа соответствовал шаг расположения в его объеме элементов кольцевидной и сферической форм, равный 2,0 см, а экспериментальному образцу второго типа – шаг, равный 4,0 см.

На рисунке 1 представлены частотные зависимости коэффициента отражения электромагнитного излучения в диапазоне 3,0–17,0 ГГц изготовленных экспериментальных образцов.

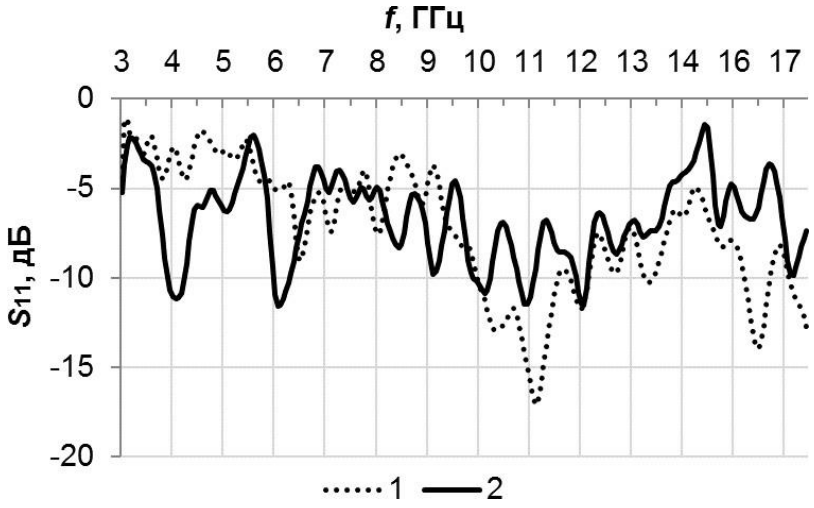


Рис. 1. Частотные зависимости коэффициента отражения электромагнитного излучения в диапазоне 3,0–17,0 ГГц экспериментального образца первого типа (кривая 1) и экспериментального образца второго типа кривая 2)

Как видно из рис. 1, среднее значение коэффициента отражения электромагнитного излучения в диапазоне частот 3,0–17,0 ГГц экспериментального образца первого типа превышает среднее значение коэффициента отражения электромагнитного излучения в диапазоне частот 3,0–17,0 ГГц экспериментального образца второго типа. Это обусловлено тем, что в объеме экспериментального образца первого типа содержится в 2,0 раза больше изготовленных на основе алюминиевой фольги элементов, чем в объеме экспериментального образца второго типа, и в связи с этим экспериментальный образец первого типа обеспечивает в большей степени рассеяние взаимодействующих с ним электромагнитных волн, чем экспериментальный образец второго типа.

Значения коэффициента передачи электромагнитного излучения в диапазоне частот 3,0–17,0 ГГц изготовленных экспериментальных образцов изменяются в пределах от –25,0 до40,0 дБ. Это обусловлено наличием в структуре этих образцов слоя на основе полимерного фольгированного материала. Значения коэффициента поглощения электромагнитного излучения в диапазоне частот 3,0–17,0 ГГц изготовленных экспериментальных образцов достигают величины 0,9.

Поглотители электромагнитного излучения, изготовленные в соответствии с предложенной методикой, представляются перспективными для использования в целях экранирования помещений, в которых расположены средства обработки информации.

Список использованных источников:

1. Quantitative Interpretation of Electromagnetic Interference Shielding Efficiency: Is It Really a Wave Absorber or a Reflector? / U. Hwang [et al.] // ACS Omega. – 2022. – Vol. 7, iss. 5. – P. 4135–4139.

МОДЕЛЬ ЭКСПЛУАТАЦИИ УЯЗВИМОСТИ ARP-ПРОТОКОЛА

Самаке Б.А., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белоусова Е.А. – канд. техн. наук

Аннотация. В данной статье рассматривается уязвимость протокола ARP с помощью атаки ARP spoofing в модели сети, спроектированной в программном эмуляторе GNS3.

Ключевые слова. ARP, ARP-spoofing, MAC-адрес, IP-адрес, локальная сеть, уязвимость.

В данной работе рассмотрена уязвимость протокола ARP (Address Resolution Protocol), который используется для идентификации MAC-адреса устройства по его IP-адресу, а также для формирования таблиц MAC-адресов на коммутаторах и ARP-таблиц на оконечных устройствах в сети. Уязвимость данного протокола заключается в попытке перехвата широковещательной рассылки ARP-пакетов, в которых есть IP и MAC-адреса устройств в сети. Таким образом, нарушитель может получить данные об устройствах в сети и реализовать атаку ARP spoofing [1].

Рассмотрим сценарий атаки, во первых необходимо провести сбор данных для получение информации (например, IP-адреса пользователя), с помощью анализатора трафика, после чего нарушитель реализует IP-адреса на своем устройстве и добавит его в таблицу MAC адресов коммутаторов. Таким образом, нарушитель сможет подключиться к сети в качестве авторизованного пользователя.

Для проверки уязвимости ARP-протокола необходимо было смоделировать локальную сеть. Для этого был произведен сравнительный анализ несколько средств моделирования такие как Cisco Packet Tracer и GNS3. Обе прогаммы эмулируют реальные сетевые устройства, различные оконечные и промежуточные устройства. Разница между рассмотренными средствами моделирования заключается в том что, Cisco Packet Tracer эмулирует устройства внутри программы, из-за чего выбор устройства ограничен несколькими сериями маршрутизаторов и коммутаторов компании Cisco. GNS3 основан на Qemu и Dynamips и является графическим интерфейсом для создания локальных сетей с использованием Qemu. В GNS3 устройства разных производителей можно добавлять самостоятельно. Также GNS3 предоставляет более точную представление в настройки оборудований [2].

На рисунке 1 представлена модель локальной сети в программном эмуляторе сети GNS3. В смоделированной сети выделено четыре виртуальные сети (VLAN), для каждой из которых настроен DHCP сервер.

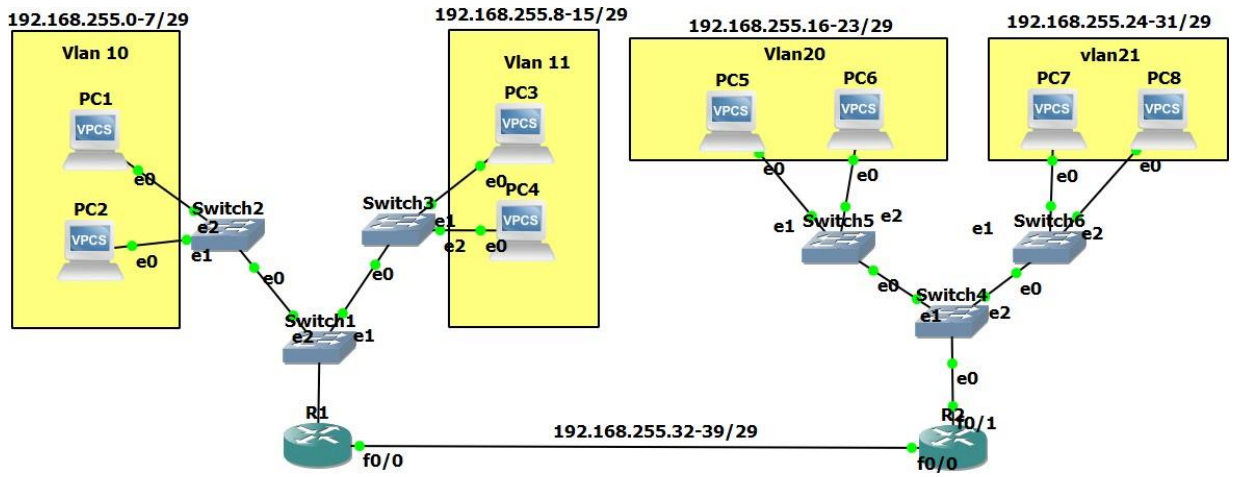


Рисунок 1 – Модель локальной сети для моделирования атаки

На рисунке 2 представлена возможность перехвата нарушителем ARP-пакета во время получение адреса с DHCP-сервера, что можно реализовать посредством использования программного сниффера Wireshark. Как видно из рисунка 2 при перехвате данного пакета нарушитель может получить информацию об адресах устройств в сети, а также информацию о номерах VLAN.

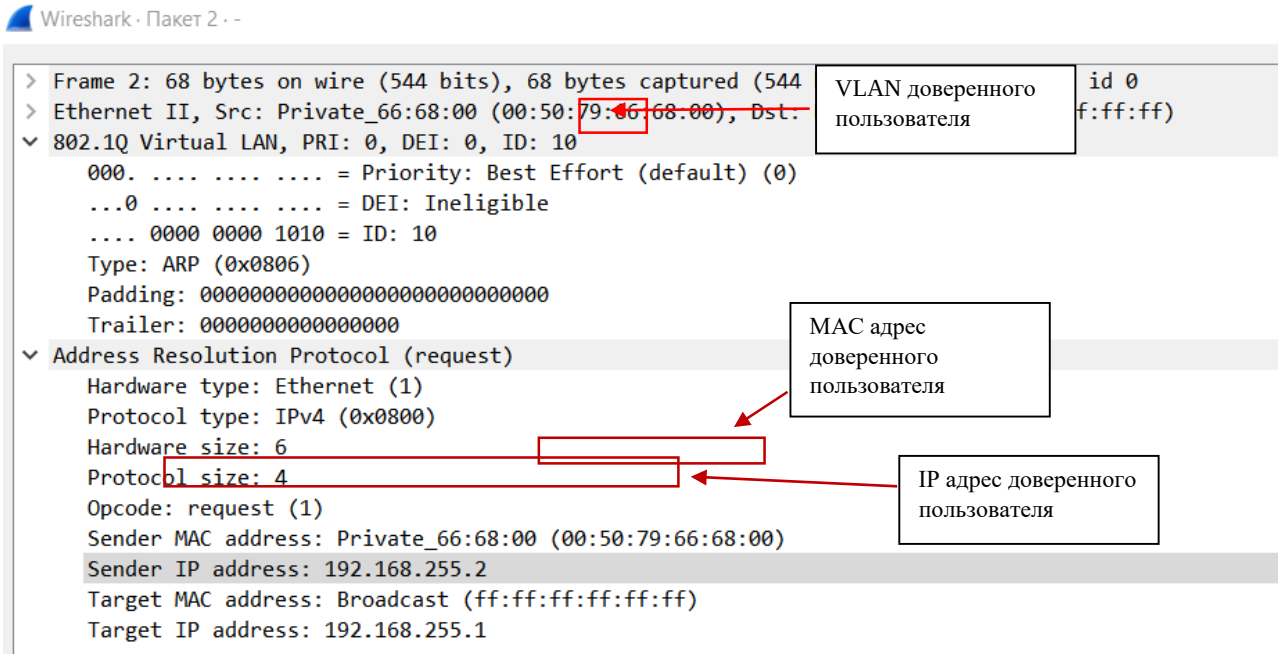
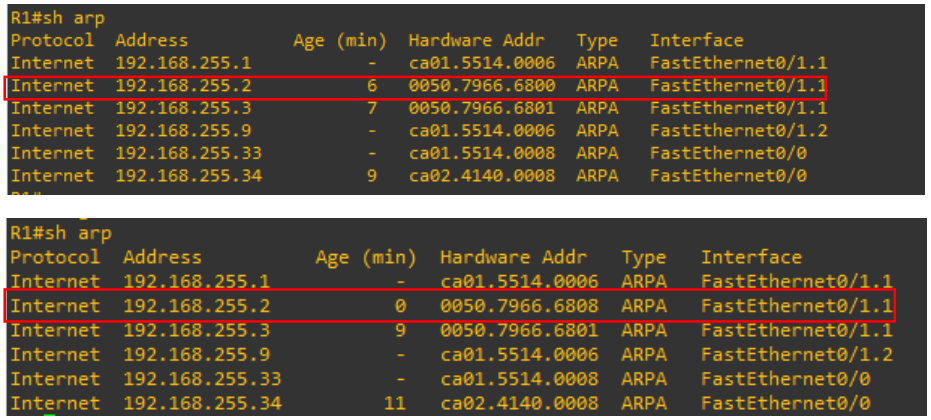


Рисунок 2 – Результат перехвата ARP-рассылки в смоделированной локальной сети

Далее нарушитель может произвести подмену записей в таблицах ARP других устройств в сети путем изменения на своем устройстве IP-адреса на адрес 192.168.255.2, полученный в перехваченном ARP-пакете. Для внесения неверной записи в таблицы ARP устройств в сети, нарушитель производит отправку ICMP пакетов, реализуя команду ping 192.168.255.26. Как видно из рисунка 3 MAC-адрес пользователя изменился на адрес нарушителя без изменение IP-адреса.



```
R1#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.255.1           -   ca01.5514.0006  ARPA   FastEthernet0/1.1
Internet  192.168.255.2           6   0050.7966.6800  ARPA   FastEthernet0/1.1
Internet  192.168.255.3           7   0050.7966.6801  ARPA   FastEthernet0/1.1
Internet  192.168.255.9           -   ca01.5514.0006  ARPA   FastEthernet0/1.2
Internet  192.168.255.33          -   ca01.5514.0008  ARPA   FastEthernet0/0
Internet  192.168.255.34          9   ca02.4140.0008  ARPA   FastEthernet0/0
```

```
R1#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.255.1           -   ca01.5514.0006  ARPA   FastEthernet0/1.1
Internet  192.168.255.2           0   0050.7966.6808  ARPA   FastEthernet0/1.1
Internet  192.168.255.3           9   0050.7966.6801  ARPA   FastEthernet0/1.1
Internet  192.168.255.9           -   ca01.5514.0006  ARPA   FastEthernet0/1.2
Internet  192.168.255.33          -   ca01.5514.0008  ARPA   FastEthernet0/0
Internet  192.168.255.34         11   ca02.4140.0008  ARPA   FastEthernet0/0
```

Рисунок 3 – Результат подмены записей в таблице ARP таблицах маршрутизатора до и после реализации атаки ARP-spoofing

После подмены нарушитель сможет перехватывать трафик предназначены для доверенного пользователя. На рисунке 4 видно, что замена записей в таблице ARP привела к возможности нарушителем получать все пакеты в сети.

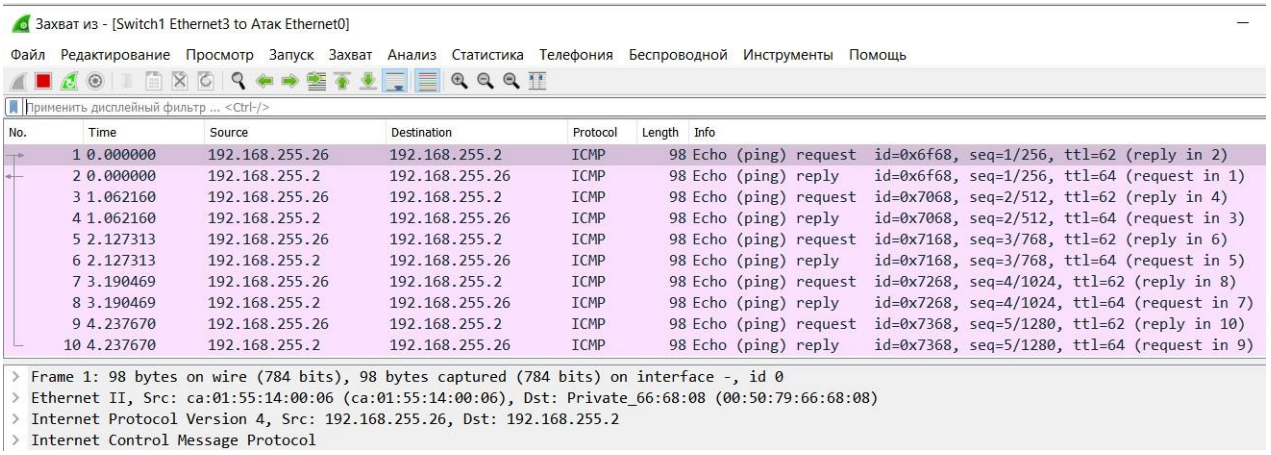


Рисунок 4 – Результат перенаправления пакетов в локальной сети

Таким образом, в работе смоделирована атака ARP-spoofing, проанализированы действия нарушителя и продемонстрированы последствия атаки. В продолжении данной работы планируется разработать комплекс мер по защите устройств локальной сети от атаки ARP-spoofing.

Список использованных источников:

1. Что такое ARP-спуфинг и как от него защититься – режим доступа: Что такое ARP-спуфинг и как от него защититься? (securitylab.ru). – Дата доступа: 25.03.2023.

2. Кулябов Д. С. Средства моделирования сетей для целей обучения– режим доступа: Средства моделирования сетей для целей обучения | Д. С. Кулябов (yamadharma.github.io). – Дата доступа: 25.03.2023.

ACTIVE DIRECTORY И БЕЗОПАСНОСТЬ

Шапошникова Н.П., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук

Аннотация. Уровень защищенности службы каталогов нередко определяет уровень безопасности всей компании. Целесообразно максимально усложнить деятельность злоумышленника, уменьшив возможные области атаки, проводить регулярный мониторинг системы в целях выявления злонамеренных действий и всегда быть готовым к отражению атак, имея детальные планы действий для разных ситуаций.

Уровень защищенности службы каталогов нередко определяет уровень безопасности всей компании. Целесообразно максимально усложнить деятельность злоумышленника, уменьшив возможные области атаки, проводить регулярный мониторинг системы в целях выявления злонамеренных действий и всегда быть готовым к отражению атак, имея детальные планы действий для разных ситуаций.

Проблемы построения безопасных ИТ-инфраструктур являются актуальными для любых организаций. Как только возникает потребность в ИТ-решениях, тут же встает вопрос их безопасности. Не существует абсолютно неуязвимых с точки зрения ИБ организаций, тем не менее необходимо создать как можно больше трудностей злоумышленнику, пытающемуся скомпрометировать или уничтожить ИТ-инфраструктуру компании. Обеспечение безопасности службы каталога – важнейшая задача ИТ и ИБ-отделов предприятия.

Ниже представлен перечень мер, которые помогут значительно снизить вероятность повреждения или внесения несанкционированных изменений в базу данных Active Directory [1]:

1 Своевременное обновление ОС и ПО позволяет уменьшить вероятность компрометации системы и осуществления несанкционированной злонамеренной деятельности внутри ИТ-инфраструктуры организации.

2 Эффективная антивирусная защита и защита от зловредного ПО позволяет существенно повысить защищенность ИТ-инфраструктуры организации в целом.

3 Регулярное резервное копирование AD обеспечивает возможность оперативно восстановить БД СК и удаленные объекты AD, а также службу каталога в ситуации катастрофического сбоя.

4 Эффективная стратегия именования объектов позволяет администраторам службы AD эффективно идентифицировать объекты и управлять данными, хранящимися в AD.

5 Безопасность контроллеров доменов (DC) обеспечивают серверы, хранящие реплику БД службы каталога AD, которые выполняют функции управления данными AD.

6 Защита учетных записей привилегированных пользователей. Ошибочное включение пользователей в высокопривилегированные группы может привести к краху системы как из-за отсутствия достаточных знаний и навыков, так и в результате злонамеренных действий [2].

7 Использование дополнительных возможностей ОС по обеспечению безопасности.

8 Использование принципа наименьших привилегий позволит существенно повысить уровень безопасности, уменьшая для злоумышленника область атаки.

9 Блокировка возможности развертывания и выполнения неавторизованных приложений и сервисов, очевидно, повышает безопасность системы.

10 Наличие доступа к Интернету значительно снижает безопасность всей инфраструктуры. Обеспечение безопасного доступа в Интернет и доступа из Интернета к ресурсам организации является одной из важнейших задач по повышению общего уровня безопасности системы.

Обеспечить безопасность AD – сложная задача, но, приняв ряд элементарных мер предосторожности, можно достаточно надежно защитить инфраструктуру AD.

Список использованных источников:

1. Москалев С., Шапиро Л. Active Directory и безопасность. Часть 1. Построение защищенных служб каталога. //«Системный администратор», №7-8, 2013 г. – С. 44-45.

2. https://www.osp.ru/winitpro/2005/03/177563

URGENT PROBLEMS OF THE DEVELOPMENT OF SOFTWARE FOR FACE RECOGNITION

Wang Kaiyu, student of the group 267311

Belarusian State University of Informatics and Radioelectronics,

Minsk, Belarus

Boiprav O.V. – Cand. Tech. Sci., Ass. Prof.

Abstract. The results of the analysis of the shortcomings of modern software tools for face recognition are presented. Taking into account these results, approaches to the development of the method for creating improved software for face recognition, which are not characterized by the established shortcomings, are determined. The procedure for one of these approaches implementing is presented.

Keywords. Face recognition, software, regularities.

The analysis of modern algorithms underlying the operation of software tools used for face recognition has been carried out. Based on the results of such an analysis, the classification of the methods underlying these algorithms was made, and their shortcomings were identified. The main of these shortcomings are the following [1–3]:
1) the high duration of the process of the system "learning", the purpose of which is to add to the database the file with the reference image of the new system user face;
2) linear dependence of the algorithm execution duration on the number of files with reference images of the system users faces;
3) high computational complexity.
Taking into account the results of the analysis, it was found that the development of the method of the development of the improved software for face recognition should be aimed at eliminating the shortcomings of modern algorithms underlying the operation of software tools used for face recognition. To achieve this aim, it is necessary to establish the following regularities:
1) the regularity of change in the duration of the process of the system "learning", depending on the number of images of new system user face, on the basis of which a file with a standard image of this face is formed;
2) the regularity of the change in the duration of the algorithm execution depending on the performance of the system hardware;
3) the regularity of the change in the computational complexity of the algorithm depending on the type of method underlying it.
A method to establish the regularities of changing the duration of the process of the face recognition system "learning", depending on the number of system user face images, which are utilized during this process, has been developed. The developed method includes the following stages.
Stage 1. Formation of three images of the same user face.
Stage 2. Entering the formed images into the system database and registering the time moment at which this action began to be implemented.
Stage 3. Registration of the time moment at which the processing of the generated images was completed and entered into the database.
Stage 4. Formation of five images of the same user face.
Stage 5. Repeat the stages 2, 3.
Stage 6. Formation of seven images of the same user face.
Stage 7. Repeat steps 2, 3.
Stage 8. Formation of nine images of the of the same user face.
Stage 9. Repeat stages 2, 3.
Stage 10. Based on the quantitative indicators of the results of the stages 1–9 implementation, plotting a graphical dependence of the duration of the system "learning" process on the number of images of the user's face of this system that are utilized during this process.

References

1. Lu, D. Face Detection and Recognition Algorithm in Digital Image Based on Computer Vision Sensor / D. Lu, L. Yan // Journal o Sensors. – 2021. – Vol. 2021. – Article ID 4796768. – https://doi.org/10.1155/2021/4796768.
2. Lazarini, M. A. A Systematic Literature Review on the Accuracy of Face Recognition Algorithms / M. A. Lazarini, R. Rossi, K. Hirama // EAI Endorsed Transactions on Internet of Things. – 2022. Vol. 8, iss. 30. – P. 1–11. – https://doi.org/10.4108/eetiot.v8i30.2346.
3. Sun Y. Research on Face Recognition Algorithm Based on Image Processing / Y. Sun, Z. Ren, W. Zheng // Comput Intell Neurosci. – 2022. – Article ID: 9224203. – https://doi.org/10.1155/2022/9224203.

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ» СТАТЬИ И ТЕЗИСЫ

УДК 621.391

СЛОЖНЕНИЕ СЛОЖНОСТИ ИТЕРАЦИИ ДЕКОДИРОВАНИЯ LDPC КОДА И ТУРБО КОДА

Абрамов И.О., Барабанов М.Ю., магистрант гр.167001

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Астровский И.И. – канд. техн. наук

Аннотация. В данной статье проведена оценка вычислительной сложности одной итерации декодирования блокового турбо кода (32,26) x (32,26), декодируемого по алгоритму Чейза, и сравнение полученной вычислительной сложности с вычислительной сложностью итерации декодирования LDPC кода, декодируемого по алгоритму минимума суммы «Min-sum normalized».

Ключевые слова. Турбо код, LDPC код, сверточный код, сравнение сложности итерации декодирования

При создании турбо кодов использовалась парадигма каскадных кодов. Сущность турбо кодирования заключается в каскадировании двух и более составляющих кодов [2]. Соединение может быть как параллельным, так и последовательным, но в обоих случаях оно происходит через перемежитель.

Турбо коды, использующие в качестве составляющих кодов сверточные коды, называются Turbo Convolution Codes (TCC) или сверточными турбо кодами. Декодируют такие коды с помощью алгоритмов Soft Output Viterby Algorithm (SOVA), Log-MAP и его модификации Max-Log-MAP.

В отличие от сверточных турбо кодов, блоковые турбо коды произведения (Turbo Product Codes (TPC)) используют в качестве составляющих кодов линейные блоковые коды БЧХ или Хэмминга. Перемежение в этом случае не требуется, а декодирование таких кодов осуществляется по алгоритму Чейза.

Для сравнения с рассмотренным выше LDPC кодом выбран двумерный блоковый турбо код (32,26) x (32,26) со скоростью кодирования 0.66. В качестве составляющих кодов используется расширенный код Хэмминга (32,26).

Работу итеративного алгоритма декодирования блокового турбо кода можно разделить на несколько этапов, представленных на рисунке 1. Подсчет элементарных операций будет вестись для этапов 1-4, выполняемых итеративно.

Рисунок 1 – Этапы декодирования блокового турбо кода

Сложность этапов 1 и 2 одинакова и в случае рассматриваемого турбо кода сводится к 32-кратному повторению процедуры обработки строки. Расчет сложности ведется для длины списка гипотез при T=4.

Шаг 1. Перед поиском четырех наименее надежных символов в рассматриваемой строке ко всем значениям надежностей символов применяется операция взятия модуля числа. Всего $N_{|a|} = 32$ операции взятия модуля числа.

Затем происходит поиск 4 наименее надежных символов. Вначале посредствам $N_{/} = 31$ сравнения определяется наименее надежный символ. Затем посредствам $N_{/} = 62$ сравнений

определяется второй с конца по надежности символ (31 сравнение надежностей между собой и 31 проверка на то, что найденный символ не является наименьшим по надежности). Для поиска третьего и четвертого символов с конца потребуется $N_/ = 93$ и $N_/ = 124$ операции сравнения, соответственно.

Всего на данном шаге обработки строки используется $N_{|a|} = 32$ операции взятия модуля числа и $N_/ = 310$ операций сравнения.

Шаг 2. На данном шаге создается 16 гипотез. Для их создания изначально нужно преобразовать «мягкие» решения на входе алгоритма обработки строки в «жесткие» решения путем $N_/ = 32$ сравнений надежностей с нулем. Далее создаются 16 гипотез путем $N_\oplus = 64$ прибавлений по модулю 2 определенных значений ко всем возможным комбинациям позиций, содержащих наименее надежные символы.

Всего на данном шаге обработки строки используется $N_/ = 32$ операции сравнения и $N_\oplus = 64$ операции сложения по модулю 2.

Шаг 3. На данном шаге происходит декодирование сформированных гипотез. 31 символ перемножается по правилам матричного умножения на транспонированную проверочную матрицу кода Хэмминга из 5 строк и 31 столбца. Для этого используется $N_x = 155$ умножений и $N_+ = 150$ сложений по модулю 2. Получившийся синдром преобразуется в число в десятичной системе счисления путем $N_x = 5$ умножений и $N_+ = 4$ сложений. По полученному значению происходит поиск номера разряда, в котором произошла ошибка. Для этого будет использовано не более $N_/ = 31$ операции сравнения. По найденному номеру разряда инвертируется жесткий символ путем $N_+ = 1$ сложения по модулю 2. Далее на основе декодированных 31 символов путем $N_\oplus = 30$ сложений по модулю 2 вычисляется последний символ гипотезы. Процедура повторяется для всех 16 гипотез.

Всего на данном шаге обработки строки используется $N_x = 2560$ операций умножения, $N_\oplus = 2896$ операций сложения по модулю 2, $N_+ = 64$ сложения, $N_/ = 496$ сравнений.

Шаг 4. Перед расчетом одной метрики значения элементов гипотезы необходимо заменить по правилу «0» на «1», а «1» на «-1». Для этого используется $N_/ = 32$ сравнения. Для расчета метрики используется $N_+ = 32$ вычитания и $N_+ = 31$ сложение, а также $N_x = 32$ умножения полученного результата на самого себя (возведение в квадрат).

Всего на данном шаге обработки строки используется $N_x = 512$ операций умножения, $N_+ = 1008$ сложений, $N_/ = 512$ сравнений.

Шаг 5. Гипотеза с наименьшим значением метрики находится путем $N_/ = 15$ сравнений метрик гипотез друг с другом.

Всего на данном шаге обработки строки используется $N_/ = 15$ сравнений.

Шаг 6. Гипотеза «конкурент» для i-ого символа находится путем $N_/ = 15$ сравнений метрик гипотез друг с другом $N_/ = 15$ проверок условия $di \neq ki$.

Всего на данном шаге обработки строки используется $N_/ = 960$ операций сравнения для поиска 32 гипотез «конкурентов».

Шаг 7. Оценка сложности ведется для расчета поправок по формуле (1).

$$w_j = ((R' - K_i)^2 - (R' - D)^2) / 4 \times d_i \quad (1)$$

Значения в скобках уже рассчитаны на шаге 4. Для расчета одной поправки используется $N_+ = 1$ вычитание и $N_x = 2$ умножения (операция деления на 4 заменена на умножение на 0.25).

Всего на данном шаге обработки строки используется $N_+ = 32$ вычитания и $N_x = 512$ умножения.

Шаг 8. Для формирования одного элемента «мягкого» входа используется $N_x = 1$ умножение и $N_+ = 1$ сложение.

Всего на данном шаге обработки строки используется $N_+ = 32$ сложения и $N_x = 32$ умножения.

После обработки всех строк и столбцов необходимо получить 64 синдрома, каждый из которых рассчитывается путем перемножения 32 символов на проверочную матрицу кода Хэмминга из 6 строк и 32 столбцов. Всего для расчета синдромов необходимо $N_x = 12288$ умножений и $N_\oplus = 11904$ сложений по модулю 2. Перед расчетом синдрома необходимо получить «жесткие» апостериорные решения посредствам $N_/ = 1024$ сравнений. $N_/ = 1$ сравнение требуется для проверки выхода за максимальное число итераций.

Сравнение сложности итерации декодирования LDPC кода и турбо кода приводится в таблице 1. Моделирование на ПК показало, что проведение итерации LDPC декодирования требует в 3 раза меньше времени, чем проведение итерации блокового турбо декодирования.

Таблица 1 – Сравнение сложности декодирования.

Операция	Количество на итерацию декодирования	
	LDPC («Min-sum normalized»)	Блоковый турбо код (Алгоритм Чейза)
Сложение	37024	72704
Умножение	38706	215040
Сравнение	64159	149825
Взятие модуля	33888	2048
Сложение по модулю 2	4218	201344

Следует подчеркнуть, что процедура декодирования блокового турбо кода может быть оптимизирована с точки зрения вычислений, как это показано в [1]. Однако в случае оптимизированного алгоритма декодирования турбо кода его сложность следует сравнивать со сложностью оптимизированного алгоритма декодирования LDPC.

Анализ соотношений между сложностью сравниваемых кодов на итерацию декодирования и их средним используемым числом итераций показывает, что в конкретном случае выгоднее проделывать больше итераций декодирования LDPC с меньшей сложностью, чем осуществлять меньшее число итераций турбо декодирования, но с большей сложностью.

Список использованных источников:

1. Архипкин, А.В. Разработка алгоритмов кодирования и декодирования для телекоммуникационных систем радиосвязи с ортогональными поднесущими : диссертация на соискание ученой степени кандидата технических наук / А.В. Архипкин. – Москва, 2008.

2. Золотарев, В.В. Обзор исследований и разработок методов помехоустойчивого кодирования / В.В. Золотарев, Г.В. Овечкин. – Москва, 2005.

UDC 621.391

COMPARISON OF THE COMPLEXITY OF THE LDPC CODE AND TURBO CODE DECODING ITERATION

Abramov I.O., Barabanov M.Yu., master students gr. 167001

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

Astrovskiy I.I. – PhD in Engineering sciences

Annotation. This article estimates the computational complexity of one iteration of decoding the block turbo code (32,26) x (32,26) decoded by the Chase algorithm, and compares the resulting computational complexity with the computational complexity of the LDPC decoding iteration of the code decoded by the minimum sum algorithm "Min-sum normalized".

Keywords. Turbo code, LDPC code, convolutional code, comparison of the complexity of the decoding iteration

УДК 621.391

ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ДЕКОДИРОВАНИЯ «MIN-SUM» И ЕГО МОДИФИКАЦИЙ

Абрамов И.О., Барабанов М.Ю. – магистранты гр.167001

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Астровский И.И. – канд. техн. наук

Аннотация. В данной статье приведена оценка сложности алгоритма декодирования LDPC кодов «Min sum» и его модификаций. Проанализированы отличия сложности алгоритмов «Min-sum», «Min-sum normalized», «Min-sum offset».

Ключевые слова. LDPC-код, адгоритм декодирования, низкополостная матрица, вычислительная сложность.

LDPC-код представляет собой линейный блочный код, характеризующийся разряжённой проверочной матрицей $H(N \times M)$, где M – количество проверочных строк; N – длина кода, т.е. количество столбцов в матрице; K – длина исходных данных. Если количество ненулевых элементов в каждой строке равно $dr < N$ и количество ненулевых элементов в каждом столбце равно $dc < M$, то код называется регулярным, в противном случае – нерегулярным.

Графически LDPC-коды можно представить с помощью графа Таннера (рисунок 1).

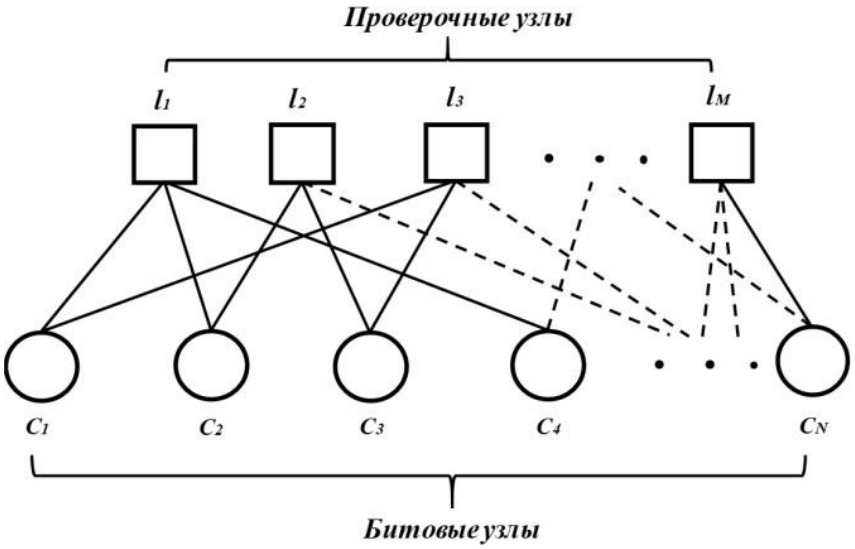


Рисунок 1 – Представление регулярного LDPC-кода в виде графа Таннера

На рис. 1 вершины $l1$, $l2 \cdot \cdot \cdot lM$ – проверочные узлы, а вершины $c1$, $c2 \cdot \cdot \cdot cN$ – битовые узлы. Таким образом, из графа видно, что $dr = 3$ и $dc = 2$.

Существует множество алгоритмов декодирования LDPC-кодов. Среди них самым известным является алгоритм «Sum-product», который обеспечивает высокую эффективность декодирования, но требует больших вычислительных затрат. В связи с этим существуют альтернативные методы, целью которых является снижение вычислительных затрат. Среди них одним из самых популярных является алгоритм «Min-sum». Алгоритм «Min-sum» является аппроксимацией алгоритма «Sum-product» с использованием простых операций, таких как поиск минимума и сложение, вместо сложных функций гиперболического тангенса и арктангенса [1].

Вычислительная сложность — понятие в информатике и теории алгоритмов, обозначающее функцию зависимости объёма работы, которая выполняется некоторым алгоритмом, от размера входных данных [3].

В данной статье рассмотрим и проведём оценку вычислительной сложности алгоритма «min-sum» и его модификаций.

Для оценки сложности алгоритмов декодирования в качестве базовой используется методика, предложенная в [2]. Данная методика в полной мере учитывает операции сложения (N+), умножения (Nx), сравнения (N/), взятия модуля числа (N|a|) и сложения по модулю 2 ($N_{\oplus}$) на одну итерацию декодирования. Операция вычитания приравнивается к операции сложения. Число операций различного типа будет зависеть от «весов» строк (k) и столбцов (j) проверочной матрицы, а также от длины кодового слова (l), количества уравнений в матрице проверки на четность (m) и алгоритма декодирования.

Работу любого алгоритма декодирования кодов с малой плотностью проверок на четность можно разделить на несколько этапов, представленных на рисунке 2. Подсчет элементарных операций будет вестись для этапов 1-4, выполняемых итерактивно.

Рисунок 2 – Этапы декодирования LDPC кодов

Алгоритм минимума суммы «Min-sum»

Шаг 1. Расчет сообщений от символьных узлов графа Таннера.

Для первой итерации сообщения от символьных узлов L(qm,l) устанавливаются как входные мягкие решения L(Cl). На последующих итерациях на данном шаге используются только операции сложения, количество которых выражается формулой:

$$\boxed{N_{+} = \sum_{i=1}^{l} (j_i - 1) \cdot j_i}, \quad (1)$$

где ji - вес i-ого столбца проверочной матрицы. Количество столбцов в матрице соответствует длине кодового слова l.

Шаг 2. Расчет сообщений от проверочных узлов графа Таннера.

Для формирования сообщений от проверочных узлов к символьным узлам используются операции сравнения, умножения и взятия модуля числа. Количество умножений, выполняемых на данном этапе, выражается формулой:

$$\boxed{N_{\times} = \sum_{i=1}^{m} k_i \cdot (k_i - 1)}, \quad (2)$$

где i k - вес i-ой строки проверочной матрицы.

Количество сравнений, выполняемых на данном этапе, выражается формулой:

$$N_{/} = \sum_{i=1}^{m} k_i \cdot (2 \cdot k_i - 3), \tag{3}$$

Количество взятий модуля числа, выполняемых на данном этапе, выражается формулой:

$$N_{|a|} = \sum_{i=1}^{m} k_i \cdot (k_i - 1), \tag{4}$$

Шаг 3. Обновление мягких решений и получение жестких решений.

На данном этапе используются операции сложения для обновления мягких решений и операции сравнения с нулем для получения жестких решений. Количество сложений, выполняемых при обновлении мягких решений, выражается формулой:

$$N_{+} = \sum_{i=1}^{l} j_i, \tag{5}$$

Количество сравнений, выполняемых для получения жестких решений, выражается формулой:

$$N_{/} = l \tag{6}$$

Шаг 4. Расчет синдрома.

На данном этапе используются только операции сложения по модулю 2 для расчета синдрома. Количество сложений по модулю 2, выполняемых на данном этапе, выражается формулой:

$$N_{\oplus} = \sum_{i=1}^{m} (k_i - 1), \tag{7}$$

Итоговые формулы для расчета количества операций.

Общее число операций сложения на одну итерацию декодирования выражается формулой:

$$N_{+} = \sum_{i=1}^{l} j_i^2, \tag{8}$$

Общее число операций умножения на одну итерацию декодирования выражается формулой:

$$\boxed{N_{\times} = \sum_{i=1}^{m} k_i \cdot (k_i - 1)}, \tag{9}$$

Общее число сравнения умножения на одну итерацию декодирования выражается формулой:

$$\boxed{N_{/} = 1 + l + \sum_{i=1}^{m} k_i \cdot (2 \cdot k_i - 3)}, \tag{10}$$

Здесь, и далее для других алгоритмов, первый член суммы, равный 1, как и в [2], учитывает сравнение счетчика итераций с максимальным числом.

Общее число операций взятия модуля числа на одну итерацию декодирования выражается формулой:

$$\boxed{N_{|a|} = \sum_{i=1}^{m} k_i \cdot (k_i - 1)}, \tag{11}$$

Общее число операций сложения по модулю 2 на одну итерацию декодирования выражается формулой:

$$\boxed{N_{\oplus} = \sum_{i=1}^{m} (k_i - 1)}, \tag{12}$$

Общее число операций различного типа, необходимых для выполнения одной итерации декодирования по алгоритму «Min-sum» с низкоплотностной матрицей проверки на четность из Subframe2 размерностью 600 на 1200, содержащей 4818 ненулевых элементов, представлено в таблице 1. Приводимые далее количественные оценки вычислительной сложности для других алгоритмов декодирования получены для этой же матрицы проверки на четность.

Таблица 1 – Сложность алгоритма «Min-sum».

Операция	Количество на итерацию декодирования
Сложение	37024
Умножение	33888
Сравнение	64159
Взятие модуля	33888
Сложение по модулю 2	4218

Алгоритм «Min-sum normalized» имеет отличия от алгоритма «Min-sum» только расчетом сообщений от проверочных узлов графа Таннера (шаг 2). Как следствие, шаги 1,3 и 4 имеют одинаковую сложность и не описываются здесь.

Шаг 2. Расчет сообщений от проверочных узлов графа Таннера.

Для формирования сообщений от проверочных узлов к символьным узлам используются операции сравнения, умножения и взятия модуля числа. Количество умножений, выполняемых на данном шаге, выражается формулой:

$$\boxed{N_{\times} = \sum_{i=1}^{l} k_i^2}, \tag{13}$$

Количество сравнений и взятий модуля числа на данном шаге не претерпело изменений по сравнению с алгоритмом «Min - sum» и может быть вычислено по формулам (3) и (4), соответственно.

Итоговые формулы для расчета количества операций.

Общее число операций сложения на одну итерацию декодирования выражается формулой:

$$\boxed{N_{+} = \sum_{i=1}^{l} j_i^2}, \tag{14}$$

Общее число операций умножения на одну итерацию декодирования выражается формулой:

$$\boxed{N_{\times} = \sum_{i=1}^{m} k_i^2}, \tag{15}$$

Общее число операций сравнения на одну итерацию декодирования выражается формулой:

$$\boxed{N_{/} = 1 + l + \sum_{i=1}^{m} k_i \cdot (2 \cdot k_i - 3)}, \tag{16}$$

Общее число операций взятия модуля числа на одну итерацию декодирования выражается формулой:

$$\boxed{N_{|a|} = \sum_{i=1}^{m} k_i \cdot (k_i - 1)}, \tag{17}$$

Общее число операций сложения по модулю 2 на одну итерацию декодирования выражается формулой:

$$\boxed{N_{\oplus} = \sum_{i=1}^{m} (k_i - 1)}, \tag{18}$$

Общее число операций различного типа, необходимых для выполнения одной итерации декодирования по алгоритму «Min-sum normalized», представлено в таблице 2.

Таблица 2 – Сложность алгоритма «Min-sum normalized».

Операция	Количество на итерацию декодирования
Сложение	37024
Умножение	38706
Сравнение	64159
Взятие модуля	33888
Сложение по модулю 2	4218

Алгоритм «Min-sum offset» имеет отличия от алгоритма «Min-sum» только расчетом сообщений от проверочных узлов графа Таннера (шаг 2). Как следствие, шаги 1,3 и 4 имеют одинаковую сложность и не описываются здесь.

Шаг 2. Расчет сообщений от проверочных узлов графа Таннера.

Для формирования сообщений от проверочных узлов к символьным узлам используются операции сложения, сравнения, умножения и взятия модуля числа.

Количество сложений, выполняемых на данном шаге, выражается формулой:

$$\boxed{N_{+} = \sum_{i=1}^{m} k_i}, \tag{19}$$

Количество сравнений, выполняемых на данном шаге, выражается формулой:

$$\boxed{N_{/} = \sum_{i=1}^{m} k_i \cdot (2 \cdot k_i - 2)}, \tag{20}$$

Количество умножений и взятий модуля числа на данном шаге не претерпело изменений по сравнению с алгоритмом «Min - sum» и может быть вычислено по формулам (2) и (4), соответственно.

Итоговые формулы для расчета количества операций.

Общее число операций сложения на одну итерацию декодирования выражается формулой:

$$\boxed{N_{+} = \sum_{i=1}^{l} j_i^2 + \sum_{i=1}^{m} k_i}, \tag{21}$$

Общее число операций умножения на одну итерацию декодирования выражается формулой:

$$N_{\times} = \sum_{i=1}^{m} k_i \cdot (k_i - 1), \tag{22}$$

Общее число операций сравнения на одну итерацию декодирования выражается формулой:

$$N_{/} = 1 + l + \sum_{i=1}^{m} k_i \cdot (2 \cdot k_i - 2), \tag{23}$$

Общее число операций взятия модуля числа на одну итерацию декодирования выражается формулой:

$$N_{|a|} = \sum_{i=1}^{m} k_i \cdot (k_i - 1), \tag{24}$$

Общее число операций сложения по модулю 2 на одну итерацию декодирования выражается формулой:

$$N_{\oplus} = \sum_{i=1}^{m} (k_i - 1), \tag{25}$$

Общее число операций различного типа, необходимых для выполнения одной итерации декодирования по алгоритму «Min-sum offset», представлено в таблице 3.

Таблица 3 – Сложность алгоритма «Min-sum offset».

Операция	Количество на итерацию декодирования
Сложение	41842
Умножение	33888
Сравнение	68977
Взятие модуля	33888
Сложение по модулю 2	4218

Проанализировав алгоритм декодирования «Min-sum» и его модификации «Min-sum normalized» и «Min-sum offset» можем сделать вывод, что:

Сложность алгоритма «Min-sum normalized» имеет отличия от сложности алгоритма «Min-sum» на число умножений, равное количеству элементов в проверочной матрице низкоплотностного кода, то есть на количество отнормированных сообщений, которое формируется от проверочных узлов графа Таннера к символьным узлам.

Сложность алгоритма «Min-sum offset» имеет отличия от сложности алгоритма «Min-sum» на число сложений и сравнений, каждое из которых равно количеству элементов в проверочной

матрице низкоплотностного кода, то есть количеству сообщений, которое формируется от проверочных узлов графа Таннера к символьным узлам.

Список использованных источников:

1. V. Sh. Le. // Optimization of the min-sum decoding algorithm for low-density parity-check codes, 2021. P 16–17.
2. Soltanov A.G. // Decoding schemes and performance evaluation of LDPC codes. Application, advantages and development prospects // Security of information technologies, 2010, M.: No. 2, P. 61-67.
3. Wikipedia, the free encyclopedia [Electronic resource]. – Access mode: https://en.wikipedia.org/wiki/Computational_complexity. – Access date: 01.03.2023.

UDC 621.391

COMPLEXITY EVALUATION OF THE "MIN-SUM" DECODING ALGORITHM AND ITS MODIFICATIONS

Abramov I.O., Barabanov M.Y.

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

Astrovskiy I.I. – PhD in Engineering sciences

Annotation. This article provides an estimate of the complexity of the decoding algorithm for LDPC "min sum" codes and its modifications. Differences in the complexity of the "min-sum", "min-sum normalized", "min-sum offset" algorithms are shown.

Keywords. LDPC code, decoding algorithm, low-bandwidth matrix, computational complexity.

УДК 621.391

АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ НА ОСНОВЕ LOW-CODE

Аракелян К.Н., магистрантка 167001

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Шевчук О.Г. – канд. тех. наук, доцент

Доклад посвящен проблеме автоматизации бизнес-процессов с целью повышения эффективности бизнеса и Low-code системам, как инструментам автоматизации.

Бизнес-процесс – совокупность различных видов деятельности, в рамках которой «на входе» используется один или более видов ресурсов, и в результате этой деятельности «на выходе» создается продукт, представляющий ценность для потребителя [1].

Однако, сложно дать однозначное определение бизнес-процесса. С другой стороны, это логическая последовательность действий человека (или группы людей) в коллективе. Часто целью его описания является анализ и регламентация тех или иных действий. Зачастую бизнес-процесс происходит с участием человека в явной или неявной форме, что может отрицательно сказываться на компании.

На рисунке 1.1 представлено графическое изображение бизнес-процесса.

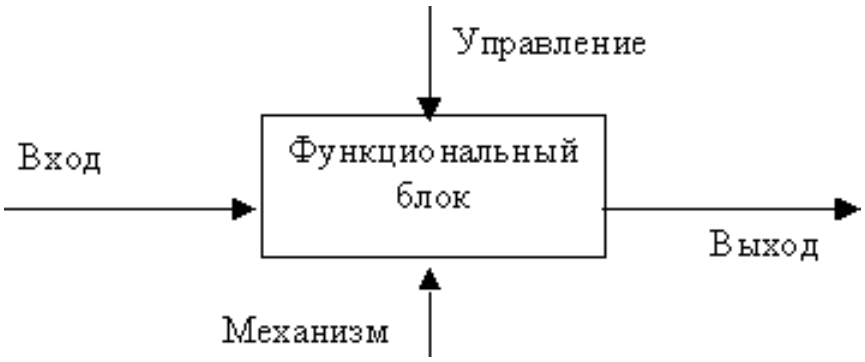


Рисунок 1 – Графическое изображение бизнес-процесса

Бизнес-процесс состоит из:

1 Выхода. Описывает то, что создается в результате деятельности, ее конкретную цель (ценность для клиента, ценность для заинтересованных лиц) – в частном случае, это товары и услуги.

2 Входа. Описывает то, что преобразуется или расходуется в процессе деятельности (например, сырье и материалы, заявка на выполнение работ, обращение клиента и т.п.).

3 Управления. Описывает целенаправленный характер деятельности и включает все допустимые управляющие воздействия (приказы, распоряжения, задания на выполнение работ и т.п.).

4 Механизма (ресурсов). Описывает ресурсы, используемые для достижения поставленной цели (например, оборудование, человеческие ресурсы). Их отличие от «Входа» в том, что они используются в производственном цикле многократно.

5 Функционального блока. Деятельность компании или ее части, по преобразованию «Входа» в «Выход», преследующего заданную цель, установленную в «Управлении» и использующая для этого имеющиеся «Ресурсы».

Для минимизации затрат и обеспечения масштабируемости компании часто используется автоматизация бизнес-процессов. Как было отмечено ранее, бизнес-процесс является последовательностью действий, которые зачастую выполняет человек. Однако, человеку тяжело работать с большим количеством информации вручную, что приводит к замедлению работы

компании и потребности вкладывать ресурсы для увеличения количества персонала. Поэтому все чаще прибегают к автоматизации бизнес-процессов.

Автоматизация бизнес-процессов (АБП) – это перенос наиболее часто выполняемых задач под контроль программно-аппаратного комплекса. С помощью таких сервисов становится возможным упростить выполнение ежедневных и рутинных задач без участия сотрудников [2].

АБП выполняет ряд задач:

1 Упрощение масштабируемости бизнеса. Когда компания растет, увеличивается объем информации, которую необходимо собирать, обрабатывать и хранить.

2 Увеличение прибыли. АБП позволяет повышать качество необходимых процессов с меньшим количеством сотрудников. Когда повседневные задачи организованы с помощью специальных программ, участие человека нужно только в нестандартных ситуациях.

3 Экономия времени. Некоторые процессы вообще не приносят компании доход, но они необходимы для жизненного цикла, иначе все остальные процессы остановятся. Автоматизация таких задач помогает сотрудникам сфокусироваться на делах, которые требуют творческого подхода или приносят прибыль.

4 Повышение эффективности и точности процессов. Есть процессы, в которых очень важна точность или долгосрочная работа над ним.

5 Улучшение процессов. Некоторые бизнес-процессы практически невозможно обработать вручную из-за большого количества информации. Автоматизация выводит компанию на новый уровень персонализации в работе с цифровыми данными и сотрудниками.

Однако сфера бизнеса изменяется с течением времени и находит отражение в тенденциях использования автоматизации бизнес-процессов для повышения эффективности. Одной из таких тенденций является переход на использование LCP (Low-code Platform) для гибкого управления бизнес-процессами. Платформы такого типа помогают руководителям отделов и бизнес-аналитикам снизить риски и решать актуальные проблемы бизнеса в кратчайшие сроки. LCP существенно упрощают автоматизацию бизнес-процессов благодаря удобным пользовательским инструментам для их моделирования, а также возможности внесения изменений без остановки действующих процессов.

Подобные решения имеют в своем составе готовые модули, компоненты и инструменты, что позволяет быстро создавать новые бизнес-приложения, добавлять, изменять и переиспользовать их функциональность. Нередко LCP по умолчанию включают необходимые инструменты для создания прототипов, отладки, версионирования и обновления своих решений.

На рисунке 1.1 представлены набор ключевой функциональности (что может входить в состав подобных платформ), а также этапы, которая проходит разработка, чтобы заложить потенциальную возможность настройки приложений без кода.

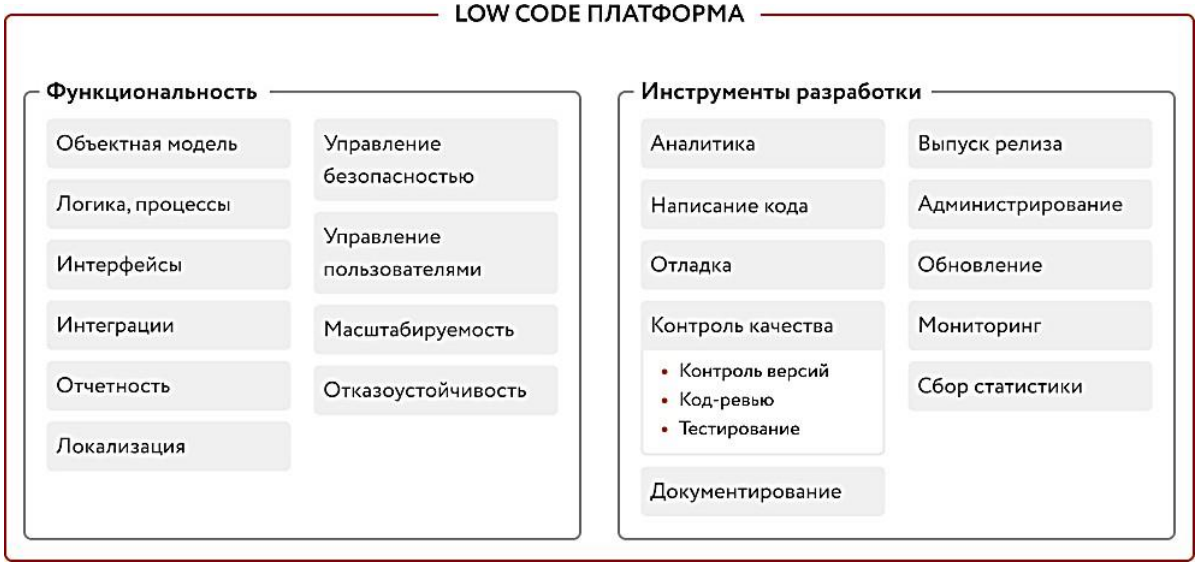


Рисунок 2 – Схема Low-code платформы

Вне зависимости от сферы применения Low-code позволяет «собирать» информационные системы и приложения различной сложности. Однако стоит обратить внимание на существование различных подходах у Low-code платформ – одни работают как конструктор: основная часть бизнес-логики задается через интерфейс, где пользовательские интерфейсы с функциями drag-and-drop заменяют традиционное программирование; другие лишь имеют готовое представление, но функциональную часть необходимо программировать кодом. Второй тип является более гибким.

Таким образом, Low-code системы в конечном счёте радикально сокращают сроки запуска в эксплуатацию IT-решений и обеспечивают быструю адаптацию к новым требованиям бизнеса, что является большим преимуществом в автоматизации.

Список использованных источников:

1. Хаммер М., Чампи Д. Реинжиниринг корпорации: манифест революции в бизнесе. - СПб., 2000. - 332
2. Davenport T. H., Short J. E. The New Industrial Engineering: Information Technology and Business Process Redesign//Sloan Management Review, 2010,, 11-27.

УДК 621.391

СИСТЕМА ДЛЯ АВТОМАТИЗАЦИИ ВЕДЕНИЯ ЖИЗНЕННОГО ЦИКЛА ПРОЕКТА

Аракелян К.Н., магистрант гр.167001

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Шевчук О.Г. – канд. тех. наук, доцент

Аннотация. В работе проанализированы преимущества автоматизации бизнес-процессов, разработана и описана Business Process Management система для компании производителя и дистрибьютора сельскохозяйственных удобрений на основе Microsoft Power Platform.

Ключевые слова. Автоматизация бизнес-процессов, Microsoft Power Platform, Low-code система.

Автоматизация бизнес-процессов может принести множество преимуществ [1]:

1 Улучшение эффективности: автоматизация позволяет ускорить выполнение рутинных задач, уменьшить количество ошибок и увеличить производительность. Это может привести к сокращению времени выполнения процессов и улучшению качества работы.

2 Снижение затрат: автоматизация может помочь сократить затраты на работу сотрудников, снизить расходы на бумагу и другие материалы, а также сократить затраты на обслуживание и поддержку систем.

3 Улучшение качества: автоматизация может помочь улучшить качество работы за счет снижения ошибок и повторяемости, а также улучшения контроля и наблюдаемости процессов.

4 Улучшение скорости: автоматизация позволяет сократить время, необходимое для выполнения процессов, а также повысить скорость реакции на изменения в бизнес-среде.

5 Улучшение точности: автоматизация позволяет снизить вероятность ошибок и повысить точность выполнения задач.

6 Увеличение прозрачности: автоматизация может улучшить наблюдаемость процессов и сделать их более прозрачными для сотрудников и руководителей.

7 Улучшение управления: автоматизация может упростить управление бизнес-процессами и улучшить возможности анализа производительности.

Эти преимущества могут помочь компаниям снизить затраты, повысить качество работы и улучшить конкурентоспособность на рынке. Поэтому в рамках настоящего проекта, была разработана Business Process Management система на основе Microsoft Power Platfrom.

Разрабатываемая BPM-система, как и большинство облачных технологий, имеющих архитектуру клиент-сервер, можно разделить на две части:

– backend-приложение. Отвечает за работу с базой данных и передает данные посредством API (Application Program Interface). Backend развернут непосредственно в сервисах Azure;

– frontend-приложение. Разрабатывалось на основе фреймворка Microsoft Power Apps.

Backend-приложение типа CRUD (сокращение от англ. Create, Read, Update, Delete), то есть обеспечивает четыре базовых функции работы с данными:

– создание;

– чтение;

– обновление;

– удаление.

Подключение и аутентификация в источнике данных выполняется отдельно от аутентификации в

службе Power Platform. Службы Power Platform обычно используют «коннекторы» для работы с внешними источниками данных, которые не являются Dataverse. Структурная схема (см. рисунок 1) иллюстрирует типичный путь с использованием соединителя управления API Azure (APIM).

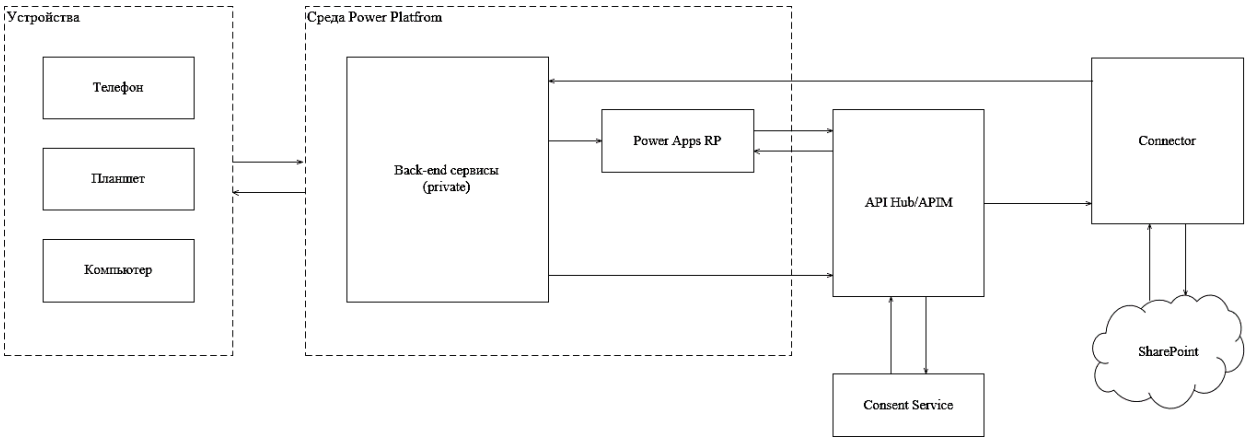


Рисунок 1 – Структурная схема backend-модуля

Frontend-модуль состоит из шести основных частей:
– главная страница веб-приложения;
– страница электронной формы 1;
– страница электронной формы 2;
– страница электронной формы 5A;
– страница электронной формы 5B;
– страница с деталями проекта и процессом утверждения.

Взаимодействие субъектов системы в рамках утверждения проекта приведены на рисунке 2.

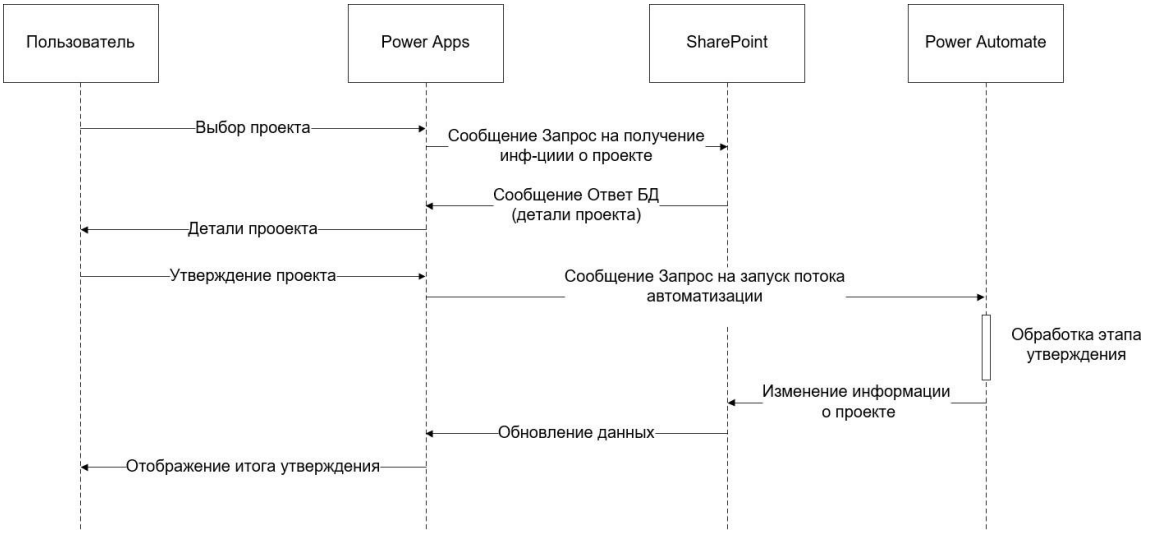


Рисунок 2 – Взаимодействие субъектов BPM-системы

Перед началом работы клиент попадает на страницу авторизации пользователя, где ему необходимо авторизоваться в системе. Если проверка не будет пройдена, то доступ пользователю будет ограничен.

После авторизации происходит вывод главной страницы с представлением данных о текущих проектах (см. рисунок 3). Далее возможно получение информации о проекте и выполнение

различных действий в зависимости от этапа проекта. Для обработки некоторых действий пользователя используются потоки автоматизации, которые обеспечивают обработку текущего действия и обновление данных в зависимости от исхода обработки. Затем данные возвращаются пользователю.

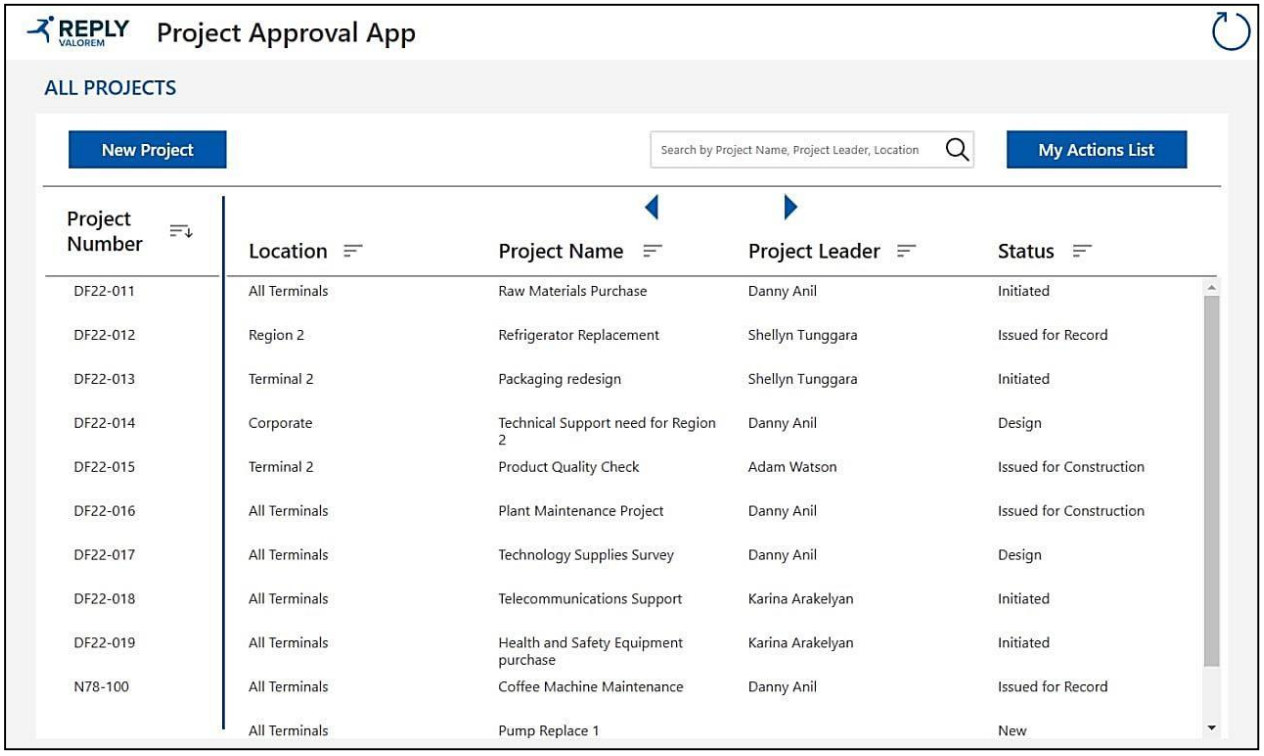


Рисунок 3 – Интерфейс главной страницы приложения

При создании нового проекта пользователь попадает на страницу заполнения формы, где есть возможность ввода первичной информации о проекте (см. рисунок 4). После отправки формы пользователь увидит уведомление об успешной отправке или ошибку, поясняющую причину, по которой запрос не был отправлен. Также во всем приложении предусмотрена валидация входных данных.

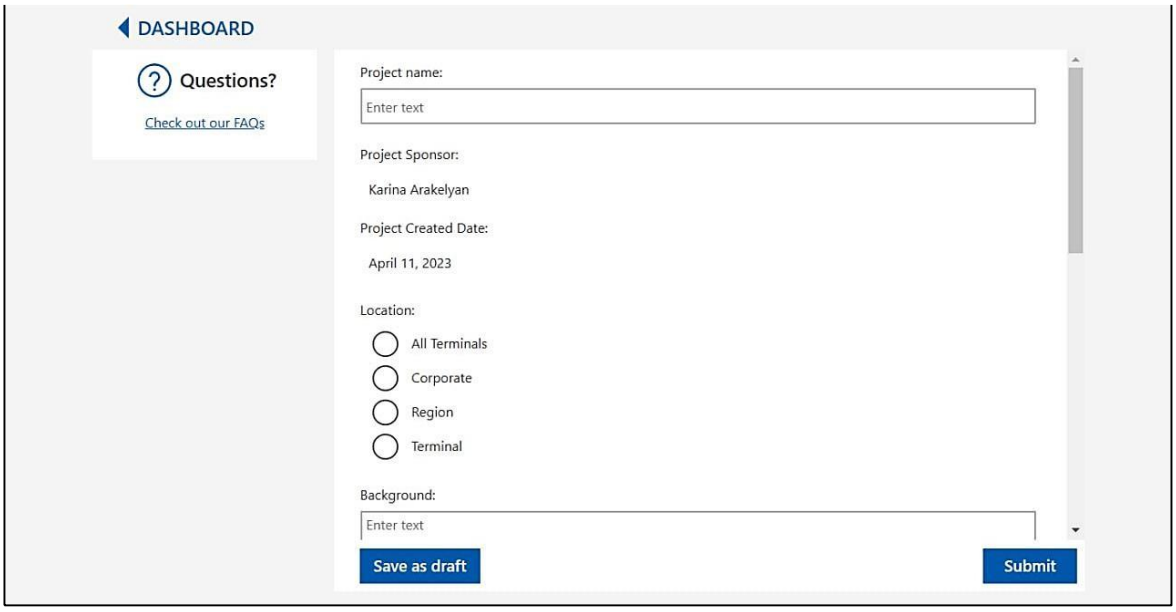


Рисунок 4 – Интерфейс формы инициации проекта

Также пользователь имеет возможность нажать на наименование проекта на главном экране, что приведет его на страницу с деталями проекта, текущим статусом, необходимыми действиями и историей пройденных этапов (см. рисунок 5).

Интерфейс будет отличаться в зависимости от роли текущего пользователя. Например, главному инженеру на вкладке деталей проекта будет доступна возможность редактирования и сохранения деталей проекта.

На вкладке «Actions» пользователь увидит доступные для него действия на данном этапе проекта. Первыми отображаются обязательные для выполнения действия, а затем необязательные, такие как смена ведущего инженера, запрос на изменение даты окончания проекта, добавление комментариев и так далее.

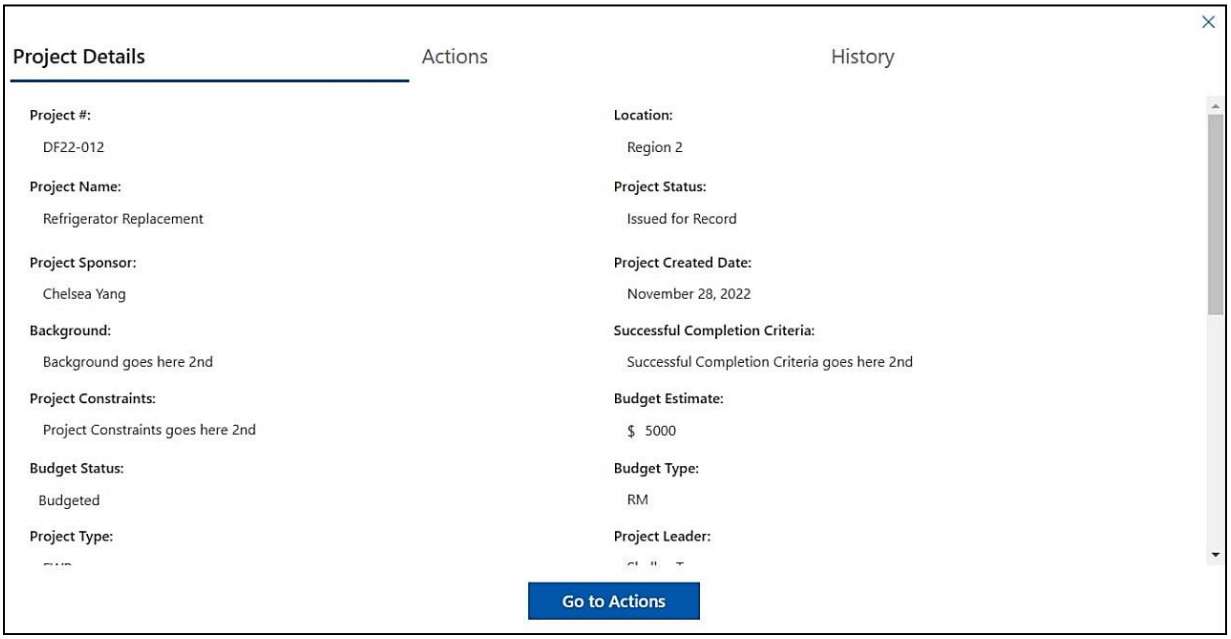


Рисунок 5 – Интерфейс страницы менеджмента проекта

Достоинствами системы являются: простота и удобство интерфейса, возможность выполнять действия над проектами, реализация по современным стандартам программирования и хорошая масштабируемость.

Список использованных источников:

1. Intelligent Process Automation: The engine at the core of the next-generation operating model [Электронный ресурс]. – Режим доступа: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/intelligent-process-automation-the-engine-at-the-core-of-the-next-generation-operating-model

UDC 621.391

AN AUTOMATED SYSTEM OF MANAGING THE PROJECT LIFECYCLE

Arakelyan K.N.

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

Shevchuk O.G. – PhD in technical sciences, associate professor

Annotation. This article provides an analysis of the benefits of automating business processes and describes the development of a Business Process Management system based on the Microsoft Power Platform for a manufacturer and distributor of agricultural fertilizers.

Keywords. Business process automation, Microsoft Power Platform, Low-code system.

УДК 621.391

ВЕКТОРНЫЙ ФИЛЬТР КАЛЬМАНА

Ахапкина А.М.[1], курсант гр. 033701

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Фильченкова Т.М. – магистр. технических наук

Аннотация. В данной статье приведены теоретические сведения и практические результаты выполнения векторного фильтра Калмана, который позволяет строить оценки подвижной модели и тем самым определять ее местоположение в пространстве относительно трех осей.

Ключевые слова. оценка, фильтр Калмана, марковская модель, шум, оси, GPS, матрица

Актуально определение местонахождения подвижных объектов (машин, самолетов, людей) как для частных, так и для государственных структур. Определение местоположения включает в себя три этапа: непосредственное определение местоположение, передача данных и управления, обработка данных.

Самым определяющим этапом является непосредственное определение местоположения движущегося объекта, ведь если на начальном этапе определить его неверно – последующие этапы будут бессмысленны. Так же не менее важным этапов является передача данных и управления подвижными объектами, который не должен затрачивать много времени.

Во многим системах GPS используется Калмановский подход, имеющий наименьшую погрешность.

В нем используется алгоритм оценки сразу по трем пространственным осям, где процедуры выполняются независимо от каждой:

$$\begin{cases} \hat{x}_k = u\left(z_k, \hat{x}_{k-1}\right) \\ \hat{y}_k = u\left(z_k, \hat{y}_{k-1}\right) \\ \hat{z}_k = u\left(z_k, \hat{z}_{k-1}\right) \end{cases} \qquad k = 1, 2, 3, \ldots \tag{1}$$

где u(○) – калмановский алгоритм построения текущей оценки.

Так как все три координаты прадставляют собой точку в трехмерном пространстве, то изменение положение объекта удобнее представить векторно-матричной марковской моделью:

$$\begin{bmatrix} x_k \\ y_k \\ z_k \end{bmatrix} = \begin{bmatrix} r_x & 0 & 0 \\ 0 & r_y & 0 \\ 0 & 0 & r_z \end{bmatrix} \cdot \begin{bmatrix} x_{k-1} \\ y_{k-1} \\ z_{k-1} \end{bmatrix} + \begin{bmatrix} \xi_{xk} \\ \xi_{yk} \\ \xi_{zk} \end{bmatrix} \tag{2}$$

или, в таких очевидных обозначениях:

$$\overline{x}_k = R \cdot \overline{x}_{k-1} + \overline{\xi}_k \tag{3}$$

Если предположить, что все случайные составляющие подчиняются нормальному закону распределения с нулевым средним и некоторыми дисперсиями. Например, для

$$M\left\{\overline{\xi}_k \cdot \overline{\xi}_k^T\right\} = M\left\{\begin{bmatrix}\xi_{xk}, \xi_{yk}, \xi_{zk}\end{bmatrix} \cdot \begin{bmatrix}\xi_{xk} \\ \xi_{yk} \\ \xi_{zk}\end{bmatrix}\right\} = \begin{bmatrix}\sigma_{\xi x}^2 & 0 & 0 \\ 0 & \sigma_{\xi y}^2 & 0 \\ 0 & 0 & \sigma_{\xi z}^2\end{bmatrix} = V_\xi \quad (4)$$

Модель наблюдения, соответственно, определяется вектором z:

$$\begin{bmatrix}z_{xk} \\ z_{yk} \\ z_{zk}\end{bmatrix} = \begin{bmatrix}x_k \\ y_k \\ z_k\end{bmatrix} + \begin{bmatrix}n_{xk} \\ n_{yk} \\ n_{zk}\end{bmatrix} \quad (5)$$

или, в векторном виде:

$$\overline{z}_k = \overline{x}_k + \overline{n}_k \quad (6)$$

Здесь дисперсии шумов будут образовывать диагональную матрицу:

$$M\left\{\overline{n}_k \cdot \overline{n}_k^T\right\} = M\left\{\begin{bmatrix}n_{xk} \\ n_{yk} \\ n_{zk}\end{bmatrix} \cdot \begin{bmatrix}n_{xk}, n_{yk}, n_{zk}\end{bmatrix}\right\} = \begin{bmatrix}\sigma_{nx}^2 & 0 & 0 \\ 0 & \sigma_{ny}^2 & 0 \\ 0 & 0 & \sigma_{nz}^2\end{bmatrix} = V_k \quad (7)$$

Имеем векторную марсковскую модель изменения объекта в пространстве и вектор наблюдений текущего местоположения объекта (рисунок 1):

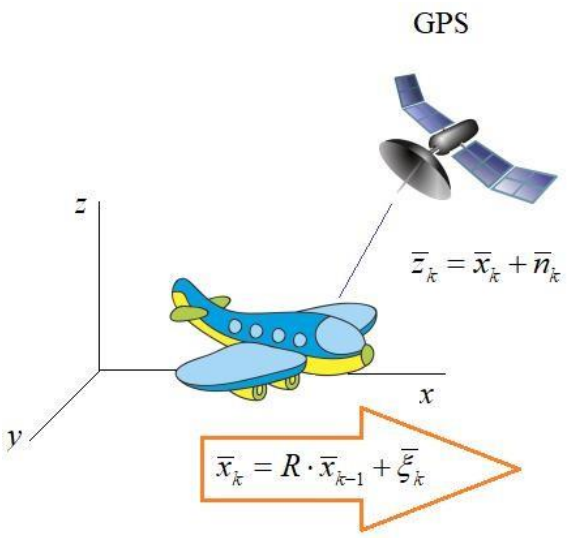


Рисунок 1 – Векторная марковская модель изменения местоположения самолета

Когда на вход приемника приходит самое первое наблюдение, то лучшая оценка – это значение самого наблюдения:

$$\hat{\bar{x}}_1 = z_1 \tag{8}$$

с дисперсией ошибок оценивания:

$$P = V_1 \tag{9}$$

В следующий момент времени модель (самолет) немного меняет свое местоположение и на вход GPS-приемника приходит очередное наблюдение:

$$\bar{z}_2 = \bar{x}_2 + \bar{n}_2 \tag{10}$$

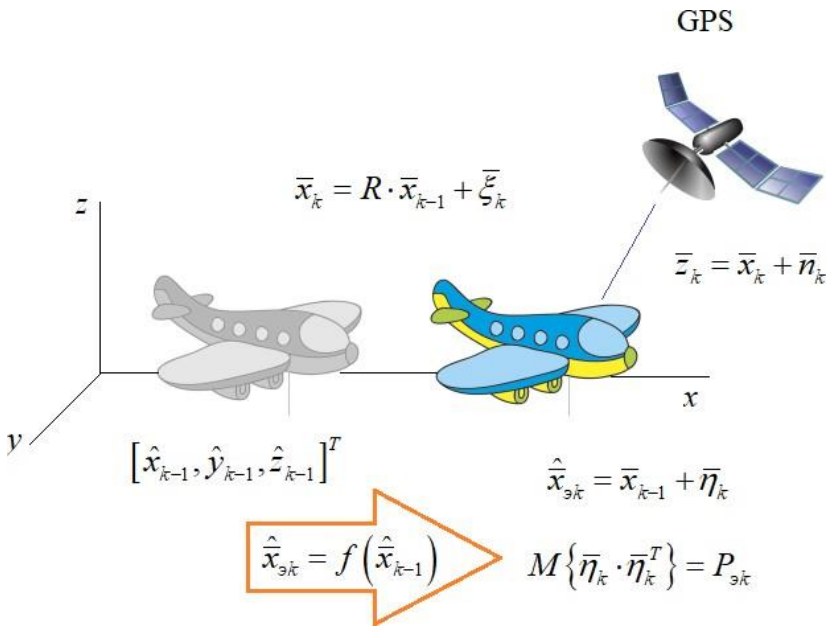


Рисунок 2 – Векторная марковская модель (самолет) в следующий момент времени

В данной ситуации при построении оценки текущего местоположения воспользуемся двумя наблюдениями. Первое – вектор $\vec{z_2}$, а второе наблюдение берется как прогноз текущего положения из предыдущей оценки $\vec{x}_1$, используя марковскую модель движения:

$$\hat{\bar{x}}_{э2} = R \cdot \hat{\bar{x}}_1 \tag{11}$$

Затем вычисляется дисперсия ошибок прогноза, которая равна:

$$P_{э2} = M\left\{\left(\bar{x}_2 - R\hat{\bar{x}}_1\right)^2\right\} = M\left\{\left(R\bar{x}_1 + \bar{\xi}_2 - R\hat{\bar{x}}_1\right)^2\right\} =$$
$$= RM\left\{\left(\bar{x}_1 - \hat{\bar{x}}_1\right)^2\right\} R^T + V_\xi = R \cdot P_1 \cdot R^T + V_\xi \tag{12}$$

В результате имеются все необходимые данные для построения оценок координат на текущем шаге с помощью векторного фильтра Калмана. Используя формулы скалярного фильтра:

$$P_k = \frac{P_{эk} \cdot \sigma_k^2}{P_{эk} + \sigma_k^2}, \qquad \hat{x}_k = \hat{x}_{эk} + \frac{P_k}{\sigma_k^2} \cdot \left(z_k - \hat{x}_{эk}\right) \tag{13}$$

Обобщенно для векторно-матричного случая:

$$P_k = P_{эk} \cdot V_k \cdot \left(P_{эk} + V_k\right)^{-1}, \qquad \hat{\bar{x}}_k = \hat{\bar{x}}_{эk} + P_k \cdot V_k^{-1} \cdot \left(\bar{z}_k - \hat{\bar{x}}_{эk}\right) \tag{14}$$

В данном случаи формально преобразовано скалярное выражение в векторное и получено возможность строить векторы оценок. В этот состоит одно из достоинств векторов и матриц: оно позволяют легко обобщать задачи на многомерный случай.

На втором шаге имеются следующие вычисления:

$$P_2 = P_{э2} \cdot V_2 \cdot \left(P_{э2} + V_2\right)^{-1}, \qquad \hat{\bar{x}}_2 = \hat{\bar{x}}_{э2} + P_2 \cdot V_2^{-1} \cdot \left(\bar{z}_2 - \hat{\bar{x}}_{э2}\right) \tag{15}$$

Вычисления на последующих шагах вычисляются рекуррентно по формулам (15).

Для реализации векторного фильтра Калмана на Python необходимо учесть, что при условии некоррелированности и шумов и независимости перемещений по каждой из координат, получено тни независимых канала оценивания параметров x,y,z:

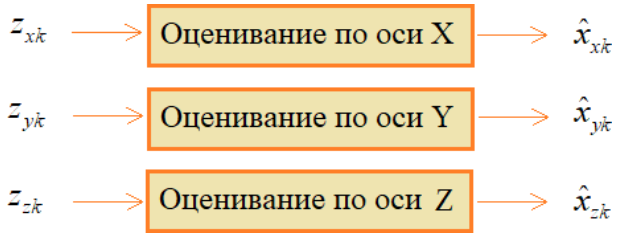


Рисунок 3 – Независимые каналы оценивания параметров

Однако, если модифицировать модель и учесть в ней скорости движения объекта по каждой координат, то получится взаимосвязь между наблюдаемыми скоростями и соответствующей координаты:

$$\begin{bmatrix} x_i \\ y_i \\ z_i \\ v_{xi} \\ v_{yi} \\ v_{zi} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & r_x & 0 & 0 \\ 0 & 0 & 0 & 0 & r_y & 0 \\ 0 & 0 & 0 & 0 & 0 & r_z \end{bmatrix} \cdot \begin{bmatrix} x_{i-1} \\ y_{i-1} \\ z_{i-1} \\ v_{xi-1} \\ v_{yi-1} \\ v_{zi-1} \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \xi_{vxi} \\ \xi_{vyi} \\ \xi_{vzi} \end{bmatrix} \tag{16}$$

Причем, векторный фильтр Каламана автоматически наилучшим образом скомбинирует эти набюлдения для вычисления оптимальной выходной оценки в соответствии с описанной моделью перемещения. И это очень удобно, ведь не нужно решать систему линейных уравнений, находить оптимальные коэффициенты, все аккуратно расписывать. Все это делается автоматически при вычислении обратных матриц в фильтре Калмана.

Далее, для второго варианта матрицы дисперсий порождающего шума и шума наблюдений, будут выглядеть следующим образом:

$$V_\xi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma_\xi^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sigma_\xi^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sigma_\xi^2 \end{bmatrix} \quad V = \begin{bmatrix} \sigma^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sigma^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sigma^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma_v^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \sigma_v^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sigma_v^2 \end{bmatrix} \tag{17}$$

Весь остальной алгоритм оценивания будет прежним:

$$P_k = P_{3k} \cdot V_k \cdot \left(P_{3k} + V_k\right)^{-1}, \qquad \hat{\bar{x}}_k = \hat{\bar{x}}_{3k} + P_k \cdot V_k^{-1} \cdot \left(\bar{z}_k - \hat{\bar{x}}_{3k}\right) \tag{18}$$

```
N = 100          # число наблюдений
dNoise = 1       # дисперсия шума
dSignal = 5      # дисперсия сигнала
r = 0.99         # коэффициент корреляции в модели движения
en = 0.1         # дисперсия СВ в модели движения

M = 3            # размерность вектора координат положения объекта
```

Рисунок 4 – Задание параметров для построения оценок

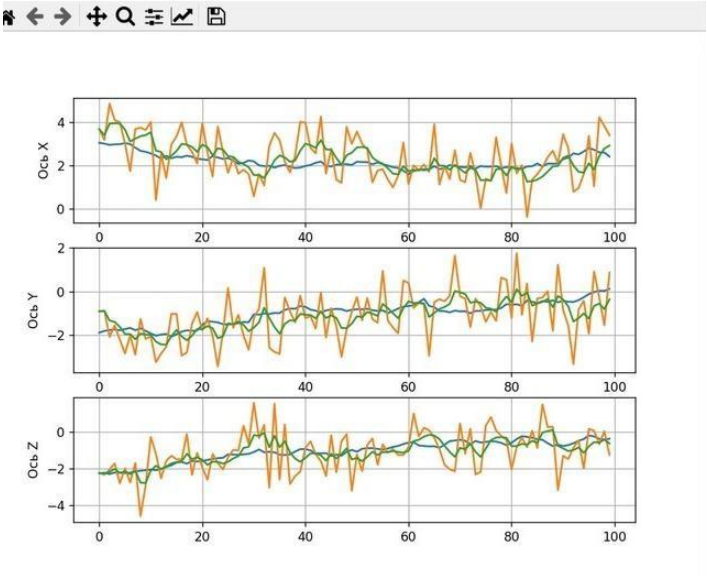


Рисунок 5 – Результат выполнения программы

Список использованных источников:

1. Mohamed Laaraiedh «Implementation of Kalman Filter with Python Language» // paper, 2012
2. Бутковский, О.А «Предельные теоремы для марковских процессов» // диссертация, 2013.
3.Пучков, А.Ю «Разработка методов фильтрации в постановке Р. Калмана в условиях случайной дискретизации сигналов» // диссертация, 2019.

УДК 004.855

ОБЗОР АКТУАЛЬНОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ВЫЧИСЛЕНИЯ ОПТИМАЛЬНОГО КОЛИЧЕСТВА НЕЙРОННЫХ СЛОЁВ И НЕЙРОНОВ В СЛОЕ

Барабанов М.Ю., Абрамов И.О. магистрант гр.167001

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Астровский И.И. – канд. техн. наук

Аннотация. В данной статье приводиться обзор актуальных исследований по теме влияния количества нейронных слоев и нейронов в слое на общую характеристику искусственной нейронной сети. Найдены наиболее распространенные подходы.

Ключевые слова. Искусственная нейронная сеть, нейронный слой, машинное обучение, обзор.

Искусственные нейронные сети являются мощным инструментом для решения различных задач, включая распознавание образов, классификацию, регрессию, распознавание речи, машинный перевод и т.д. Одним из ключевых параметров нейронной сети является количество нейронных слоев и нейронов в каждом слое. Оптимальный выбор количества слоев и нейронов может существенно повлиять на производительность искусственной нейронной сети и качество ее работы. Об этом напрямую может свидетельствовать улучшение лингвистической нейронной модели GPT с каждой последующей версией [1]: увеличение количества слоев продемонстрировано на рисунке 1.

Model Name	n_{params}	n_{layers}	d_{model}	n_{heads}	d_{head}	Batch Size	Learning Rate
GPT-3 Small	125M	12	768	12	64	0.5M	6.0×10^{-4}
GPT-3 Medium	350M	24	1024	16	64	0.5M	3.0×10^{-4}
GPT-3 Large	760M	24	1536	16	96	0.5M	2.5×10^{-4}
GPT-3 XL	1.3B	24	2048	24	128	1M	2.0×10^{-4}
GPT-3 2.7B	2.7B	32	2560	32	80	1M	1.6×10^{-4}
GPT-3 6.7B	6.7B	32	4096	32	128	2M	1.2×10^{-4}
GPT-3 13B	13.0B	40	5140	40	128	2M	1.0×10^{-4}
GPT-3 175B or “GPT-3”	175.0B	96	12288	96	128	3.2M	0.6×10^{-4}

Рисунок 1 – Данные об улучшениях лингвистической модели GPT

Многие исследования были проведены для определения оптимального количества нейронных слоев и нейронов в каждом слое. Некоторые из этих исследований описывают определенные методы и эвристики для выбора количества слоев и нейронов, в то время как другие исследования сравнивают различные архитектуры ИНС, чтобы определить, какая из них является наилучшей для данной задачи.

Существует несколько подходов к определению оптимального количества слоев и нейронов. Один из таких подходов - это эмпирический метод, основанный на экспериментальном тестировании различных конфигураций сетей. Однако этот метод является довольно затратным по времени и ресурсам, так как в некотором смысле основан на удаче подбора данных.

Другой подход основан на математических моделях, таких как теория информации и теория сложности. В этих моделях оптимальное количество слоев и нейронов определяется с учетом статистических свойств данных, на которых будет работать сеть. Однако эти модели могут быть достаточно сложными и трудными для понимания.

Одним из основных критериев количества нейронных слоев долгое время была теорема Цыбенко, она же универсальная теорема аппроксимации. Данная теорема, доказанная Джорджем Цыбенко в 1989 году, утверждает, что искусственная нейронная сеть прямой связи (в которых связи не образуют циклов) с одним скрытым слоем может аппроксимировать любую непрерывную функцию многих переменных с любой точностью. Условиями выполнения являются: достаточное

количество нейронов скрытого слоя, удачный подбор весов нейронов скрытого и выходного нейрона, а также смещения весов входного слоя. [2]

Однако, более новые исследования показали, что использование нескольких скрытых слоев может привести к лучшим результатам для некоторых задач. [3] Хотя эта теорема утверждает, что достаточно одного скрытого нейронного слоя для любой задачи, она не говорит ничего о времени требуемое на обучение этой системы и количество нейронов внутри скрытого слоя, число которых может потребоваться значительно больше, чем в архитектуре с двумя и более скрытыми нейронными слоями.

Долгое время использовался только один скрытый нейронный слой по причине технической ограниченности в обучении большого количества слоев. Изменение произошло в 2006 году после выхода работы Hinton и Osindero, основной особенностью которой является алгоритм быстрого обучения глубоких сетей. [4]

Далее, в статье [2] было проведено исследование оптимального количества нейронов в скрытых слоях для классификации изображений. Авторы рассмотрели наборы данных MNIST и CIFAR-10 и исследовали производительность нейронных сетей с различным количеством нейронов в скрытых слоях. Они показали, что оптимальное количество нейронов может варьироваться в зависимости от конкретной задачи и набора данных.

Другие исследования сравнивают различные архитектуры искусственных нейронных сетей, такие как персептрон, многослойный персептрон, сверточная нейронная сеть и рекуррентная нейронная сеть. Например, в статье "ImageNet Classification with Deep Convolutional Neural Networks" авторы использовали сверточные нейронные сети для классификации изображений на датасете ImageNet и достигли значительного улучшения результатов по сравнению с традиционными методами, включая многослойные персептроны. [6] Таким образом, важно понимать не только сложность работы нейронной сети для определения количества слоев, но также и её архитектуру, так как разные нейронные слои могут по-разному обрабатывать нужные типы данных.

Наиболее частые рекомендации, упомянутые в сети Интернет, по определению количества нейронных слоев для создания нейронной сети продемонстрированы в таблице 1.

Таблица 1 – Общие сведенья о количестве

Количество скрытых слоев	Применение
0	Только способно представлять линейные разделимые функции или решения
1	Может аппроксимировать любую функцию, которая содержит непрерывное отображение из одного конечного пространства в другое
2	Может представлять произвольную границу решения с произвольной точностью с рациональными функциями активации и может аппроксимировать любое гладкое отображение с любой точностью.
Более 2	Дополнительные слои могут изучать сложные представления (своего рода автоматическая разработка признаков) для слоев слоев

Важно понимать, что определение числа слоев нейронной сети недостаточно для построения нейронной сети, важно также определить количество нейронов в каждом слое. Чаще всего в задачах регрессии и распознавания, количество нейронов с каждым последующим слоем уменьшается, что следует из работы сети. Однако не все задачи сводятся к такому рода работе. Из наиболее частых рекомендаций по определению количества нейронов можно найти следующие:

- Количество скрытых нейронов должно быть между размером входного слоя и размером выходного слоя.;
- Количество скрытых нейронов должно составлять 2/3 размера входного слоя плюс размер выходного слоя.;
- Количество скрытых нейронов должно быть менее чем в два раза больше размера входного слоя.

Результаты, которые могут быть получены на основе нейронных сетей с разным количеством слоев могут сильно отличаться, так как сети получив одинаковое количество обучаемого материала по-разному смогут адаптироваться к нему. Опасным может быть не только недообучение сети, но и переобучение, когда построенная модель хорошо объясняет примеры из обучающей выборки [7][8],

но относительно плохо работает на примерах, не участвовавших в обучении. Нагляднее процесс переобучения можно увидеть на рисунке 2.

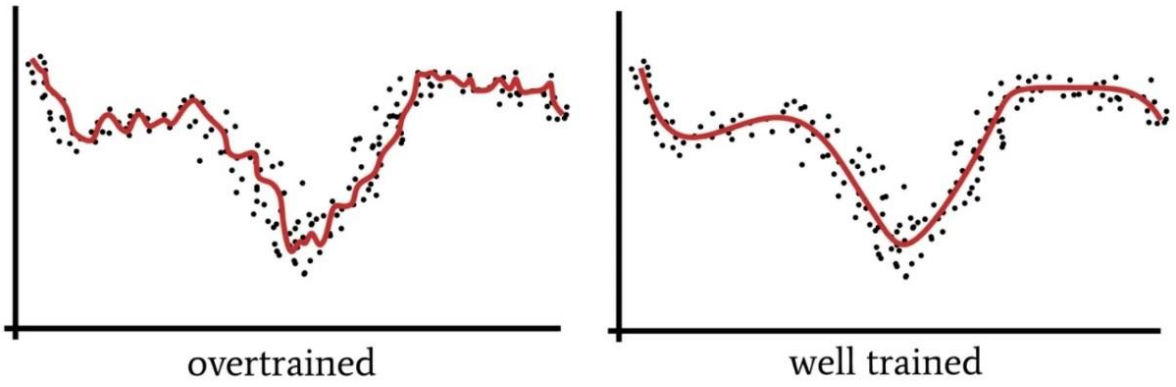


Рисунок 2 – Результаты переобученной и хорошо натренированной ИНС

Именно поэтому так важно определение количества нейронных слоев и нейронов в слое для дальнейшего создания и тренировки в сети, ведь как малое, так и чрезмерное количество слоев и нейронов могут привести к неудачным результатам.

В целом, определение оптимальной конфигурации нейронной сети - это сложная задача, которая требует сбалансированного подхода и учета множества факторов. Из многих исследований, проведенных в области определения оптимального количества нейронных слоев и нейронов, можно сделать вывод, что нет универсального правила для выбора архитектуры ИНС. Несмотря на это, исследователи продолжают работать над различными методами и подходами для решения этой задачи. Оптимальное количество слоев и нейронов зависит от конкретной задачи, объема данных и других факторов, поэтому необходимо проводить тщательный анализ с регулярной проверкой системы эмпирическими результатами.

Список использованных источников:

1. Tom B. Brown, Benjamin Mann, Nick Ryder // Language Models are Few-Shot Learners - 2020. P. 6

2. Approximation by superpositions of a sigmoidal function [Электронный ресурс] – режим доступа: https://web.archive.org/web/20151010204407/http://deeplearning.cs.cmu.edu/pdfs/Cybenko.pdf

3. LeCun, Y., Bengio, Y., & Hinton, G.// Deep learning. Nature 521(7553), – 2015 - P. 436-444.

4. A fast learning algorithm for deep belief nets ∗ [Электронный ресурс] – режим доступа: https://www.cs.toronto.edu/~hinton/absps/fastnc.pdf

5. Srivastava, N. // Dropout: a simple way to prevent neural networks from overfitting. The Journal of Machine Learning Research Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. - 2014 – P.15

4. Zhang, W., & Du, Y. // An empirical study on the optimal number of hidden neurons in neural network. IEEE Access – 2018 – P. 4850-4862.

6. ImageNet Classification with Deep Convolutional Neural Networks [Электронный ресурс] – режим доступа: https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf

7. Simonyan, K., & Zisserman, A. //. Very deep convolutional networks for large-scale image recognition. – 2015 – P. 1409-1556.

8. Muhammad Uzair. Effects of Hidden Layers on the Efficiency of Neural networks Muhammad Uzair, Noreen Jamil. // IEEE 23rd International Multitopic Conference – 2020

УДК 53.047

МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ТКАНИ ТЕЛА ЧЕЛОВЕКА ЧАСТОТОЙ 2.4 ГГц

Бекабаев Д.Д., магистрант гр.167001, Савицкий В.А. – магистр. тех. наук, аспирант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Шевчук О.Г. – канд. тех. наук

Аннотация. В статье рассматривается влияние электромагнитного излучения на ткани человеческого тела частотой 2,4 ГГц. Приведены диэлектрические параметры человеческих тканей для данной частоты, а также физико-термические свойства слоев кожи.

Ключевые слова. электрическое поле, магнитное поле, электромагнитое поле, электромагнитное излучение

Характер взаимодействия ЭМП (электромагнитного поля) с различными тканями определяется их электрическими и магнитными свойствами. Параметрами этих свойств являются: удельная электропроводность ϭ, характеризующая концентрацию и подвижность свободных заряженных частиц биологических тканей, а также их диэлектрическая (ε) и магнитная (μ) проницаемость. Они отражают степень уменьшения силовых характеристик электрического и магнитного полей в различных тканях по сравнению с вакуумом. На основе этих параметров можно рассчитать силовые характеристики электромагнитного поля в тканях и количественно оценить процессы, происходящие при воздействии ЭМП на ткани. В состав различных тканей и сред организма входят ионы, пространственно ориентированные полярные и неполярные макромолекулы различных линейных размеров и диполи воды. Разные ткани содержат их в неодинаковой пропорции, поэтому каждая из них обладает различными диэлектрическими свойствами и электропроводностью.

Электропроводность живых тканей определяется концентрацией ионов и их подвижностью. В межклеточной жидкости с максимальным содержанием носителей тока – ионов – удельная электропроводность достаточно высока и составляет 1 См/м. В цитозоле, содержащем органеллы и крупные белковые макромолекулы, напротив, она понижается до 0.003 См/м. Удельная электропроводность плазмолеммы и внутриклеточных мембран, составляющих до 50 % массы клетки, еще ниже: $(1 – 3)\ 10^{-11}$ См/м. Электропроводность кожи зависит от ее толщины, состояния дериватов и содержания воды. Толщина эпидермиса большинства участков тела составляет 0,07 – 0,12 мм.

Из-за малого количества межклеточной жидкости и выраженной компартментализации (наличия мембранных ячеек) цитозоля. существенно ограничивающей подвижность содержащихся в нем ионов, удельная электропроводность целых органов и тканей значительно меньше, чем составляющих их сред.

Диэлектрическая проницаемость характеризует способность к пространственному смешению структур тканей и образованию объемного дипольного момента (поляризации). Она обусловлена преимущественно связанными зарядами, полярными и неполярными макромолекулами различных линейных размеров и диполями воды. Относительная диэлектрическая проницаемость различных тканей для постоянного электрического поля составляет $10^3 – 10^6$. Кардинальной особенностью организма человека является наличие частотной зависимости (дисперсии) пассивных электрических свойств тканей, связанных с неодинаковым состоянием заряженных частиц, при воздействии ЭМП различной частоты.

В отличие от электрического поля биологические ткани ослабляют внешнее магнитное поле в очень малой степени (порядка 0,001%). Большинство из них относятся к диамагнетикам (сумма орбитальных и спиновых магнитных моментов составляющих их биологических молекул равна нулю), которые слабо преобразуют энергию магнитного поля. Энергия магнитного поля, поглощаемая, например, плазмолеммой. не превышает 10^{-26} Дж. Магнитная проницаемость клеток и практически всех жидкостей организма составляет 0,99995. Лишь некоторые молекулы, входящие в состав различных структур организма (молекулярный кислород, соли железа, некоторые гидроперекиси и радикалы), имеют суммарный магнитный момент, не зависящий от внешнего магнитного поля. Такие низкомолекулярные соединения относят к парамагнетикам, магнитная проницаемость которых составляет 1,00005. Различие магнитных проницаемостей диа- и

парамагнетиков существенно не изменяет характера взаимодействия последних с внешним магнитным полем, так как их величины имеют одинаковый порядок.

Известны исследования по электрическим характеристикам различных типов тканей организма []. В большинстве случае результаты исследований были опубликованы с указанием конкретных частот или диапазонов частот. Было показано, что электрические характеристики тканей организма зависят от частоты, и при моделировании значение эти характеристик должны быть интерполированы с учетом частоты и типа тканей организма.

Для моделирования индуцированной плотности тока или других параметров, таких как плотность потока энергии, SAR и воздействие полей, можно также использовать упрощенную форму однородного тела с равномерной удельной электропроводностью. Подходящими для моделирования тела человека являются вытянутые сфероиды и однородные модели тела. Простые диски и кубоиды также часто используются в качестве методов для подтверждения вычислений, так как геометрию и ситуацию воздействий легче смоделировать, а затем сравнить с известными результатами и теоретическими данными.

Диэлектрические свойства такой модели часто являются усредненными для всего тела на рассматриваемых частотах, но могут, напротив, быть типичными для отдельных частей тела или типов тканей организма, в таблице 1 представлены значения параметров диэлектрических свойств слоев человеческих тканей.

Таблица 1 – Диэлектрические свойства слоев кожи

Ткань	2,4 ГГц	
	Диэлектрическая проницаемость, ε	Проводимость σ, См/м
Эпидермис	3,39	0,3
Дерма	4,28	18,2
Подкожный жир	3,76	7,1
Мышцы	24,4	33,6

Реакции тканей организма на термические факторы определяются их теплофизическими свойствами. Параметры теплофизических свойств тканей организма приведены в таблице 2

Таблица 2 – Физико-термические свойства слоев кожи

Ткань	Удельная теплоемкость C, Дж/кг * К	Удельная теплопроводность К,Вт/м*К	Плотность p, кг/м^3	Толщина x, м
Эпидермис	3600	0,235	1190	0,00008
Дерма	3300	0,445	1116	0,002
Подкожный жир	2700	0,185	971	0,01
Мышцы	4000	0,5	1000	0,03

Модель кожи, состоящая из четырех разных слоев, а именно: эпидермис, дерма, подкожный жир и мышцы подвергаются воздействию частоты мобильной связи 2.4 ГГц (рисунок 1). Микрополосковая антенна располагается на расстоянии 2 см от слоя эпидермиса. Электромагнитная энергия передается во входной порт антенны, далее в окружающее пространство и поглощается многослойной кожной тканью.

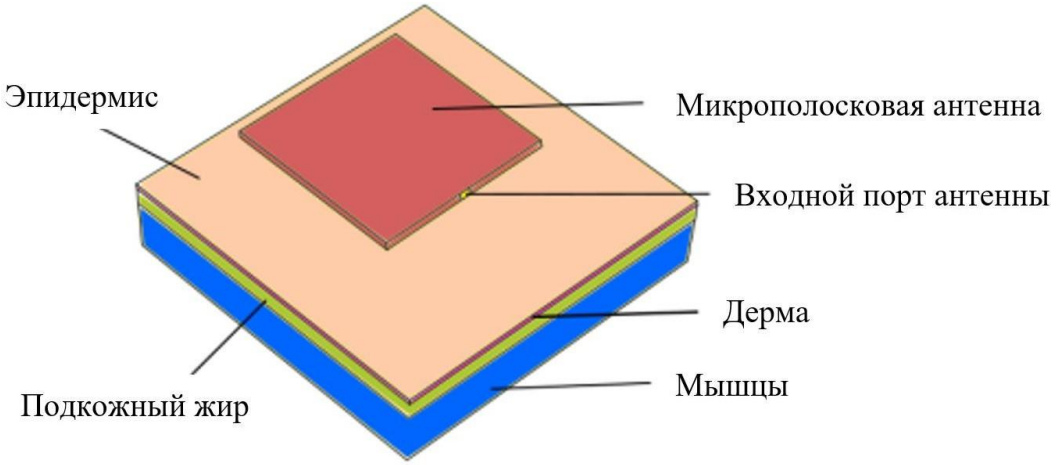


Рисунок 1 – Схематическая геометрия многослойной кожной ткани с патч антенной

Структура патч антенны представлена на рисунке 2, а ее параметры для выбранной ранее частоте представлены в таблице 3.

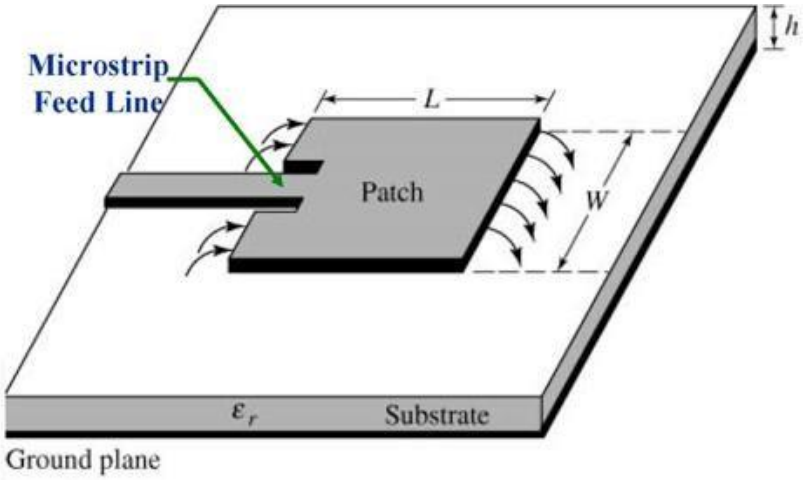


Рисунок 2 – Структура патч антенны

Таблица 3 – Параметры патч антенны

Частота, ГГц	Диэлектрическая проницаемость ε_r	Толщина диэлектрика h, мм	Ширина антенны W, мм	Длина антенны L, мм
2,4	4,7	0,2	37,0	28,8

На основании приведенных ранее данных проведено моделирование в программном продукте CST Studio Suite, полученные результаты представлены на рисунках 3 и 4.

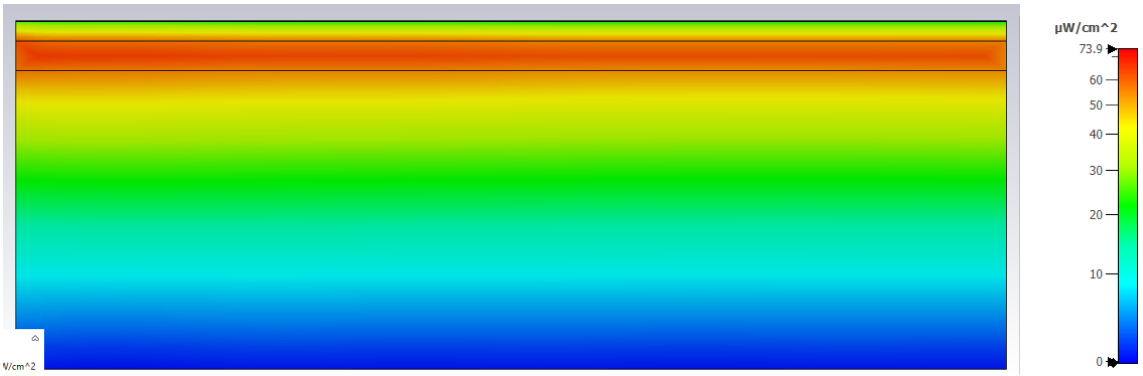


Рисунок 3 – Плотность потока энергии электромагнитного излучения в тканях тела человека при воздействии частотой 2.4 ГГц

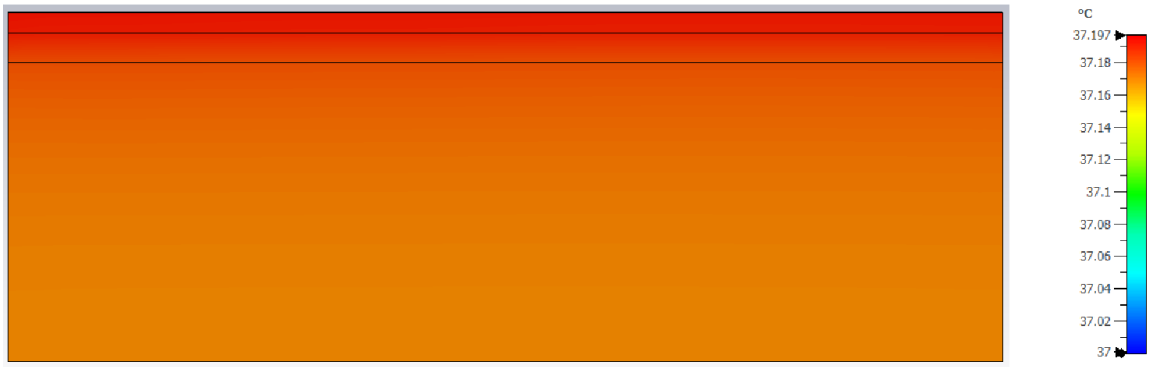


Рисунок 4 – Нагрев тканей в результате воздействия электромагнитного излучения в тканях тела человека при воздействии частотой 2.4 ГГц

Нагрев эпидермиса и дермы, при воздействии электромагнитным излучением частотой 2.4 ГГц составил 0,2 градуса, при этом плотность потока энергии электромагнитного излучения (ППЭ) составила 73,9 мкВт/см^2. В соответствии с [3] при продолжительности воздействия менее 3,0 часов данное воздействие электромагнитным излучением на ткани тела человека допускается.

Список использованных источников:

1. Гигиеническая оценка электромагнитных излучений : учебно-методическое пособие / И.В. Скоробогатая, Э.И Леонович. – Минск : БГМУ, 2018. – 39 с..

2. IEC Committee Draft (CD) 85/214/CD: Measurement and evaluation of high frequency (9 kHz yo 300 GHz) electromagnetic fields with regard to human exposure.

3. Санитарные нормы и правила «Требования к электромагнитным излучениям радиочастотного диапазона при их влздействии на человека от 05.03.2015.

УДК 621.317.3

МЕТОДИКА ПОВЕРКИ ПРИБОРА КАБЕЛЬНОГО ИРК-ПРО ГАММА

Валова И.Н., магистрантка группы 267041

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

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

Аннотация. В работе описаны методики поверки кабельного прибора ИРК-ПРО Гамма. Приводятся метрологические характеристики поверяемого прибора и выбранных эталонных средств поверки, схемы поверки и значения поверяемых точек, а также способы оценки погрешностей измерений.

Ключевые слова. Методика, поверка, прибор, кабельный.

При строительстве кабельных линий связи и дальнейшей их надежной эксплуатации большую роль играет метрологическое обеспечение (МО). Одной из важных задач МО является контроль метрологических характеристик (МХ) используемых измерительных приборов, который на разных стадиях жизненного цикла приборов осуществляется при проведении государственных испытаний, поверки, калибровки и метрологической экспертизы. Эти виды работ по метрологической оценке выполняются с использованием специально разработанных научно-обоснованных методик.

В статье рассматривается методика поверки (МП) прибора кабельного ИРК-ПРО Гамма. МП разработана в соответствие с требованиями [1].

Прибор ИРК-ПРО Гамма предназначен для определения расстояния до места изменения волнового сопротивления всех типов кабелей, измерения сопротивления изоляции, сопротивления шлейфа и электрической емкости кабеля, определения омической асимметрии, а также работу в режиме импульсного рефлектометра, предназначенного для определения расстояний до мест сосредоточенных неоднородностей.

При поверке прибора определяются его следующие основные МХ: определение абсолютной погрешности измерения сопротивления изоляции, определение абсолютной погрешности измерения сопротивления шлейфа, определение абсолютной погрешности определения расстояния до места повреждения изоляции кабеля, определение абсолютной погрешности измерения электрической емкости кабеля.

Для определения этих МХ при поверке прибора были выбраны следующие эталонные средства поверки: магазин сопротивлений Р40104, диапазон 100 – 1000 МОм; магазин сопротивлений Р40103, диапазон 1 МОм – 10 ГОм; магазин сопротивлений Р40102, диапазон 0,01 – 100 МОм; магазин сопротивлений Р4831, диапазон 0,01 – 110000 Ом; магазин емкостей Р5025, диапазон 0,0001 – 111 мкФ.

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

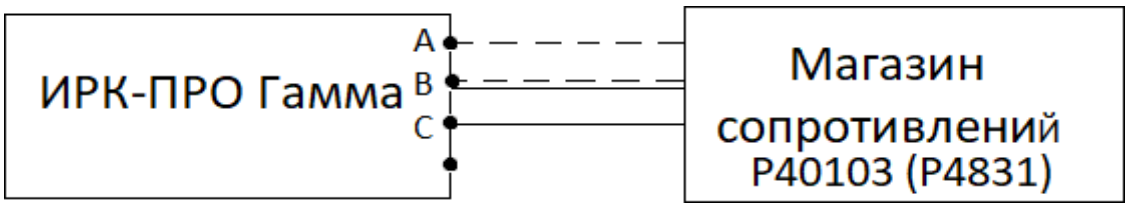


Рисунок 1 – Схема соединения приборов при определении абсолютной погрешности измерения сопротивлений изоляции и шлейфа

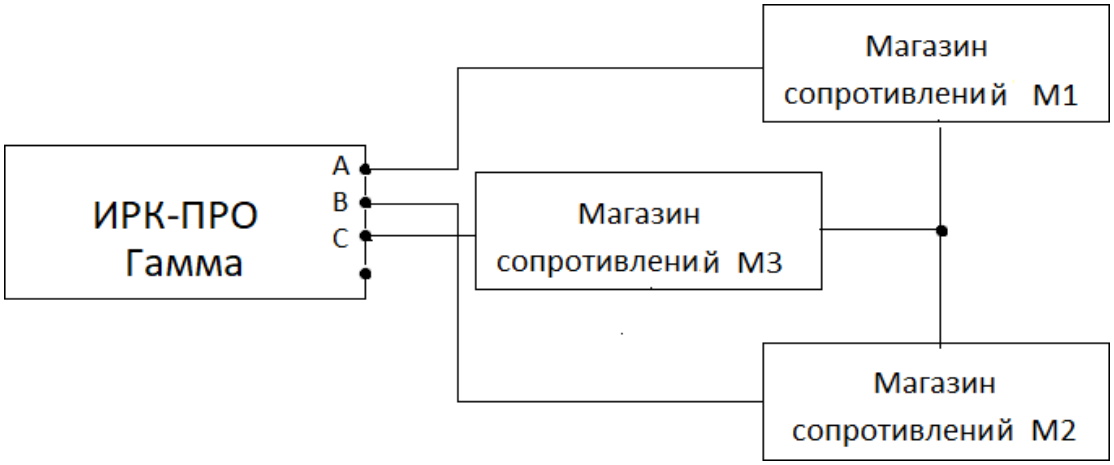


Рисунок 2 – Схема соединения приборов при определении абсолютной погрешности определения расстояния до места повреждения изоляции кабеля

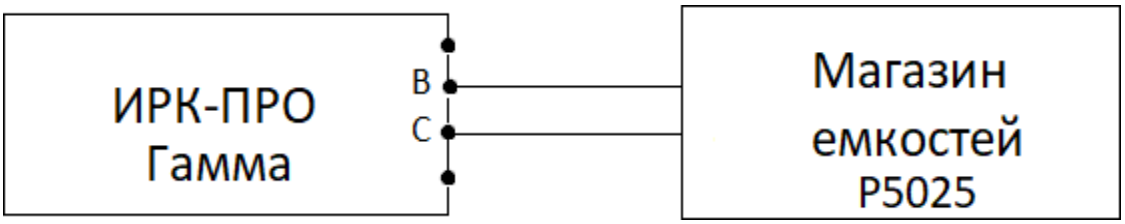


Рисунок 3 – Схема соединения приборов при определении абсолютной погрешности измерения электрической емкости кабеля

Определение МХ поверяемого прибора.

1. Определение абсолютной погрешности измерения сопротивления изоляции.

Данную операцию поверки выполняют при включенном приложении «Мостовые измерения» в режиме работы прибора «Изоляция». В соответствии со схемой рисунка 1 ко входам В и С прибора подключают магазин сопротивлений Р40103. На магазине сопротивлений устанавливают последовательно: 10; 100; 500 кОм;1; 5; 10; 50; 100; 500; 1000; 10000 МОм.

Для каждого выставленного на магазине сопротивления измерения проводятся n раз (n≥3).

Абсолютную погрешность измерения сопротивления изоляции для каждой поверяемой точки поверяемого прибора определяют по формуле:

$$\Delta R = \frac{1}{n}\sum_{i=1}^{n} R_{ui} - R_M, \quad (1)$$

где R_{ui} – измеряемое значение сопротивления; n – количество измерений; R_M – значение сопротивлений, выставляемых на магазине сопротивления.

Результаты поверки считаются удовлетворительными, если полученные значения абсолютной погрешности не превышают значений, указанных в таблице 1.

Таблица 1 – Пределы допускаемой абсолютной погрешности измерения сопротивления изоляции

$R_м$	10 кОм	100 кОм	500 кОм	1 МОм	5 МОм	10 МОм	100 МОм	500 МОм	1 Гом	10 Гом
$\Delta R_и$	±2 кОм	±11 кОм	±51 кОм	±100 кОм	±500 кОм	±1 МОм	±10 МОм	±50 МОм	±100 МОм	±1 Гом

2. Определение абсолютной погрешности измерения сопротивления шлейфа.

Операцию поверки выполняют при включенном приложении «Мостовые измерения» в режиме работы прибора «Шлейф». В соответствие со схемой рисунка 1 ко входам А и В прибора подключают магазин сопротивлений Р4831. На этом магазине устанавливают последовательно следующие значения сопротивления: 1,0; 0,5;1; 10; 50; 100; 500; 1000; 1900; 5000;9900 Ом. Проводят поверяемым прибором измерения установленных сопротивлений.

Расчет абсолютной погрешности измерения сопротивления шлейфа определяют по формуле (1) при замене $\Delta R_и$ на $\Delta R_ш$, а. $R_{иi}$ на $R_{шi}$.

Результаты поверки считаются удовлетворительными, если полученные значения абсолютной погрешности не превышают значений, указанных в таблице 2.

Таблица 2 – Пределы допускаемой абсолютной погрешности измерения сопротивления шлейфа

$R_{ш,}$ Ом	0,1	0,5	1	10	50	100	500	1000	1900	5000	9900
$\Delta R_{ш,}$ Ом	±0,1	±0,1	±0,1	±0,1	±0,1	±0,2	±0,6	±1,0	±1,9	±100	±100

3. Определение абсолютной погрешности определения расстояния до места повреждения кабеля.

Операцию поверки выполняют при включенном приложении «Мостовые измерения» в режиме работы прибора «Утечка». Приборы соединяют в соответствие со схемой рисунка 2. В качестве магазинов сопротивлений М1 и М2 используют два магазина Р4831, а М3 – Р40102. На магазинах сопротивлений устанавливают последовательно значения сопротивлений из таблицы 3. Проводят измерения расстояния для всех установленных значений.

Абсолютную погрешность измерения расстояния до места повреждения кабеля определяют по формуле (1) при замене , $\Delta R_и$ на ΔL, а $R_{иi}$ на $L_{иi}$.

Получаемая погрешность ΔL не должна превышать значений допускаемой погрешности $\Delta L_{д,}$ указанной в таблице 3.

Таблица 3 – Пределы допускаемой погрешности при измерении расстояния до места повреждения изоляции кабеля

М1, Ом	М2, Ом	Шлейф, Ом	L_u, м	Пределы допускаемой абсолютной погрешности $\Delta L_д$ при М3=0,1,2,3 МОм
100	0	100	0	±2 м
50	50	100	1000	±3 м
500	0	500	0	±2 м
250	250	500	1000	±3 м
1000	0	1000	0	±2 м
500	500	1000	1000	±3 м

3. Определение абсолютной погрешности измерения электрической емкости кабеля.

Операцию поверки выполняют при включенном приложении «Мостовые измерения» в режиме работы прибора «Емкость». В соответствии со схемой рисунка 3 ко входам В и С прибора подключают магазин емкостей Р5025. На магазине емкостей последовательно устанавливают: 0,1; 1; 10; 100; 500; 750 нФ; 1; 1,5; 1,95 мкФ. Проводят измерения для всех установленных значений на магазине.

Абсолютную погрешность измерения электрической емкости кабеля определяют по формуле (1), при замене ΔR_u на ΔC_{ui}, а $R_м$ на $C_м$. Полученная погрешность ΔС не должна превышать предела допустимой погрешности $\Delta C_д$, указанной в таблице 4.

Таблица 4 – Пределы допускаемой погрешности измерения емкости кабеля.

См, нФ	0,1	1	10	100	500	750	1000	1500	1950
$\Delta C_{д,}$ нФ	±0,1	±0,2	±0,3	±3	±11	±16	±21	±31	±40

Список использованных источников:

1. Постановление Госстандарта №40 от 21.04.2021г. «Об осуществлении метрологической оценки в виде работ по государственной поверке средств измерений».

2. Руководства по эксплуатации приборов ИРК-ПРО Гамма, Р340104, Р40102, Р4831, Р5025.

УДК 621.391

ПЛАНИРОВАНИЕ VPN-ТУННЕЛЕЙ ПРИ ИСПОЛЬЗОВАНИИ МЕТОДА ИНЖИНИРИНГА, ОСНОВАННОГО НА ПРИСВОЕНИИ КОЭФФИЦИЕНТОВ РАСПРЕДЕЛЕНИЯ ПОТОКА ТРАФИКА В СЕТИ ЭЛЕКТРОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Врублевский С.С., адъюнкт

Военная академия Республики Беларусь

г. Минск, Республика Беларусь

Машкин Е.В. – канд. техн. наук

В работе предложен метод инжиниринга трафика, основанного на присвоении коэффициентов распределения потока трафика, характеризующего долю трафика, при планировании VPN-туннелей в сетях электросвязи специального назначения. Показано что, использовать все возможные маршруты для планирования VPN-туннелей не представляется возможным, так как отдельные ребра являются составными элементами различных маршрутов.

Предоставление современных инфокоммуникационных услуг в сети электросвязи специального назначения (СЭСН) предполагает широкое использования IP-шифраторов и криптомаршрутизаторов совместно с технологией виртуальных частных сетей (Virtual Private Network, VPN).

Использование IP-технологий делает СЭСН во многом схожими с сетью электросвязи общего пользования (СЭОП), однако можно выделить отличительную особенность: в сети доступа в СЭСН есть высокоскоростные участки в десятки и сотни Мбит/с, а на транспортном уровне пропускная способность может существенно снижаться (до пропускной способности эквивалентной цифровому потоку Е1 – 2048 кбит/с), что создает эффект «бутылочного горлышка», тем самым ухудшая показатели качества обслуживания пользователей. Следовательно, необходимо применять дополнительные методы, учитывающие наличие низкоскоростных участков в СЭСН и позволяющие максимально
и сбалансированно использовать весь ресурс сети, а не только ресурс отдельных каналов связи.

В теории построения инфокоммуникационных сетей данный класс методов получил название Traffic Engineering (ТЕ – инжиниринг трафика). На сегодняшний день не существует универсального и стандартизированного подхода применения данных методов не только в СЭСН, но и в СЭОП.

Методы ТЕ позволяют не только определить оптимальный маршрут для потока трафика, но и резервируют для него пропускную способность ресурсов сети, находящихся в этом маршруте [1].

Из существующих методов ТЕ в предложенной модели применен метод, в котором исходными данными для инжиниринга являются характеристики сети, где в качестве ресурса сети используется пропускная способность.

Исходя из концепции ТЕ, между маршрутизаторами *i* и *j* в СЭСН существует в общем случае не один оптимальный маршрут, а множество маршрутов $\left\{p^{\langle ij \rangle}\right\}$

$$p^{\langle ij \rangle} = \begin{bmatrix} p_1^{\langle ij \rangle} \\ p_2^{\langle ij \rangle} \\ \dots \\ p_e^{\langle ij \rangle} \end{bmatrix}, \quad (1)$$

где $p_e^{\langle ij \rangle} = \{i,f,q,\dots, j\}$ – маршрут между маршрутизаторами *i* и *j*.

При этом каждому маршруту $p_e^{\langle ij \rangle}$ присваивается коэффициент распределения потока трафика $k_{ij}^{\{e\}} = k_{ij}^{\{i,f,q,\dots,j\}}$, характеризующий долю трафика, передаваемого по данному маршруту. Коэффициент распределения потока трафика для маршрута равен отношению минимальной пропускной способности маршрута к максимальной пропускной способности сети q_{ij_Σ} между узлами *i* и *j*, определенной в результате решения задачи о максимальном потоке [2]. Пример определения данного коэффициента представлен на рисунке 1.

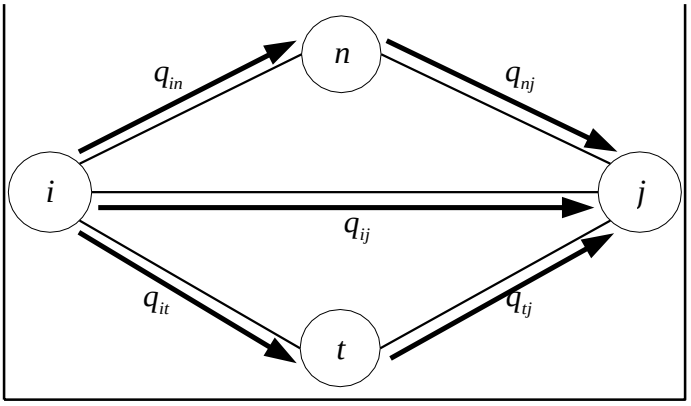


Рисунок 1 – Прохождение потока трафика между точками *i* и *j*

Поток трафика между точками *i* и *j* проходит по трем маршрутам: $\{i,n,j\}$, $\{i,t,j\}$, $\{i,j\}$, каждому присваивается свой коэффициент распределения потока трафика, который рассчитывается как

$$k_{ij}^{\{i,n,j\}} = \frac{q_{ij}^{\{i,n,j\}}}{q_{ij_\Sigma}}, \quad (2)$$

$$k_{ij}^{\{i,t,j\}} = \frac{q_{ij}^{\{i,t,j\}}}{q_{ij_\Sigma}}, \quad (3)$$

$$k_{ij}^{\{i,j\}} = \frac{q_{ij}^{\{i,j\}}}{q_{ij_\Sigma}}, \quad (4)$$

где $q_{ij}^{\{i,n,j\}} = min\{q_{in}, q_{nj}\}$, $q_{ij}^{\{i,t,j\}} = min\{q_{it}, q_{tj}\}$, $q_{ij}^{\{i,j\}} = q_{ij}$ – минимальные пропускные способности маршрутов $\{i,n,j\}$, $\{i,t,j\}$, $\{i,j\}$, соответственно.

Использовать все возможные маршруты для планирования VPN-туннелей не представляется возможным, так как отдельные ребра являются составными элементами различных маршрутов. Следовательно, по мере насыщения ребер планируемыми VPN-туннелями, количество маршрутов будет уменьшаться, до тех пор, пока не станет равным нулю. Указанная итеративная процедура представлена выражением (5),

$$\begin{cases} q_{ij_\Sigma}(1) = q_{ij_\Sigma} - q_{ij_\Sigma}^{\{1\}}; \\ q_{ij_\Sigma}(2) = q_{ij_\Sigma}(1) - q_{ij_\Sigma}^{\{2\}}; \\ \dots \\ q_{ij_\Sigma}(e) = q_{ij_\Sigma}(e-1) - q_{ij_\Sigma}^{\{e\}} = 0, \end{cases} \quad (5)$$

где $q_{ij_\Sigma}(e)$ – суммарная пропускная способность между точками *i* и *j* на шаге *e*, равная разности суммарной пропускной способности между точками *i* и *j* на шаге $e-1$ и минимальной пропускной способности маршрута *e* между точками *i* и *j*;

e – количество маршрутов.

Применение методов ТЕ в СЭСН при планировании VPN-туннелей позволит обеспечить сбалансированную загрузку сети (до 100 % ресурса сети) в сравнении с традиционными одномаршрутными протоколами RIP и OSPF (обеспечивают использование до 40 % ресурса сети).

Список использованных источников:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – СПб. : Питер, 2015. – 992 с..

2. Харари, Ф. Теория графов / Ф. Харари ; под ред. Г. П. Гаврилова. пер. с англ. – 2-е изд. – М. : Едиториал УРСС, 2003. – 296 с

УДК 621.391

ВЫБОР ПЛАТФОРМЫ ВИДЕОКОНФЕРЕНЦСВЯЗИ ДЛЯ УЧЕБНОГО ПРОЦЕССА: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ ПАРАМЕТРОВ

Довгулевич Е.В., магистрант гр.267041

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

Шевчук О.Г. – канд. техн. наук, доцент

Аннотация. В данном тезисе проведен сравнительный анализ основных параметров платформ видеоконференцсвязи для учебного процесса.

Ключевые слова. Видеоконференцсвязь, облачные сервисы видеоконференцсвязи, параметры видеоконференцсвязи.

Сегодня видеоконференцсвязь является неотъемлемой частью многих организаций, в том числе и учебных учреждений. Одним из ключевых инструментов онлайн-обучения является платформа видеоконференцсвязи, при выборе которой необходимо учитывать множество факторов, таких как функциональность, качество передачи видео и голоса, надежность, безопасность, совместимость программного обеспечения, удобство использования, стоимость. В данном тезисе будет проведен сравнительный анализ основных параметров платформ видеоконференцсвязи для учебного процесса.

В первую очередь следует определить параметры, по которым далее будем анализировать программные продукты. Поскольку рассматривать в рамках одних и тех же критериев облачных сервисов (cloud-based) и локальных (on-premise) некорректно, то для сравнения возьмем исключительно облачные решения. Они на текущий момент предоставляют наиболее широкий функционал и, кроме того, не требуют от организации аппаратных ресурсов для развертывания, а значит соотношение скорости их внедрения и необходимых для этого усилий наиболее оптимально [1]. Среди сервисов видеоконференцсвязи, которые широко используются в образовании, можно отметить Zoom, Microsoft Teams, Google Meet, Cisco Webex, Skype.

Первым критерием для сравнения является функциональность платформы. При выборе системы видеоконференцсвязи необходимо убедиться, что она поддерживает все необходимые функции. Возможность проведения онлайн-занятий и осуществление обменом файлов поддерживают все перечисленные сервисы видеоконференцсвязи. Важной функцией для студентов, которые не могут посещать занятия в режиме реального времени является возможность записи занятий, предоставляемая всеми указанными выше платформами. Проведение параллельных занятий для разных групп, управление доступом студентов к материалам и занятиям, возможность подключения большого количества участников позволяют сервисы видеоконференцсвязи Zoom, Microsoft Teams и Cisco Webex. Исходя из вышеперечисленных функций, можно сделать вывод, что все платформы имеют схожие базовые функции.

Вторым критерием является качество передачи видео и голоса, обусловливаемое различными факторами, такими как пропускная способность канала связи и использование кодеков. Системы конференцсвязи Cisco Webex и Microsoft Teams, поддерживают передачу видео и голоса высокого качества даже при низкой пропускной способности канала связи. Google Meet и Zoom имеют оптимизацию видео и аудио потоков в зависимости от качества канала связи на стороне конечного пользователя. В целом, все системы конференцсвязи стремятся обеспечить максимальное качество передачи данных при использовании доступных ресурсов.

Важным параметром при выборе платформы видеоконференцсвязи является обеспечение информационной безопасности, в части касающейся защиты от перехвата данных, управления доступом и хранения пользовательской информации [2]. Анализ безопасности программ для видеоконференций обозначил следующие важные моменты, на которые необходимо обращать внимание при выборе системы – это наличие сквозного шифрования, защиты от несанкционированного доступа, наличие двухфакторной аутентификации и количество уязвимостей.

Все сервисы видеоконференцсвязи придерживаются высоких стандартов безопасности. Каждый сервис имеет свои преимущества и недостатки, и лучше всего выбирать, основываясь на потребности и требования организации. Для удобства основные параметры, касающиеся безопасности приложений для видеоконференций представлены в таблице 1.

Проанализировав базу данных MITRE по уязвимостям в ПО (CVE - Common Vulnerabilities and Exposures) за 2021-2022 годы было обнаружено, что в приложениях Zoom, Microsoft Teams было зарегистрировано не менее 5 уязвимостей за этот период, Cisco Webex не менее 4 уязвимостей. Это демонстрирует, что в приложениях были обнаружены некоторые уязвимости, которые могут повлиять на безопасность пользователей. Однако обычно компании выпускают исправления на такие уязвимости в своих обновлениях. В Google Meet не зарегистрировано уязвимостей за этот период. Но это не гарантирует, что таких уязвимостей не было, потому что не все уязвимости, возникающие в ПО, могут быть зарегистрированы в базе данных MITRE [3].

Таблица 1 – Основные параметры, касающиеся безопасности приложений для видеоконференций.

Приложения / Основные параметры	Zoom	Microsoft Teams	Cisco Webex	Google Meet
Шифрование данных	AES 256-битное шифрование	AES 256-битное шифрование	TLS 1.2/AES 256-битное шифрование	TLS и SRTP
Двухфакторная аутентификация	есть	есть	есть	есть
Возможность управления персональными данными на сервере	нет	есть	нет	нет
Возможность управления персональными данными на стороне клиента	есть	есть	есть	есть
Наличие комнаты ожидания	есть	есть	есть	есть
Соответствие стандартам безопасности	HIPAA,GDPR, FEBRA, SOC 2, ISO 27001	HIPAA, ISO 27001, SOC 1 и SOC 2	SOC 2, ISO 27001, HIPAA, PCI DSS и GDPR	SOC 2, ISO 27001 и HIPAA

В заключение, проведенный сравнительный анализ основных параметров видеоконференцсвязи для учебного процесса позволяет сделать вывод о том, что выбор платформы должен основываться на ряде факторов, включая доступность функциональных возможностей, а также безопасность и конфиденциальность данных. Необходимо учитывать, что каждая платформа имеет свои достоинства и недостатки, и выбор должен быть обоснованным и основываться на конкретных требованиях и задачах. Также, стоит учитывать, что технологии видеоконференцсвязи продолжают развиваться и улучшаться, поэтому важно следить за новыми тенденциями и обновлениями, чтобы выбирать наиболее подходящие решения для эффективной организации учебного процесса.

Список использованных источников:

1. ВКС для корпоративного использования: что выбрать и как сравнить? [Электронный ресурс]. Режим доступа: https://slddigital.com/article/vks-dlya-korporativnogo-ispolzovaniya-chto-vybrat-i-kak-sravnit/.Дата доступа: 05.04.2023.

2. Сравнение сервисов видеоконференций с точки зрения их безопасности. [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/compare/Video-conferencing-software-security. Дата доступа: 10.04.2023.

3. Search CVE List. [Электронный ресурс]. https://cve.mitre.org/cve/search_cve_list.html. Дата доступа: 03.04.2023.

МЕТОДИКА ВЫПОЛНЕНИЯ ИЗМЕРЕНИЙ ОПТИЧЕСКОЙ ДЛИНЫ ЛИНИИ (ВОЛОКЛА) ОПТИЧЕСКИМ РЕФЛЕКТОМЕТРОМ MTP6000

Ковалёв Д.В. магистрант гр.267041, Орехов А.К. магистрант гр.267041

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Белошицкий А. П. – кандидат технических наук, доцент

Доклад посвящён разработке методики выполнения измерений оптической длины линий (расстояния до неоднородности) оптическим рефлектометром MTP6000. В методике приводятся описание метода и схемы измерения, метрологические характеристики рефлектометра, порядок проведения измерений и модель измерения.

Для достижения высоких эксплуатационных показателей волоконно-оптических линий связи (ВОЛС) большую роль играет метрологическое обеспечение (МО) при их строительстве и эксплуатации. Одной из важных задач МО является разработка методик выполнения измерений (МВИ) позволяющих определять показатели качества ВОЛС с необходимой точностью и достоверностью.

В докладе рассматривается МВИ оптической длины линии (расстояния до неоднородностей линии) с использованием оптического рефлектометра MTP6000.

Измерения оптической длины волокна оптического кабеля выполняют согласно ГОСТ 26814-86 методом прямых измерений при прохождении по оптическому волокну мощного одиночного оптического импульса. Метод прямых измерений основан на регистрации обратно рассеянного излучения в оптическом волокне при прохождении через него оптического импульса и измерении зависимости от времени мощности этого излучения. Метод пригоден для определения распределения оптических потерь по длине волокна, затухания волокна, неоднородностей (обрыв, место сварки и т.д.), значения потерь на неоднородностях, а также определения оптической длины волокна и расстояния до места обрыва. Измерение оптической длины оптического волокна или расстояния до места обрыва оптического волокна методом прямых измерений производят по схеме, изображённой на рисунке 1.

Рисунок 1 - Схема подключения оптического волокна к рефлектометру.

Настоящая методика обеспечивает выполнение измерений оптической длины оптического волокна (расстояния до места обрыва) ВОЛС при использовании оптического рефлектометра MTP 6000, метрологические характеристики которого приведены в таблице 1.

Таблица 1 - Метрологические характеристики оптического рефлектометра MTP 6000

Характеристики	Величина
Длины волн излучения	(1310 ± 20) нм, (1490 ± 20) нм , (1550 ± 20) нм и (1625 ± 20) нм.
Диапазоны измеряемых расстояний	2; 5; 10; 20; 40; 80; 120; 160 и 240 км.
Пределы допускаемого значения абсолютной погрешности измерения расстояний	$\Delta L = \pm(0.5 + \Delta p + 3 * 10^{-5} L)$; Δp - разрешение 0,16; 0,32; 0,64; 1,3; 2,5; 5,1; 3,8 и 7,6 м. в зависимости от диапазона измерений L - измеряемое расстояние, м.

При измерении оптической длины (расстояния) до неоднородности маркер устанавливается на ее левый край (см. рисунок 2). Расстояние при этом указывается в километрах в верхней части маркера. Для более точного измерения расстояния рекомендуется максимально растянуть рефлектограмму по горизонтали и вертикали. Точность определения расстояния по рефлектограмме зависит, в частности, от правильности установки значения показателя преломления ОВ. Если оно неизвестно, а известна точно длина измеряемого ОВ, то можно установить любой маркер на конец ОВ и осуществить корректировку показателя преломления так, чтобы длина ОВ, измеренная по рефлектограмме, совпадала с известной.

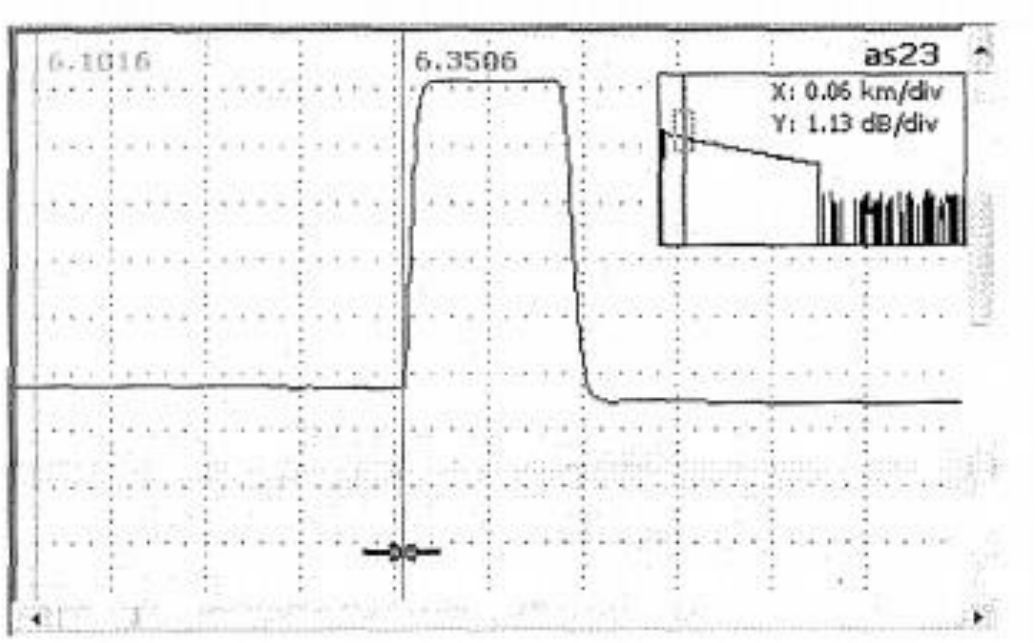


Рисунок 2 - Изображение экрана рефлектометра в режиме измерения расстояния.

Для составления модели измерения оптической длины с помощью рефлектометра были проанализированы источники неопределённости измерений. Основными источниками неопределённости измерений для данной измерительной задачи являются: неправильная установка длины волны излучения, длительности импульса, коэффициента преломления, ошибка оператора, разрешающая способность и погрешность измерения рефлектометра. При правильном выборе длины волны, длительности импульса и корректном выполнении измерений первые три составляющие неопределённости в модели измерения можно не учитывать.

Для оценки точностных характеристик данной МВИ была разработана методика оценки неопределённости измерений. В этой методике была предложена следующая модель измерения

$$L_{\text{ОВ}} = L_p + \Delta L + \Delta_{\text{кп}} + \Delta p \quad (1),$$

где, $L_{\text{ОВ}}$- оптическая длина ОВ, м;

ΔL- поправка на погрешность измерения расстояния рефлектометром, м;

$\Delta_{\text{кп}}$- поправка на неточность установки показателя преломления, м;

Δp- поправка на разрешающую способность рефлектометра.

Разработанная методика ведения измерений обеспечивает выполнение измерений оптической длины ОВ и строительных длин ВОЛС, а также определять расстояния до повреждений (обрыва) оптического волокна с необходимой точностью и достоверностью.

Список использованных источников:

1. ГОСТ 26814- 86. Кабели оптические. Методы измерения параметров — М.: Изд-во стандартов, 1986. – 32с.

УДК 621.391

ОЦЕНКА КАЧЕСТВА КОМБИНИРОВАННЫХ АСМ-ИЗОБРАЖЕНИЙ НА ОСНОВЕ ЛОКАЛЬНОЙ КОРРЕЛЯЦИОННОЙ МЕТРИКИ

Левоненко И.И., студент гр.160801; Ловецкий М.Ю., аспирант

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Цветков В.Ю. – д.т.н, профессор

Аннотация. Рассматривается задача взвешенного сложения компонентных изображений атомного силового микроскопа (АСМ). Получены зависимости локальной корреляционной метрики от размера окна корреляционного анализа и вклада компонентных АСМ-изображений в результирующее комбинированное АСМ-изображений.

Ключевые слова. Атомная силовая микроскопия, оценка качества комбинирования изображений, глобальная корреляция изображений, локальная корреляция изображений.

Введение

Атомно-силовая микроскопия (АСМ) поверхности материала использует несколько параллельных синхронизированных измерительных каналов для различных физических величин (высоты, вязкости и жесткости поверхности, деформации зонда и рассеивания энергии). Формируемые в этих измерительных каналах значения компонуются в несколько двухмерных матриц чисел, представляемых многоканальными АСМ-изображениями, в которых яркости пикселей каждого канала отражают значения измеряемой физической величины в соответствующих точках поверхности. Для эффективного визуального анализа многоканальных АСМ-изображений необходимо объединять их каналы для отображения на стандартных мониторах, имеющих относительно узкий динамический диапазон, с минимальными искажениями и потерями деталей. В данной работе рассматриваются комбинированные полутоновые АСМ-изображения на основе двух измерительных каналов.

Для объединения изображений используются подходы, основанные на взвешенном сложении, методе главных компонент [1], дискретном вейвлет-преобразовании [2], однако они специально не ориентированы на объединение изображений, формируемых в измерительных каналах атомного силового микроскопа. Отсутствуют рекомендации по выбору алгоритма для эффективного формирования комбинированных АСМ-изображений. Для их разработки необходима оценка качества комбинированных изображений. Известные показатели качества изображений основаны на анализе краев [3, 4], взаимной информации [5], оценке количества информации в изображении [6], оценке точности визуальной информации в различных масштабах представления изображения [7], однако они специально не ориентированы на оценку качества комбинированных АСМ-изображений. Относительной простотой вычислений отличается коэффициент корреляции, использующий средние значения изображений, но не учитывающий локальные особенности распределения яркости. Для оценки качества АСМ-изображений, отличающихся существенными локальными неоднородностями распределения яркости, представляет интерес метрика качества комбинирования компонентных АСМ-изображений на основе коэффициентов локальной корреляции, учитывающая вклад каждого из компонентных АСМ-изображений в результирующее комбинированное АСМ-изображение и корреляцию между компонентными АСМ-изображениями. Локальная корреляция обеспечивает более высокую точность оценки качества комбинирования АСМ-изображений по сравнению с глобальной корреляцией, но ее значения зависят от размера окна анализа.

Целью работы является определение вкладов значений пикселей компонентных АСМ-изображений, обеспечивающих передачу в комбинированное АСМ-изображение наиболее полной информации об объектах определенного размера.

Формирование комбинированных АСМ-изображений

Исходя из предположения о независимости эффективности методов объединения изображений и точности показателей качества комбинированных изображений для формирования

комбинированных АСМ-изображений выбран простейший метод взвешенного сложения. Согласно данному методу значения пикселей $m_C(y,x)$ комбинированного АСМ-изображения $M_C = \|m_C(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ вычисляются на основе значений пикселей АСМ-изображений $M_1 = \|m_1(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ первого и $M_2 = \|m_2(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ второго измерительных каналов атомного силового микроскопа с помощью выражения

$$m_C(y,x) = \left[k\, m_1(y,x) + (1-k)\, m_1(y,x) \right] \tag{1}$$

при $y = \overline{0,Y-1}$, $x = \overline{0,X-1}$,

где k – коэффициент, определяющий вклад значений пикселей каждого компонентного АСМ-изображения M_1 и M_2 в значения пикселей комбинированного АСМ-изображения M_C, $0 < k < 1$; Y, X – размеры (в пикселях) компонентных и комбинированного АСМ-изображений по вертикали и горизонтали; $[\ ]$ – операция округления значений пикселей до ближайшего целого.

Меньшие значения коэффициента k на рис. 1 соответствуют меньшей относительной доли значений компонентного АСМ-изображения M_1 в комбинированном АСМ-изображении M_C по сравнению с компонентным АСМ-изображением M_2.

Оценка качества комбинирования АСМ-изображений на основе коэффициента локальной корреляции

Повышение точности корреляционной оценки качества комбинирования АСМ-изображений достигается за счет учета локальных особенностей распределений значений пикселей в компонентных и комбинированном АСМ-изображениях. Для этого используется коэффициент $r_{\mathrm{L}}(A,B)$ локальной корреляции двух АСМ-изображений $A = \|a(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$ и $B = \|b(y,x)\|_{(y=\overline{0,Y-1},x=\overline{0,X-1})}$, вычисляемый с помощью выражения

$$r_{\mathrm{L}}(A,B,p) = \frac{\sum_{y=0}^{Y-1}\sum_{x=0}^{X-1} \left|a(y,x) - a_{\mathrm{L}}(y,x,p)\right| \left|b(y,x) - b_{\mathrm{L}}(y,x,p)\right|}{\sqrt{\sum_{y=0}^{Y-1}\sum_{x=0}^{X-1} \left(a(y,x) - a_{\mathrm{L}}(y,x,p)\right)^2 \sum_{y=0}^{Y-1}\sum_{x=0}^{X-1} \left(b(y,x) - b_{\mathrm{L}}(y,x,p)\right)^2}}, \tag{2}$$

где $a_{\mathrm{L}}(y,x,p)$, $b_{\mathrm{L}}(y,x,p)$ – средние значения яркостей пикселей изображений A и B в окрестности пикселя с координатами (y,x) размером $p \times p$ пикселей, $a_{\mathrm{L}}(y,x,p) = \frac{1}{p^2}\sum_{j=0}^{p}\sum_{i=0}^{p} a(y+j, x+i)$, $b_{\mathrm{L}}(y,x,p) = \frac{1}{p^2}\sum_{j=0}^{p}\sum_{i=0}^{p} b(y+j, x+i)$.

Для оценки качества комбинирования АСМ-изображений с учетом корреляции между комбинированным АСМ-изображением и каждым из двух компонентных АСМ-изображений, а также между компонентными АСМ-изображениями может использоваться локальная корреляционная метрика $D_{\mathrm{L}}(k)$, вычисляемая с помощью выражения (чем больше ее значение, тем лучше)

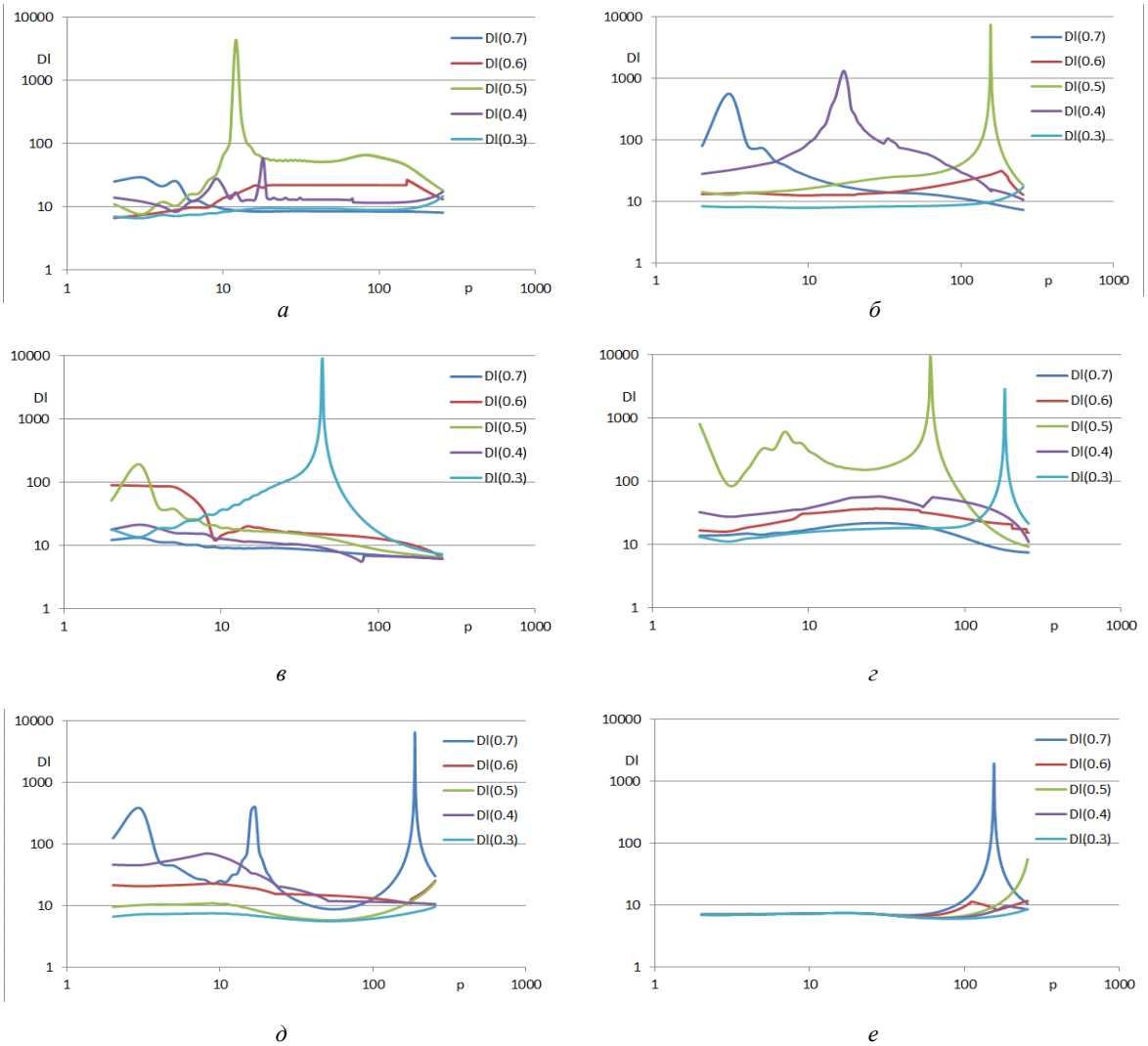
$$D_{\mathrm{L}}(k) = \frac{r_{\mathrm{L}}(M_C, M_1, k) + r_{\mathrm{L}}(M_C, M_2, k)}{\left|r_{\mathrm{L}}(M_C, M_1, k) - r_{\mathrm{L}}(M_C, M_2, k)\right| r_{\mathrm{L}}(M_1, M_2, 0{,}5)}. \tag{3}$$

Локальная корреляционная метрика $\boxed{D_{\mathrm{L}}(k)}$ позволяет определить значение k, обеспечивающее лучшее соотношение вкладов компонентных АСМ-изображений в комбинированное АСМ-изображение по сравнению с глобальной корреляционной метрикой.

Зависимости метрики качества комбинирования компонентных АСМ-изображений от размера окна корреляционного анализа

На рис. 2 приведены зависимости значений метрики $\boxed{D_{\mathrm{L}}(k)}$ от размера p окна корреляционного анализа и коэффициента k для 10 комбинированных АСМ-изображений. Из рис. 2 следует, что для локальные максимальные значения метрики $\boxed{D_{\mathrm{L}}(k)}$ зависят от значения p. На рис. 3, 4 приведены компонентные АСМ-изображения, полученные при различных значениях k.

При необходимости передачи в комбинированные АСМ-изображения наиболее полной информации о мелких объектах (p = 3) компонентных АСМ-изображений необходимо использовать значения k, равные 0,7, 0,7, 0,5, 0,5, 0,7, 0,7, 0,5 для АСМ-изображений 1–5, 9, 10 соответственно. В этом случае выбор значения k для АСМ-изображений 6–8 не имеет существенного значения.



а *б*

в *г*

д *е*

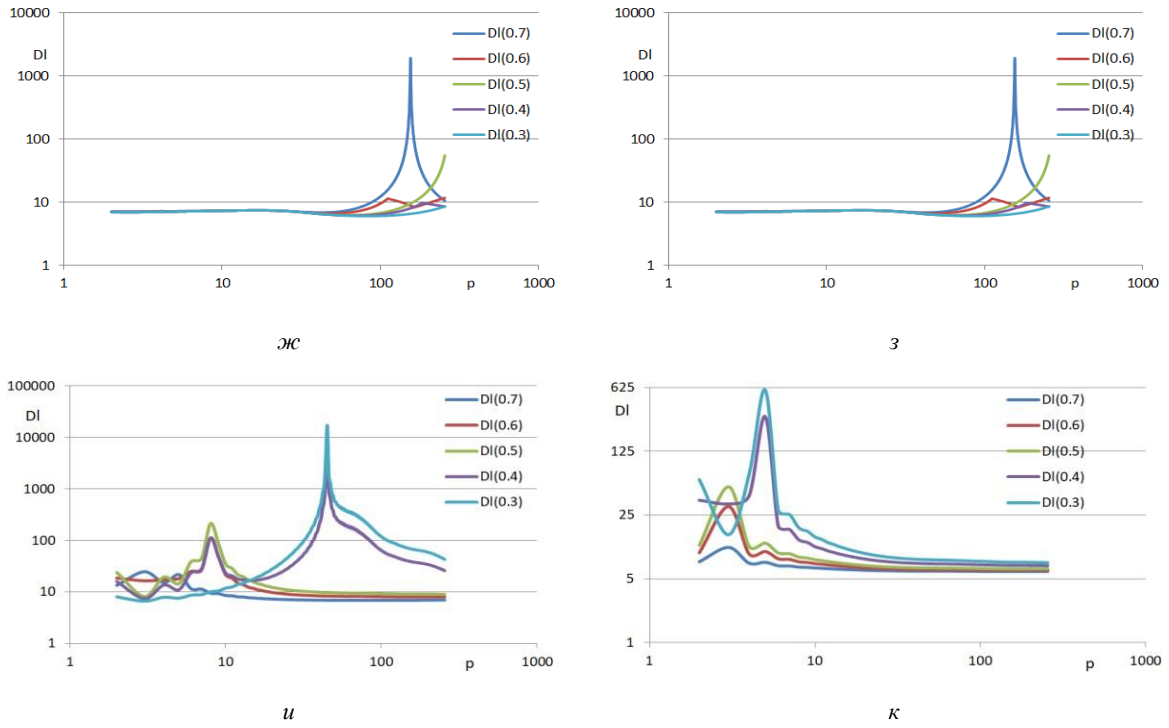


Рис. 2. Зависимости значений локальной корреляционной метрики от размера окна корреляционного анализа для компонентных АСМ-изображений: а – АСМ-1; б – АСМ-2; в – АСМ-3; г – АСМ-4; д – АСМ-5; е – АСМ-6; ж – АСМ-7; з – АСМ-8; и – АСМ-9; к – АСМ-10

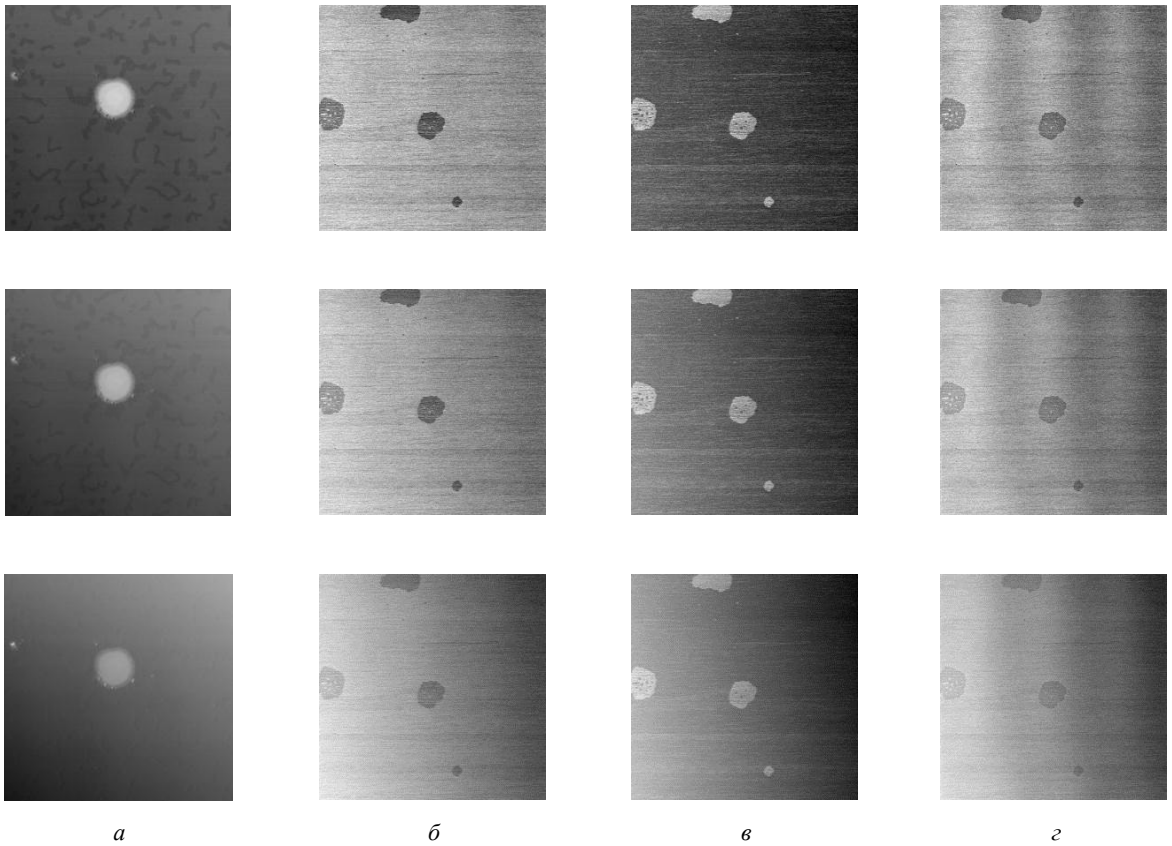
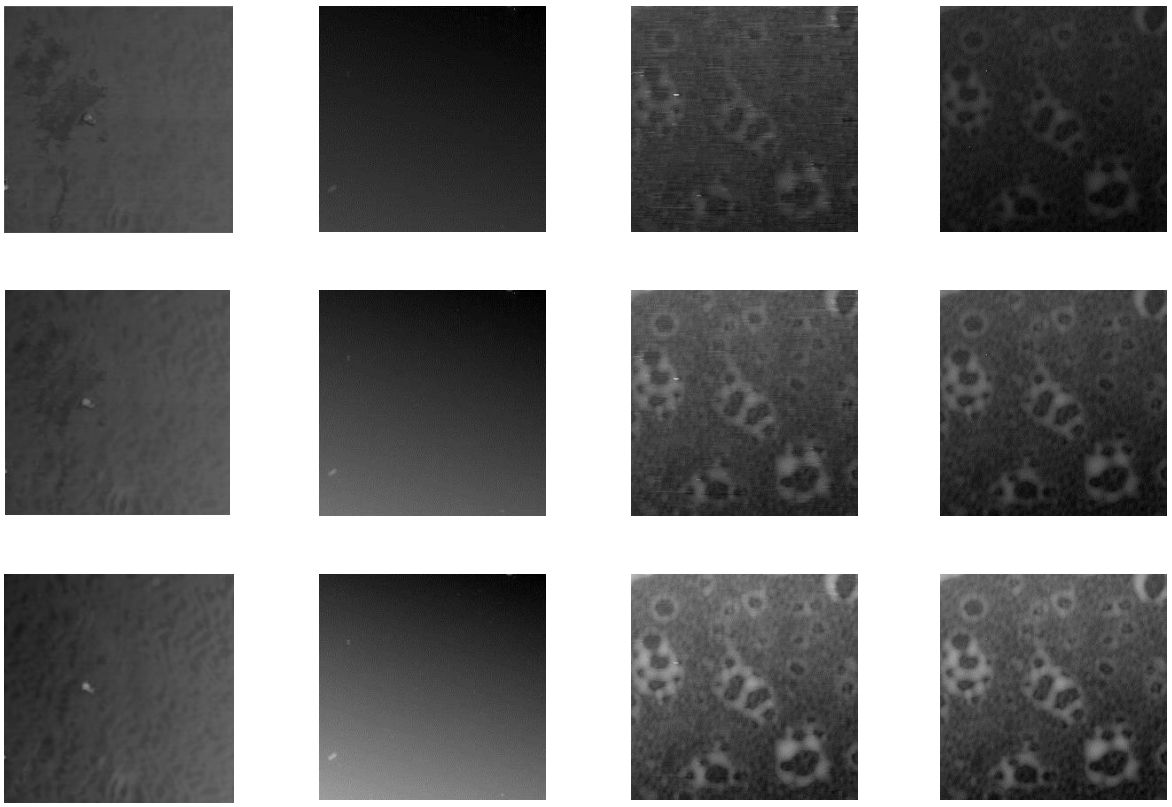


Рис. 3. Комбинированные АСМ-изображения при значениях k=0,7 (верхний ряд), k=0,5 (средний ряд), k=0,3 (нижний ряд): а – АСМ-5; б – АСМ-6; в – АСМ-7; г – АСМ-8

При необходимости передачи в комбинированные АСМ-изображения наиболее полной информации о более крупных объектах (p > 3) необходимо использовать различные значения k, обеспечивающие для различных АСМ-изображений наибольшие значения метрики $\boxed{D_{\mathrm{L}}(k)}$.



а *б* *в* *г*

Рис. 4. Комбинированные АСМ-изображения при значениях k=0,7 (верхний ряд), k=0,5 (средний ряд), k=0,3 (нижний ряд): а – АСМ-1; б – АСМ-3; в – АСМ-9; г – АСМ-10

Из рис. 2 следует, что по глобальному максимальному значению локальной корреляционной метрики $\boxed{D_{\mathrm{L}}(k)}$ во всем диапазоне изменения значения p можно определить значение k, обеспечивающее лучшие условия для передачи в комбинированное АСМ-изображение информации об объектах компонентных АСМ-изображений, имеющих наиболее часто встречающиеся размеры. С учетом данного свойства разработана схема адаптивного взвешенного сложения компонентных АСМ-изображений (рис. 5) с автоматическим выбором значения k, определяющим вклад значений пикселей компонентных АСМ-изображений в комбинированное АСМ-изображение.

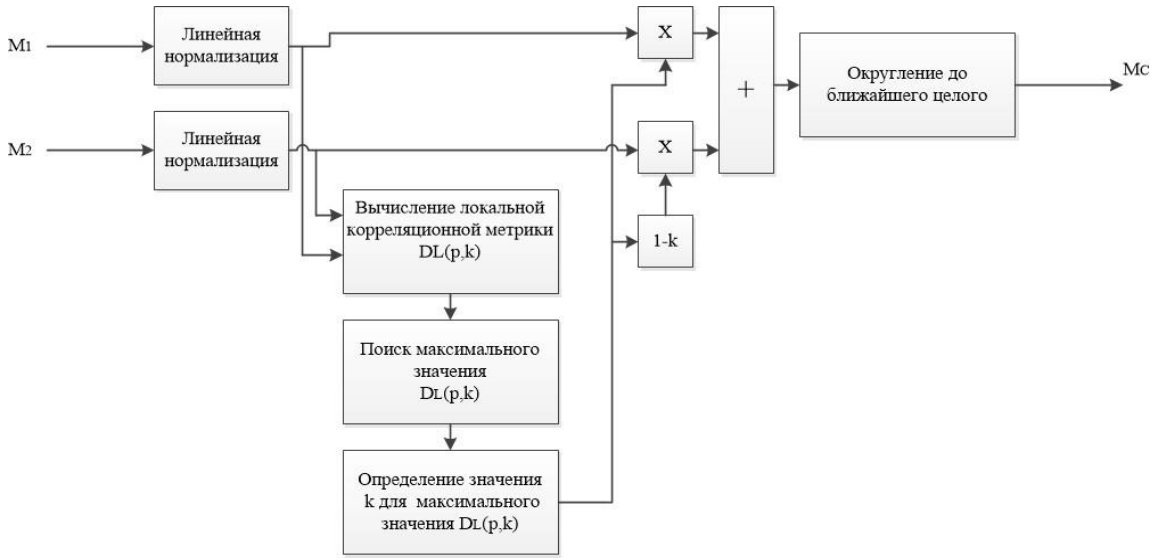


Рис. 5. Схема адаптивного формирования комбинированного АСМ-изображения на основе взвешенного сложения компонентных АСМ-изображений с автоматическим определение вклада значений пикселей компонентных АСМ-изображений в комбинированное АСМ-изображение

Заключение

Получены зависимости значений локальной корреляционной метрики от размера окна корреляционного анализа и вклада компонентных АСМ-изображений в комбинированное АСМ-изображение. По данным зависимостям установлены вклады значений пикселей компонентных АСМ-изображений, обеспечивающих передачу в комбинированное АСМ-изображение наиболее полной информации об объектах определенного размера. Предложена схема адаптивного взвешенного сложения компонентных АСМ-изображений с автоматическим определением вклада значений пикселей компонентных АСМ-изображений в комбинированное АСМ-изображение.

Список использованных источников:

1. Jifeng S., Yuanjiao J., Shaoyong Z. // Proceedings of the SPIE International Conference on Space Information Technology. 2008. Vol. S98S. P. 739-744.
2. Zhang A.K., Dare. Y.P. // ISPRS Journal of Photogrammetric and Remote Sensing. 2007. Vol.62, No. 4. P.249-263.
3. Petrovic V., Xydeas C. // Tenth IEEE International Conference on Computer Vision (ICCV'05). 2005. Vol. 1, P. 1866-1871.
4. Piella G., Heijmans H. // Proceedings International Conference on Image Processing (Cat. No.03CH37429). 2003. P. 111-173.
5. Qu G., Zhang D., Yan P. // Opt. Express. 2001. Vol. 9. P. 184-190.
6. Aslantas V., Bendes E. // AEU – International Journal of Electronics and Communications. 2015. P. 1890-1896.
7. Han Y., Cai Y., Cao Y., Xu X. // Inf. Fusion. 2013. Vol. 14. No. 2. P. 127–135.

UDC 621.391

QUALITY EVALUTION OF COMBINED AFM IMAGES BASED ON LOCAL CORRELATION METRIC

I.I. Levonenko, student gr. 160801; M.Yu. Lavetski, PhD student

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

V.Yu. Tsviatkou – Doctor of Engineering, professor

Annotation. The problem of weighted addition of component images of an atomic force microscope (AFM) is considered. The dependences of the local correlation metric on the size of the correlation analysis window and the contribution of component AFM images to the resulting combined AFM images are obtained. A scheme for adaptive weighted summation of component AFM images is proposed.

Keywords. Atomic force microscopy, image combination quality assessment, global image correlation, local image correlation.

УДК 621.391

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ МЕТОДА НАИМЕНЬШИХ КВАДРАТОВ В СТАТИЧЕСКИХ ЗАДАЧАХ

Легейда Е.П. гр.263101

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ИКТ

Аннотация. В данной статье рассмотрена тема метод наименьших квадратов в статистических задачах обработки результатов измерений. Представлена методика обработки результатов измерений с использованием метода наименьших квадратов. Приведены примеры применения метода наименьших квадратов.

Ключевые слова: метод наименьших квадратов, статистика, обработка результатов измерений, оценка погрешности измерений.

При проведении измерений в физике, инженерии, экономике и других науках важно не только получить числовые результаты, но и оценить их точность. Один из основных вопросов, которые возникают при обработке экспериментальных данных, – это определение наиболее вероятного значения измеряемой величины. В этом докладе рассматривается метод наименьших квадратов, который широко используется для решения этой проблемы.

Первый шаг в определении вероятнейшего значения измеренной величины - это оценка погрешности измерений. Эта погрешность может быть вызвана различными факторами, включая неточность измерительного прибора, нестабильность условий эксперимента, ошибки оператора и другие. Чтобы учесть эти погрешности, обычно проводят несколько измерений и вычисляют среднее значение.

Однако даже при использовании многократных измерений остается неопределенность относительно того, какое значение является наиболее вероятным. Для решения этой проблемы используется метод наименьших квадратов.

Метод наименьших квадратов (МНК) – это статистический метод, который используется для нахождения наилучшей линейной аппроксимации экспериментальных данных. Он основан на минимизации суммы квадратов отклонений между исходными данными и прямой линией, наиболее близкой к этим данным.

Предположим, что у нас есть набор данных, представляющий собой набор значений x и соответствующих им значений y. Мы хотим найти уравнение линейной функции, которая наилучшим образом описывает эти данные. Уравнение линейной функции имеет следующий вид:

$$y = ax + b$$

Чтобы найти наилучшую линейную аппроксимацию, мы ищем значения a и b, которые минимизируют сумму квадратов отклонений между исходными данными и линией. Эта сумма квадратов отклонений выглядит следующим образом:

$$\sum_{i=1}^{n}(y_i - ax_i - b)^2$$

где n – количество точек данных.

Для минимизации этой суммы квадратов можно применить метод дифференциального исчисления и найти значения a и b, приравняв производные по a и b к нулю. Это приводит к следующим уравнениям:

$$\sum_{i=1}^{n} y_i = a\sum_{i=1}^{n} x_i + nb$$

$$\sum_{i=1}^{n} x_i\, y_i = a\sum_{i=1}^{n} x_i^2 + \sum_{i=1}^{n} x_i$$

Решая эти уравнения относительно a и b, мы получаем следующие значения:

$$a = \frac{n\sum_{i=1}^{n} x_i\, y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2}$$

$$b = \frac{\sum_{i=1}^{n} y_i - b\sum_{i=1}^{n} x_i}{n}$$

Небольшой пример:

x	1	2	3	4	5
y	1.1	3.8	6.5	10.2	13.1

y = a + bx

$$\sum_{i=1}^{5} x_i\, y_i = 134.5$$

$$\sum_{i=1}^{5} x_i = 15$$

$$\sum_{i=1}^{5} y_i = 34.7$$

$$\sum_{i=1}^{5} x_i^2 = 55$$

$$a = \frac{n\sum_{i=1}^{n} x_i\, y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2} = 3.04$$

$$b = \frac{\sum_{i=1}^{n} y_i - b\sum_{i=1}^{n} x_i}{n} = -2.18$$

y = 3.14x - 2.18

Таким образом, мы получаем уравнение линейной функции, которое наилучшим образом аппроксимирует исходные данные.

Одним из преимуществ метода наименьших квадратов является то, что он позволяет оценить точность вероятнейшего значения. Для этого используется среднеквадратическая ошибка (Mean Squared Error (MSE)), которая определяется как среднее значение квадратов отклонений между исходными данными и линейной аппроксимацией:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - ax_i - b)^2$$

Стандартная ошибка оценки (SE) может быть вычислена как квадратный корень из MSE:

$$SE = \sqrt{\frac{1}{n-2}\sum_{i=1}^{n}(y_i - ax_i - b)^2}$$

Эта ошибка оценки показывает, насколько точно линейная аппроксимация соответствует исходным данным. Чем меньше SE, тем более точна линейная аппроксимация.

Заключение. Метод наименьших квадратов является мощным инструментом для определения вероятнейшего значения измеренной величины и оценки его точности. Этот метод широко используется в физике, инженерии, экономике и друг их областях, где необходимо аппроксимировать данные линейной функцией. Кроме того, метод наименьших квадратов может быть обобщен на другие типы функций, такие как полиномы и экспоненциальные функции. В этих случаях процесс минимизации суммы квадратов отклонений аналогичен, но используются соответствующие функциональные формы.

Несмотря на все преимущества метода наименьших квадратов, следует помнить, что он предполагает линейную зависимость между переменными. Если зависимость не является линейной, результаты метода могут быть неточными или непригодными для использования.

УДК 621.391

РАСЧЕТ КРИТЕРИЕВ ТОЧНОСТИ РЕЗУЛЬТАТОВ РАВНОТОЧЕЧНЫХ И НЕРАВНОТОЧЕЧНЫХ ИЗМЕРЕНИЙ

Мателенок М.С. гр.263101

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ИКТ

Аннотация. В данной статье рассмотрена тема расчет критериев точности результатов равноточных и неравноточных измерений. Представлены для расчета критерии точности результатов равноточных и неравноточных измерений. Приведены примеры применения критериев точности результатов равноточных и неравноточных измерений.

Ключевые слова: равноточные измерения, неравноточные измерения, критерий точности, нормальный закон распределения, ошибки.

Равноточными (равнорассеянными) называются независимые измерения постоянной величины, результаты которых могут рассматриваться как случайные, распределенные по одному и тому же закону. В большинстве случаев при обработке равноточных измерений исходят из предположения нормального закона распределения результатов и случайных погрешностей измерений. При обработке результатов измерений, если известна систематическая погрешность, в каждый из результатов измерений вносят поправку. Поскольку систематическая погрешность таким образом устранена из результатов измерений, то дисперсия погрешности является одинаковой для всех измерений. Равноточные измерения выполняются одним и тем же средством измерений.

Многократные измерения одного постоянного размера величины по градуированным шкалам интервалов и отношений выполняются в последовательности, показанной на рис. 1.

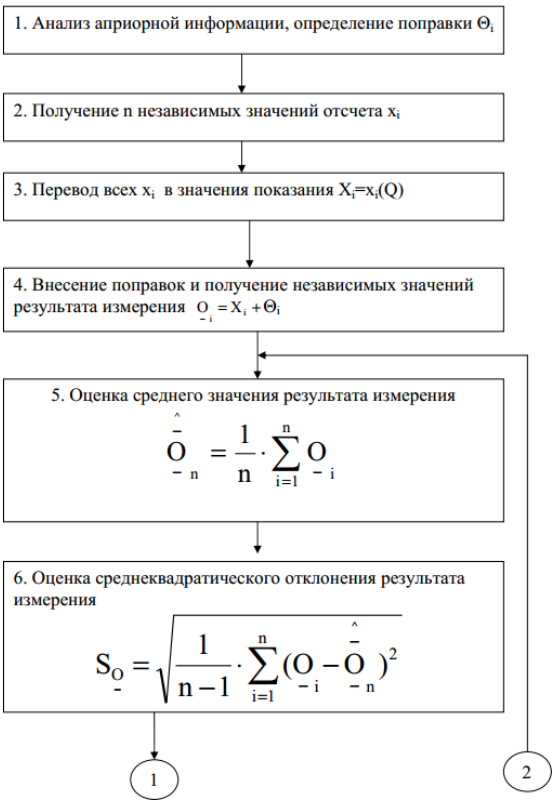


Рисунок 1 – Порядок выполнения многократного измерения при равноточных значениях отсчета

Перед выполнением измерений необходимо провести тщательный анализ априорной информации. Прежде всего, при необходимости, должен быть рассмотрен вопрос об исключении, компенсации или учете влияющих факторов. При подготовке к измерениям принимаются такие меры, как термостатирование (кондиционирование), экранирование помещений, а также амортизация средств измерений. Важным действием подготовительного этапа является анализ влияющих факторов и определение способа их исключения.

Грубой ошибкой или промахом является значение отсчета, существенно отличающееся от ожидаемого значения при данных условиях проведения измерительного эксперимента. Обычно грубые ошибки являются следствием значительного (иногда внезапного) изменения условий эксперимента: броски напряжения источника электропитания, неучтенное изменение окружающей температуры, а также неправильный отсчет показаний средства измерений или описки в протоколе эксперимента. Данные ошибки, согласно теории надежности больших систем, могут иметь существенные вероятности их появления. Иногда отличие результатов измерений настолько велико, что ошибка является явно видимой. В этом случае необходимо выяснить и устранить причину отклонений или отбросить этот результат как заведомо неверный. Если отличия не так велики, то это может быть следствием как ошибки, так и рассеивания отсчета. Поэтому ошибки можно отнести к категории случайных погрешностей и для их выявления следует применять методы проверки гипотез теории вероятностей.

Наиболее простым и производительным методом обнаружения ошибок в массивах экспериментальных данных является правило «трех сигм». Сущность правила состоит в следующем. Если при многократном измерении одной и той же величины постоянного размера сомнительное значение результата измерения отличается от среднего значения больше чем на три величины среднего квадратического отклонения, то с вероятностью 0,997 оно является ошибочным и его следует отбросить.

При осуществлении точных измерительных экспериментов и известном (нормальном) законе распределения погрешностей результатов измерений используется другой метод обнаружения ошибок, являющийся модификацией правила «трех сигм». В этом случае проверяемая гипотеза состоит в том, что некоторый результат не содержит грубой погрешности и принадлежит совокупности возможных значений результатов измерений с данным законом распределения.

Неравноточными являются измерения, в которых средние арифметические значения в рядах измерений являются оценками одного и того же значения измеряемой величины, а оценки дисперсий существенно отличаются друг от друга.

Необходимость обработки результатов неравноточных рядов измерений возникает, главным образом, при решении измерительной задачи выявления не исключенных систематических погрешностей. В этом случае измерения одной и той же величины проводятся несколькими операторами различными методами и разнотипными средствами, имеющими разную точность.

Если в сформированных рядах результатов полученные средние арифметические значения различаются несущественно и не выявляются систематические погрешности измерений, то целесообразно объединить все результаты в единый массив с целью получения более достоверной оценки измеряемой величины.

Если средние арифметические значения корректно проведенных измерений одной и той же величины различными методами и средствами отличаются существенно, то по вычисленным значениям определяется систематическая погрешность метода или средства измерения.

Необходимость обработки результатов неравноточных измерений возникает также, если контроль изделий проводится в разных лабораториях различными методами и получены отличающиеся друг от друга экспериментальные данные. В данном случае, используя все имеющиеся результаты измерений, необходимо получить более достоверное значение величины.

Данная оценка является средневзвешенной, а обратные дисперсии рядов измерений выступают при этом как веса отдельных средних арифметических. Веса характеризуются степенью доверия к соответствующим наблюдениям. Чем больше наблюдений в каждом ряду и чем меньше дисперсия результатов, тем больше степень доверия к полученному среднему арифметическому ряда и тем с большим весом оно учитывается при определении истинного значения измеряемой величины.

До сих пор мы говорили о результатах измерений, точность которых (степень доверия к ним) была одинаковая, весьма близкая по величине. Строго говоря, в природе измерений не существует равноточных величин. Обеспечить это весьма сложно, да во многих случаях и нет в этом необходимости. К равноточным измерениям можно отнести все результаты, погрешности которых не выходят за пределы допустимой величины, например, двойной средней квадратической погрешности.

Часто приходится иметь дело с разнородными величинами. Например, при выполнении геодезических измерений использовать результаты длин линий, которые значительно отличаются по величине, либо измерены разными по точности приборами, либо однородные величины в группе измерены равноточно, но с разным числом измерений в группах и т.п. В этом случае, при оценке точности, говорят о неравноточных измерениях.

Если в качестве веса результата измерения взять число, которое характеризует точность, то по смыслу слова вес можно сказать, что, чем больше вес результата, тем выше его точность (тем меньше погрешность, с которой получен данный результат). Т.е. вес находится в обратно пропорциональной зависимости от погрешности результата.

УДК 621.391

ОБРАБОТКА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ПОСРЕДСТВОМ СВЕРТКИ

Матусевич П.А.[1], Сурвило И.С.[1], Турло А.В.[1]студенты гр.060801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ИКТ

Аннотация. В данной статье рассмотрена тема свертки цифровых изображений. Описаны основные принципы свертки и применение этого метода для обработки изображений. Рассмотрены популярные ядра для свертки и объяснены их различия. Приведены примеры применения свертки и обозначены преимущества этого метода обработки изображений.

Ключевые слова. свертка, обработка изображений, ядро свертки, эффекты свертки, применение свертки.

Изображения, созданные с помощью цифровых технологий, встречаются практически повсеместно. Как следствие, важность научных исследований в этой области, в связи с распространением компьютеров, систем машинного зрения и инструментов для обработки и хранения данных и изображений, значительно возросла. Свертка изображений является актуальной и важной технологией в области обработки изображений.

Свертка используется во многих областях, одними из основных являются:

1. Компьютерное зрение: свертка используется для обнаружения и выделения объектов на изображении, распознавания образов, сегментации изображений, устранения шума и т.д.
2. Обработка сигналов: свертка используется для фильтрации сигналов, устранения шума, сжатия данных, анализа спектра и т.д.
3. Финансы: свертка используется для анализа временных рядов, таких как котировки акций, курсов валют и т.д.
4. Сети передачи данных: свертка используется для обработки сигналов в сетях передачи данных, например, для декодирования сигналов, устранения шума и т.д.
5. Машинное обучение: свертка используется в глубоком обучении для извлечения признаков из изображений, аудио и видео, и для классификации и распознавания объектов.

В данной работе наибольшее внимание будет уделено свертке изображений. Свертка изображений — это математическая операция, которая позволяет применять ядро (или фильтр) к каждому пикселю изображения, чтобы получить новое изображение с измененными свойствами. Ядро свертки (или фильтр) — это матрица коэффициентов, которая перемещается по изображению с определенным шагом (шаг свертки). Каждый элемент ядра умножается на соответствующий элемент изображения, на котором оно находится, а затем все эти произведения суммируются. Этот процесс повторяется для каждой позиции ядра на изображении, пока все изображение не будет пройдено сверткой. Размер и значения коэффициентов ядра определяют, какой эффект будет иметь свертка на изображение. Например, если использовать ядро, которое содержит высокие значения в центре и низкие значения по краям, то свертка будет выделять контуры объектов на изображении. Если использовать ядро с отрицательными коэффициентами, то свертка будет осуществлять инверсию цветов на изображении.

Различные ядра могут быть использованы для достижения различных эффектов при обработке изображений, таких как фильтрация шума, увеличение резкости, обнаружение краев и текстур, и т.д. Кроме того, для определенных задач, таких как обнаружение объектов на изображении, могут быть использованы специально обученные ядра. В целом, ядро свертки является одним из наиболее важных элементов при обработке изображений с помощью свертки. От правильного выбора ядра зависит, какую информацию можно извлечь из изображения и какую задачу можно решить. Существует множество различных готовых ядер для свертки, каждое из которых может быть использовано для обработки изображений в зависимости от задачи. Ниже перечислены некоторые из наиболее популярных ядер для свертки изображений:

1. Ядро Собеля — это ядро используется для обнаружения краев на изображении. Оно содержит значения, которые позволяют определить направление края и его интенсивность. Пример работы данного ядра представлен на рисунке 1.
2. Ядро Гаусса — это ядро используется для размытия изображения или уменьшения шума. Оно содержит значения, которые имеют распределение Гаусса вокруг центрального пикселя. Пример работы так же представлен на рисунке 2.

3. Ядро Прюитта — это ядро также используется для обнаружения краев на изображении, но оно более чувствительно к углам и содержит больше информации об угле края.

4. Ядро Лапласа — это ядро используется для обнаружения текстур на изображении. Оно содержит значения, которые выделяют области с различными интенсивностями.

5. Ядро медианного фильтра — это ядро используется для удаления шума на изображении. Оно заменяет каждый пиксель на медианное значение в окрестности этого пикселя.

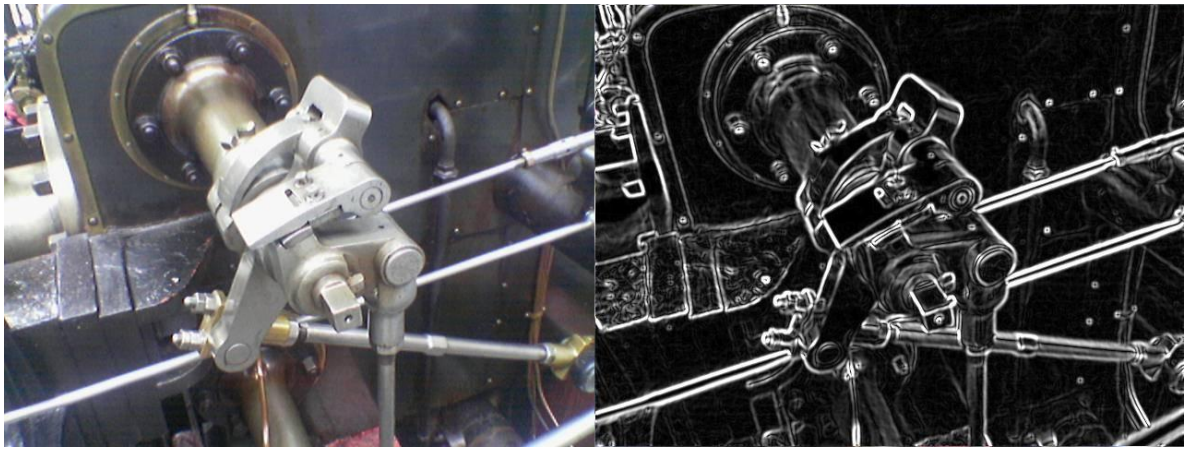


Рисунок 1 – Применение ядра Собеля к изображению.

Рисунок 2 – Применение ядра Гаусса к изображению.

Таким образом применяя разнообразные фильтры и их комбинации можно добиться требуемых эффектов. Самыми часто используемыми эффектами обработки изображений являются:

1. Сглаживание изображения. Это эффект, который используется для смягчения изображения и удаления мелких деталей, что помогает сделать изображение более пригодным для обработки. Сглаживание может быть полезно, когда нужно уменьшить шум в изображении или сделать его более однородным.

2. Усиление краев. Применяется для выделения границ объектов на изображении. Усиление краев может быть полезным, когда требуется сделать объекты более яркими и контрастными, и выделить их на фоне.

3. Изменение контраста и яркости. Это эффект, который используется для изменения контраста и яркости изображения. Можно использовать этот эффект, чтобы сделать изображение более ярким или темным, увеличить контрастность, и сделать цвета более насыщенными или менее яркими.

4. Изменение размера изображения - используется для изменения размера изображения. С помощью свертки можно уменьшить или увеличить изображение, чтобы оно стало более пригодным для использования в различных контекстах.

5. Удаление шума. Это эффект, для удаления мелких деталей и других элементов, которые могут выглядеть как шум.

6. Выделение текста. Используется для выделения текста на изображении делая его более четким и контрастным, что поможет улучшить его читаемость.

7. Детектирование границ. Эффект, который используется для выделения границ между объектами на изображении.

8. Осветление и затемнение определенных областей изображения. Применяется для изменения яркости и контраста определенных областей на изображении [1].

В рамках статьи, была разработана программная реализация свертки. В нее включен алгоритм итеративного перебора каждого элемента изображения из каждого канала, расчет свертки с использованием ядра в центре которого находится якорь и применение быстрого алгоритма, основанного на быстром преобразовании Фурье. Весь этот функционал был помещен в одну подпрограмму. В качестве аргументов, данная функция принимает трехмерный массив, представляющий собой разделенное на каналы изображение, ядро свертки, являющееся фильтром по отношению к многоканальному изображению, и дополнительные отвечающие за внутреннюю работу подпрограммы опции.

В рамках итеративного алгоритма перебора, передвижение идет по строкам и столбцам массива разных каналов. Для получения значения, которое запишется в матрицу отфильтрованного изображения, умножаются значения одного из каналов на ядро свертки. Данный алгоритм имеет следующий вид:

```
new_image = full([new_image_height, new_image_width, new_image_channels], 1)


for image_str_num in range(new_image_height):
    for image_pixel_num in range(new_image_width):
        for image_channel_num in range(new_image_channels):
            new_image_pixel = sum(image[image_str_num:image_str_num + kernel_height,
                                        image_pixel_num:image_pixel_num + kernel_width,
                                        image_channel_num] * kernel)
            new_image[image_str_num][image_pixel_num][image_channel_num] = new_image_pixel
```

Рисунок 3 – Алгоритм свертки

Для реализации быстрой свертки и, соответственно, быстрой фильтрации изображения за основу взято быстрое преобразование Фурье. В алгоритме вычисляется спектр каждого из каналов изображения и по отдельности умножаются на спектр ядра свертки. Каждое полученное значение записывается в матрицу, которая и является представлением нового, отфильтрованного изображения:

```
kernel = pad(kernel, ((0, new_image_height - 1), (0, new_image_width - 1)))
fft_kernel = fft2(kernel)

new_image_channel = list()

for image_channel_num in range(new_image_channels):
    new_image_channel.append(real(ifft2(fft2(image[:, :, image_channel_num])*fft_kernel)))

new_image_height, new_image_width = new_image_channel[0].shape
new_image = full([new_image_height, new_image_width, len(new_image_channel)], 0.00000)

if new_image_channels > 1:
    for image_str_num in range(new_image_height):
        for image_pixel_num in range(new_image_width):
            for image_channel_num in range(new_image_channels):
                new_image[image_str_num][image_pixel_num][image_channel_num] = \
                    new_image_channel[image_channel_num][image_str_num][image_pixel_num]
else:
    new_image = new_image_channel[0]
```

Рисунок 4 – Алгоритм быстрой свертки

Используя один из вышеперечисленных алгоритмов, получается отфильтрованное изображение, выводящееся в графический интерфейс пользователя в формате «до-после», где левое изображение - исходное, а правое - отфильтрованное К примеру, применив сглаживающий фильтр Гаусса, с размером ядра свертки 13x13, получается следующее изображение:

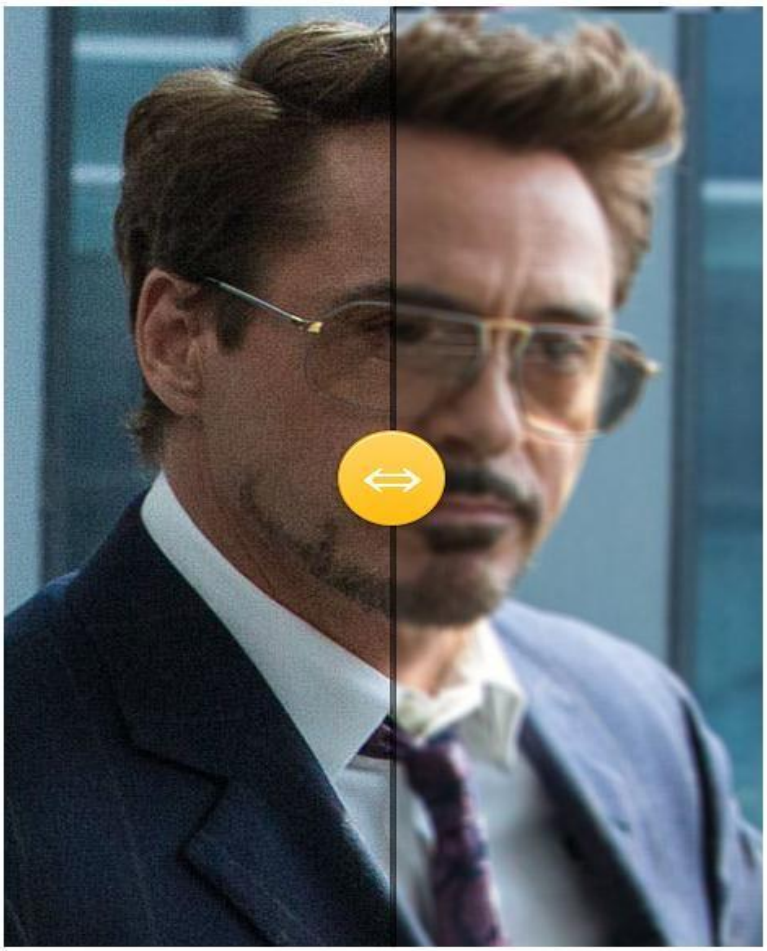


Рисунок 5 – Пример работы алгоритмов

Подводя итог, можно сказать, что свертка является мощным инструментом для обработки изображений, который может использоваться для создания различных эффектов и улучшения качества изображений. С её помощью можно изменять яркость, контрастность, цветовую гамму и другие параметры изображения, а также обнаруживать границы объектов на изображении, улучшать резкость и детализацию изображения. Всё вышеперечисленное доказывает, что свертка - актуальная и важная технология в обработке изображений и сигналов, а ее применение продолжает расширяться в различных областях науки и технологий.

Список использованных источников:

1. Гонсалес Р. Цифровая обработка изображений / Гонсалес Р., Вудс Р. // Москва: Техносфера, 2005.

УДК 621.391

АТАКА ЧЕРВОТОЧИНЫ В МОБИЛЬНЫХ AD-HOC СЕТЯХ

Нгуен Ч.Т, магистрант гр.215101

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Цветков В.Ю. – Доктор. тех. наук

Аннотация. Данная статья представляет обзор атаки червоточины на мобильные ad-hoc сети. В статье описываются основные характеристики и последствия этой атаки и методы, которые злоумышленники используются для выполнения такой атаки.

Ключевые слова. MANET, атака червоточины, ad-hoc.

Введение. В настоящее время беспроводные сети широко используются в различных областях, в том числе и в мобильных ad-hoc сетях (MANET). Однако, в связи с их открытой структурой и динамичностью, они становятся более уязвимыми для атак и угроз безопасности. Одной из серьезных угроз безопасности MANET является атака червоточины. Атака червоточины MANET представляет собой атаку на протоколы маршрутизации в MANET, которая осуществляется с помощью внедрения злонамеренных узлов в сеть. В этой атаке злоумышленник использует уязвимость в протоколе маршрутизации, чтобы внедрить свой злонамеренный узел в сеть. Этот узел затем может захватывать информацию, перехватывать пакеты данных или нарушать работу сети. Цель данной статьи является представлением обзор атаки червоточины MANET на мобильные ad-hoc сети. В статье будут описаны основные характеристики и последствия этой атаки, а также приведены методы для выполнения этой атаки.

Основная часть. Атака червоточины направлена на подслушивание информации, иногда хакеры устраивают атаки, чтобы нарушить производительность сети. Для атаки хакеры используют два вредоносных узла, которые соединяются друг с другом через частную ссылку, называемую туннелированием или с использованием механизмов инкапсуляции. Атаки через червоточины могут выполняться в двух режимах: скрытом режиме и режиме присоединения [1].

Использование частной ссылки: для атаки хакеры используют 2 вредоносных узла (M_1, M_2), которые соединяются друг с другом через частный путь, называемый туннелем [2, 3]. Получив запрос маршрутизации RREQ, злонамеренный узел M_1 пересылает пакет RREQ к M_2 через туннель, M_2 продолжает пересылать RREQ к месту назначения. Получив пакет RREQ, узел назначения отправляет пакет RREP через туннель к источнику. В результате исходный узел устанавливает маршрут через туннель, поскольку этот маршрут стоит меньше, чем фактический маршрут. На рисунке 1 описана атака червоточины с использованием частной ссылки.

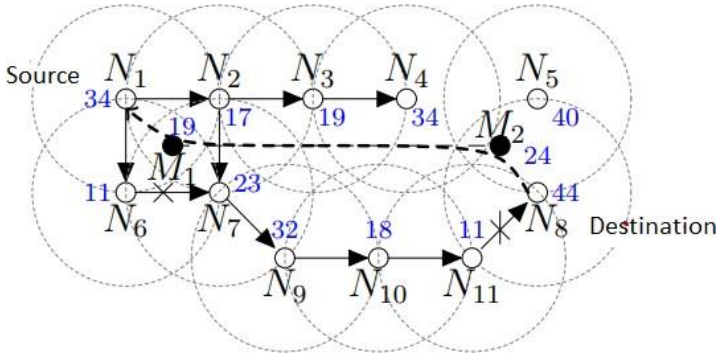


Рисунок 1 – атака червоточины с исползованием частной ссылки

Описание процесса, посредством которого исходный узел N_1 обнаруживает маршрут к месту назначения N_8 в топологии сети с двумя вредоносными узлами (M_1, M_2), соединяющимися через туннель. Исходный узел N_1 широковещательно передает пакет RREQ для обнаружения маршрута к целевому узлу N_8. Первый пакет RREQ к месту назначения на туннельном маршруте: $\{N_1 x\, M_1 x\, M_2 x N_8\}$. Когда пакет получает пакет RREQ, злонамеренный узел M_1 добавляет новую

запись в таблицу маршрутизации, чтобы представить маршрут к источнику N_1, информация о записи: Node= N_1, NH = N_1, HC = RREQ.HC+1=1, SN=35. Точно так же злонамеренный узел M_2 добавляет новую запись в таблицу маршрутизации, чтобы представить маршрут к источнику N_1, через следующий переход M_1, информация записи: Node =N_1, NH=M_1, HC=RREQ.HC+1=2, SN=35. Наконец, после получения пакета RREQ узел назначения N_8 добавляет новую запись в таблицу маршрутизации, чтобы представить маршрут обратно к N_1 через следующий переход M_2, информация записи: Node= N_1, NH= M_2, HC=RREQ. .HC+1=3, SN=35, и узел назначения N_8 отвечает на маршрут, посылая пакет RREP в направлении $\{N_8 x\ M_2 x\ M_1 x\ N_1\}$. Кроме того, второй пакет RREQ также достигает пункта назначения по маршруту $\{N_1 \rightarrow N_2 \rightarrow N_7 \rightarrow N_9 \rightarrow N_{10} \rightarrow N_{11} \rightarrow N_8\}$. Но узел назначения N_8 отбрасывает второй полученный пакет RREQ, поскольку он уже обработан. Детали управляющего пакета и таблицы маршрутизации перечислены в таблице 1.

Таблица 1 – Результат обнаружения маршрута при атаке червоточины

Пакет	Узел	Информация о пакете [LH] [IP_{src}, IP_{dst}, HC, SN]	Таблица маршрутизации			
			Node	NH	HC	SN
RREQ	N_1	$[N_1]$ $[N_1, N_8, 0, 35]$	NULL			
	N_2	$[N_2]$ $[N_1, N_8, 1, 35]$	N_1	N_2	1	35
	N_3	$[N_3]$ $[N_1, N_8, 2, 35]$	N_1	N_2	2	35
	N_4	$[N_4]$ $[N_1, N_8, 3, 35]$	N_1	N_3	3	35
	N_5	Пакет RREQ не получен				
	N_6	$[N_6]$ $[N_1, N_8, 1, 35]$	N_1	N_1	1	35
	N_7	$[N_7]$ $[N_1, N_8, 2, 35]$	N_1	N_1	2	35
	N_8	$[N_8]$ $[N_1, N_8, 3, 35]$	N_1	M_2	3	35
	N_9	$[N_9]$ $[N_1, N_8, 3, 35]$	N_1	N_7	3	35
	N_{10}	$[N_{10}]$ $[N_1, N_8, 4, 35]$	N_1	N_9	4	35
	N_{11}	$[N_{11}]$ $[N_1, N_8, 5, 35]$	N_1	N_{10}	5	35
	M_1	$[M_1]$ $[N_1, N_8, 1, 35]$	N_1	N_1	1	35
	M_2	$[M_2]$ $[N_1, N_8, 2, 35]$	N_1	M_1	2	35
RREP	N_8	Инициализация пакета RREP $[N_8]$ $[N_8, N_1, 0, 45]$				
	M_2	$[M_2]$ $[N_8, N_1, 1, 45]$	N_8	N_8	1	45
	M_1	$[M_1]$ $[N_8, N_1, 2, 45]$	N_8	M_2	2	45
	N_1	$[N_1]$ $[N_8, N_1, 3, 45]$	N_8	M_1	3	45

Использование инкапсуляции: этот метод использует 2 вредоносных узла, которые отображаются в сети как обычные узлы. Получив пакет RREQ, злонамеренный узел инкапсулирует его перед передачей пакета RREQ получателю через другие промежуточные узлы. Инкапсуляция выполняется таким же образом при получении пакета RREP. Цель состоит в том, чтобы снизить стоимость пакета управления путем, установив значение поля HC равным 0. Кроме того, злонамеренный узел увеличивает значение поля ID_broadcast пакета RREQ, чтобы сосед согласился обработать пакет, если он уже получил его тот же пакет от другого соседа. Цель состоит в том, чтобы исходный узел установил путь по маршруту, содержащему вредоносный узел, потому что стоимость ниже, чем фактический маршрут. В зависимости от местоположения маршрут

содержит один или два вредоносных узла [2, 3]. Атака с использованием метода инкапсуляции описана на рисунке 2.

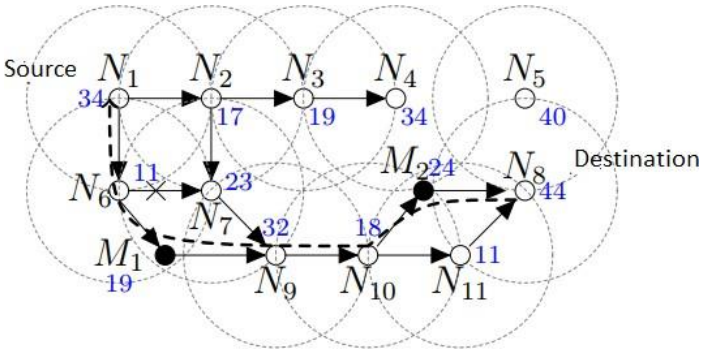


Рисунок 2 – Атака червоточины с использованием инкапсуляции

На рисунке 2. показаны два вредоносных узла M_1 и M_2, использующие инкапсуляцию для атаки на сеть. Узел N_9 получает оба пакета RREQ от источника N_1 по маршруту $\{N_1 \rightarrow N_2 x\, N_7\}$ и $\{N_1 \rightarrow N_6 x\ M_1\}$. Узел N_9 обнаруживает, что расход поиска через следующий переход M_1 составляет 1 переход, потому что значение HC пакета RREQ повторно инициализируется при пересылке через M_1 . Таким образом, N_9 устанавливает обратный маршрут к источнику через следующий переход M_1, добавляя новую запись в таблицу маршрутизации, информация о записи: NODE=N_1, NH=M_1, HC=RREQ.HC+1=1, SN=35. Пакеты RREQ, поступающие от N_7, не принимаются из-за более высокой стоимости. Узел назначения N_8 получает 2 пакета RREQ, приходящих от узлов N_{11} и M_2, пакет, приходящий от N_{11} имеет стоимость 3 переходов, поскольку он должен пересылаться через 3 промежуточных узла, включая $\{N_9, N_{10}, N_{11}\}$, в то время как пакет RREQ поступает от M_2 стоит 1 переход. Следовательно, узел назначения устанавливает маршрут к источнику через следующий переход M_2 , добавляя новую запись в таблицу маршрутизации, информация о записи: NODE=N_1, NH=M_2, HC=RREQ.HC+1=1, SN=35. Пакет RREQ, поступающие от N_{11}, не принимаются из-за больших накладных расходов. Узел назначения N_8 отвечает на исходный маршрут, посылая пакет RREP в направлении $\{N_8 \rightarrow M_2 \rightarrow N_{10} \rightarrow N_9 \rightarrow M_1 \rightarrow N_6 \rightarrow N_1\}$. Все промежуточные узлы сохраняют маршрут к месту назначения N_8 каждый раз, когда они получают пакет RREP, и пересылают пакет RREP обратно к источнику, используя запись в таблице маршрутизации. В результате исходный узел N_1 устанавливает маршрут к месту назначения через следующий переход N_1 со стоимостью назначения 2 перехода, этот маршрут содержит два злонамеренных узла M_1 и M_2, как подробно описано в таблице 2.

Таблица 2 – Результат обнаружения маршрута при атаке червоточины

Пакет	Узел	Информация о пакете [LH] [IP_{src}, IP_{dst}, HC, SN]	Таблица маршрутизации			
			Node	NH	HC	SN
RREQ	N_1	[N_1] [N_1, N_8 , 0, 35]	NULL			
	N_2	[N_2] [N_1, N_8 , 1, 35]	N_1	N_1	1	35
	N_3	[N_3] [N_1, N_8 , 2, 35]	N_1	N_2	2	35
	N_4	[N_4] [N_1, N_8 , 3, 35]	N_1	N_3	3	35
	N_5	с				
	N_6	[N_6] [N_1, N_8 , 1, 35]	N_1	N_1	1	35
	M_1	[M_1] [N_1, N_8 , 0, 35]	N_1	N_6	2	35
	N_7	[N_7] [N_1, N_8 , 2, 35]	N_1	N_2	2	35

Пакет	Узел	Информация о пакете [LH] [IP_{src}, IP_{dst}, HC, SN]	Таблица маршрутизации			
			Node	NH	HC	SN
	N_8	$[N_8]$ $[N_1, N_8$, 6, 35]	~~N_1~~ N_1	~~N_{11}~~ M_2	~~6~~ 1	~~35~~ 35
	N_9	$[N_9]$ $[N_1, N_8$, 3, 35]	~~N_1~~ N_1	~~N_7~~ M_1	~~3~~ 1	~~35~~ 35
	N_{10}	$[N_{10}]$ $[N_1, N_8$, 4, 35]	N_1	N_9	4	35
	N_{11}	$[N_{10}]$ $[N_1, N_8$, 5, 35]	N_1	N_{10}	5	35
	M_2	$[M_2]$ $[N_1, N_8$, 0, 35]	N_1	N_{10}	3	35
RREP	N_8	Инициализация пакета RREP $[N_8]$ $[N_8, N_1$, 0, 45]				
	M_2	$[M_2]$ $[N_8, N_1$, 0, 45]	N_8	N_8	1	45
	N_{10}	$[N_{10}]$ $[N_8, N_1$, 1, 45]	N_8	M_2	1	45
	N_9	$[N_9]$ $[N_8, N_1$, 2, 45]	N_8	N_{10}	2	45
	M_1	$[M_1]$ $[N_8, N_1$, 0, 45]	N_8	N_9	3	45
	N_6	$[N_6]$ $[N_8, N_1$, 1, 45]	N_8	M_1	1	45
	N_1	$[N_1]$ $[N_8, N_1$, 2, 45]	N_8	N_2	2	45

Заключение. В статье представлены два метода атаки червоточины, которые злоумышленники используют для атаки. В туннельном режиме управляющий пакет не изменяется при прохождении через вредоносный узел, поэтому решения по обеспечению безопасности, использующие проверку целостности пакетов, не будут работать. В механизме инкапсуляции злонамеренный узел изменил параметры пакета, поэтому может использовать механизм проверки целостности пакета, чтобы определить, была ли сеть атакована.

Список использованных источников:

1. Wormhole Attack Detection Technique in Mobile Ad Hoc Networks / Kaur P., Kaur D., Mahajan R // Vol. 97. P. 2939–2950.

2. Wormhole Attack in Wireless Ad Hoc Networks / Khabbazian M., Mercier H., Bhargava V.K // Vol. 8. P.736–745.

3. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET / Jen S.M., Laih C.S., Kuo W.C// Vol. 9. P. 5022–5039

UDC 621.391

WORMHOLE ATTACK IN MOBILE AD-HOC NETWORKS

Nguyen T.T

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

Tsvetkov V.Y. – Doctor of Technical Sciences

Annotation. This article provides an overview of the MANET wormhole attack on mobile ad-hoc networks. The article describes the main characteristics and consequences of this attack and the methods used by attackers to carry out such an attack.

Keywords. MANET, wormhole attack, ad-hoc.

УДК 621.391

МОДЕЛИРОВАНИЕ ПРОКОЛОВ МАРШРУТИЗАЦИИ ПРИ АТАКЕ ЧЁРНОЙ ДЫРЫ В МОБИЛЬНЫХ AD-HOC СЕТЯХ

Нгуен Ч.Т, магистрант гр.215101

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Цветков В.Ю. – Доктор. тех. наук

Аннотация. В статье представлено моделирование протоколов маршрутизации: AODV, IDSAODV в мобильных ad-hoc сетях при атаке чёрной дыры.

Ключевые слова. Атака чёрной дыры, AODV, IDSAODV.

Введение. При атаке чёрной дыры [1] злонамеренный узел утверждает, что у него есть действительный маршрут ко всем другим узлам в сети для перехвата трафика между узлами. После получения переданных данных он не пересылает, а отбрасывает все эти пакеты. Следовательно, этот узел чёрной дыры может отслеживать и анализировать трафик всех узлов в сети, на которую он напал.

AODV (Ad hoc On-demand Distance Vector) – Это протокол маршрутизации с одним маршрутом, использующий проактивное обнаружение маршрута. Исходный узел обнаруживает маршрут только тогда, когда ему нужно переслать данные. При каждом обнаружении маршрута исходный узел устанавливает уникальный маршрут к месту назначения и имеет наилучшую стоимость маршрута. Расходы маршрутизации протокола AODV определяется на основе количества переходов для достижения пункта назначения. Протокол AODV часто становится жертвой атак чёрной дыры. В каждом пакете маршрутизации AODV некоторые важные поля, такие как количество переходов HC, порядковый номер назначения, SN источника и получателя, заголовок IP, IP-адреса источника и получателя AODV, идентификационный номер RREQ. Ошибки в любом из вышеперечисленных полей могут привести к сбою AODV. Для выполнения атаки чёрной дыры в протоколе AODV злонамеренный узел ждет пакета RREQ, отправленного от его соседей. Когда он получает пакет RREQ, он немедленно отправляет ответ на пакет RREP с ложным содержимым, устанавливая самое высокое значение SN и минимальное значение HC, не выполняя проверку таблицы маршрутизации, чтобы увидеть, существует ли маршрут к месту назначения, прежде чем другие узлы отправят ответ о маршруте. Затем любые данные, передаваемые от исходного узла к узлу назначения, полностью отбрасываются злоумышленником, вместо того, чтобы пересылаться в соответствующий пункт назначения.

Протокол IDSAODV (Intrusion Detection System Ad hoc On-demand Distance Vector) – это безопасный протокол маршрутизации против атак чёрной дыры. Протокол IDSAODV основан на идее, что рабочий механизм протокола AODV заключается в проверке номера SN ответного пакета RREP. Если в сети присутствует узел чёрной дыры, то этот узел чёрной дыры немедленно ответит на пакет RREP с наивысшим присвоенным номером SN и, конечно же, немедленно ответит узлу-источнику, отправившем запрос RREQ. Следовательно, необходимо только отбросить первый полученный пакет RREP и принять второй пакет RREP с наивысшим SN, чтобы установить маршрут связи с использованием механизма буферизации пакетов.

В этой статье представлено моделирование протоколов AODV и IDSAODV при атаке чёрной дыры с помощью программного обеспечения для моделирования NS2. Затем сравните производительность протоколов маршрутизации на основе параметра коэффициента успешной доставки пакетов (Packet Delivery Ratio) и накладных расходов на маршрутизацию.

Основная часть. Сценарий моделирования построен на 20 узлах со случайным расположением инициализации в географической области размером 1000 м × 1000 м с дальностью радиопередачи каждого узла 250 м (радиус). Координаты каждого узла в месте области моделирования имеют форму (x, y, z), где z имеет значение 0. Узлы двигаются в соответствии с моделью Random Waypoint [2], что означает, что узел сначала занимает случайное положение в области моделирования и остается там в течение периода, называемого временем паузы. По истечении этого временного интервала узел случайным образом выбирает пункт назначения в области моделирования и скорость, которая равномерно распределяется между [мин. скорость, макс. скорость]. Затем узел перемещается в новое место с выбранной скоростью. При достижении нового местоположения узел делает паузу на выбранный период времени согласно равномерному

распределению между [Pmin, Pmax], а затем возобновляет процесс. При моделировании инициализация позиций узлов и процесс движения в соответствии с приведенной выше моделью выполняется с помощью инструмента «./setdest» – инструмент, которры был установлен в эмуляторе NS-2. Запуска setdest для создания топодогии сети с различными скоростями движения 10, 15 м/с. Параметры моделирования представлены в таблице 1.

Таблица 1 – Параметры моделирования

Параметры	Значения
Область моделирования	1000 м × 1000 м
Количество узлы	20
Радиус покрытия	250 м
Контракт трафика	CBR
Количество соединений	10
Скорость доставки пакетов	4 пакета/с
Скорость движения	10, 15 м/с
Количество злонамеренных узлов	0, 2, 4
Размер пакетов	512 bytes

Для каждой скорости движения будут установлены протоколы AODV и IDSAODV с увеличением доли узлов чёрной дыры по сравнению с общим количеством сетевых узлов. Результаты анализа протоколов с учетом скорости движения узлов сети и увеличения доли узлов-чёрных дыр в общем количестве узлов представлены на рисунках 1, 2, 3, 4.

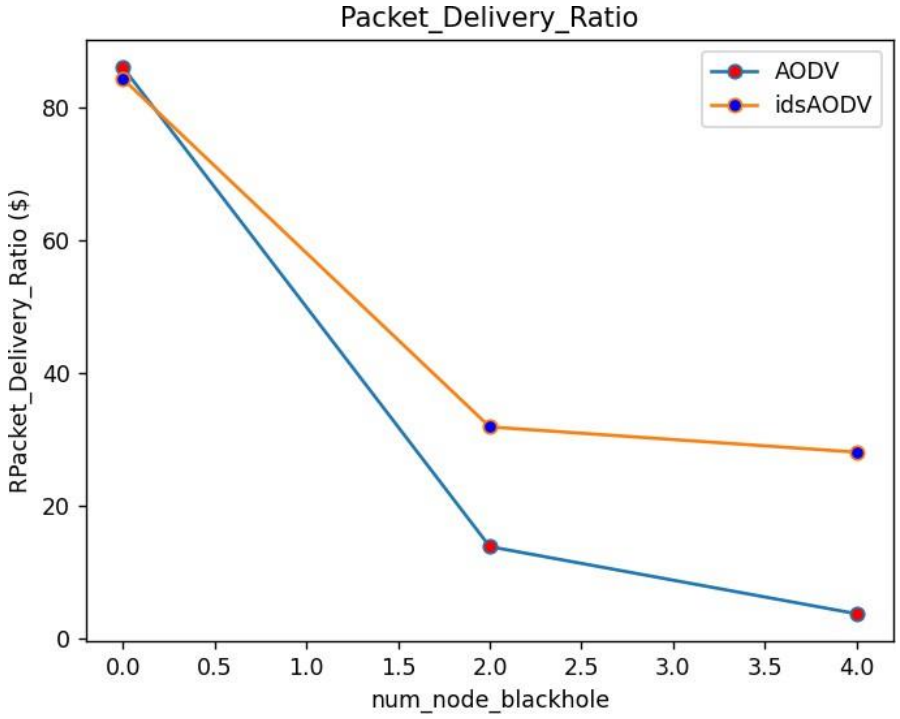


Рисунок 1 – Коэффициент успешной доставки пакетов при движении узлов 10 м/с

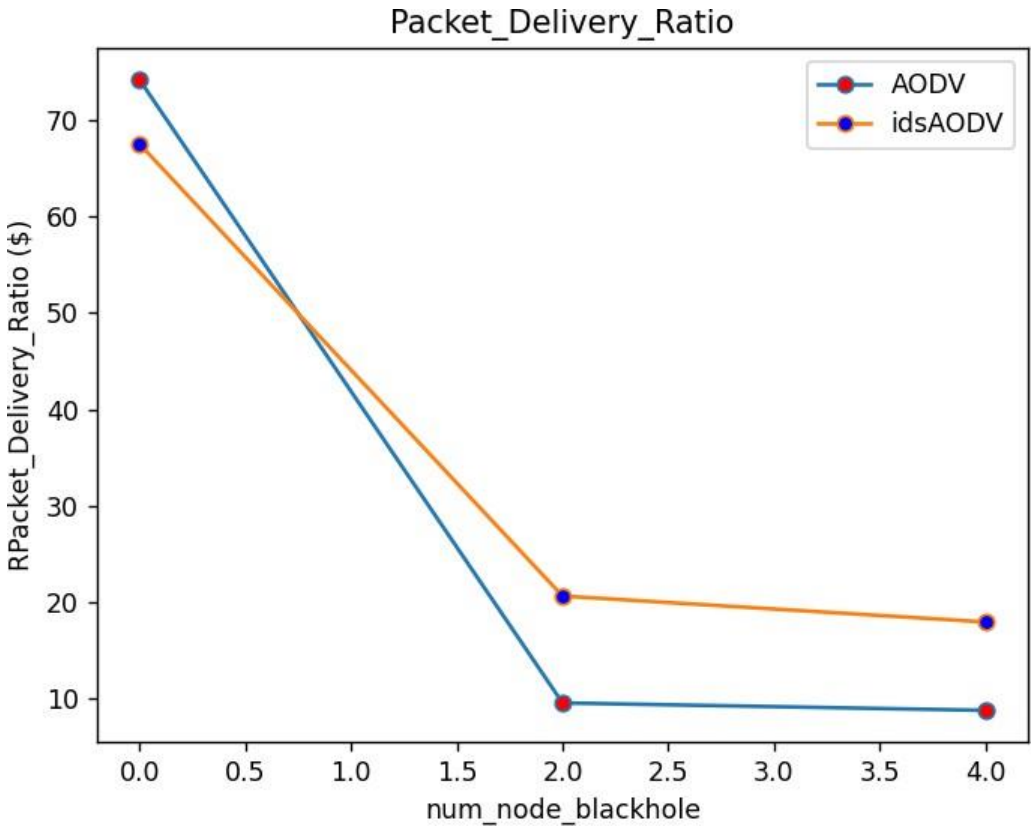


Рисунок 2 – Коэффициент успешной доставки пакетов при движении узлов 15 м/с

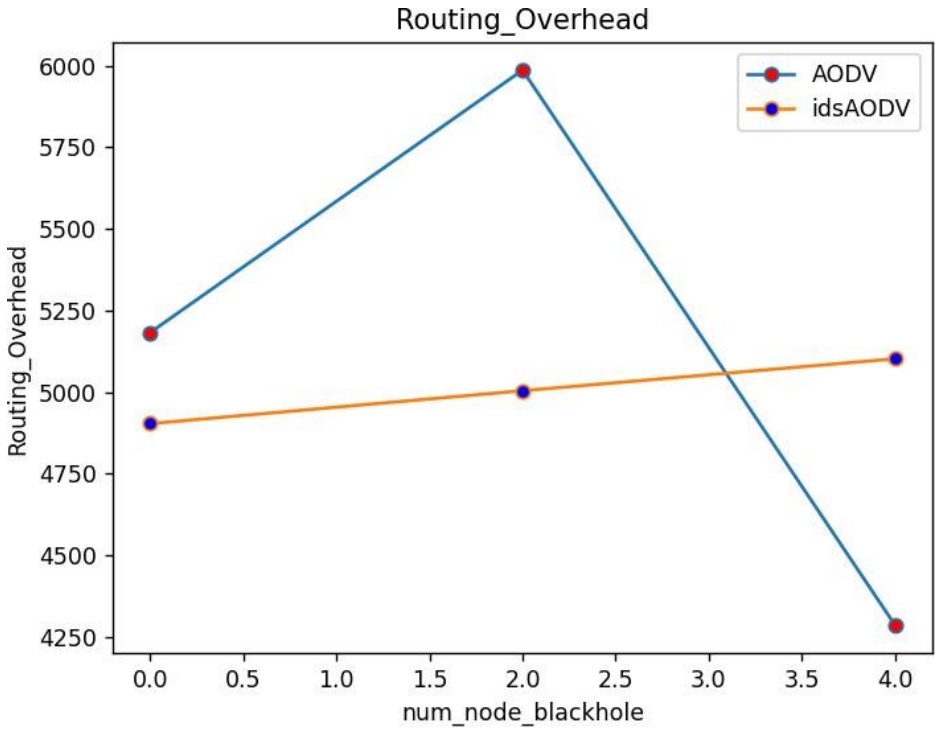


Рисунок 3 – Расходы на маршрутизацию, когда узлы перемещаются со скоростью 10 м/с

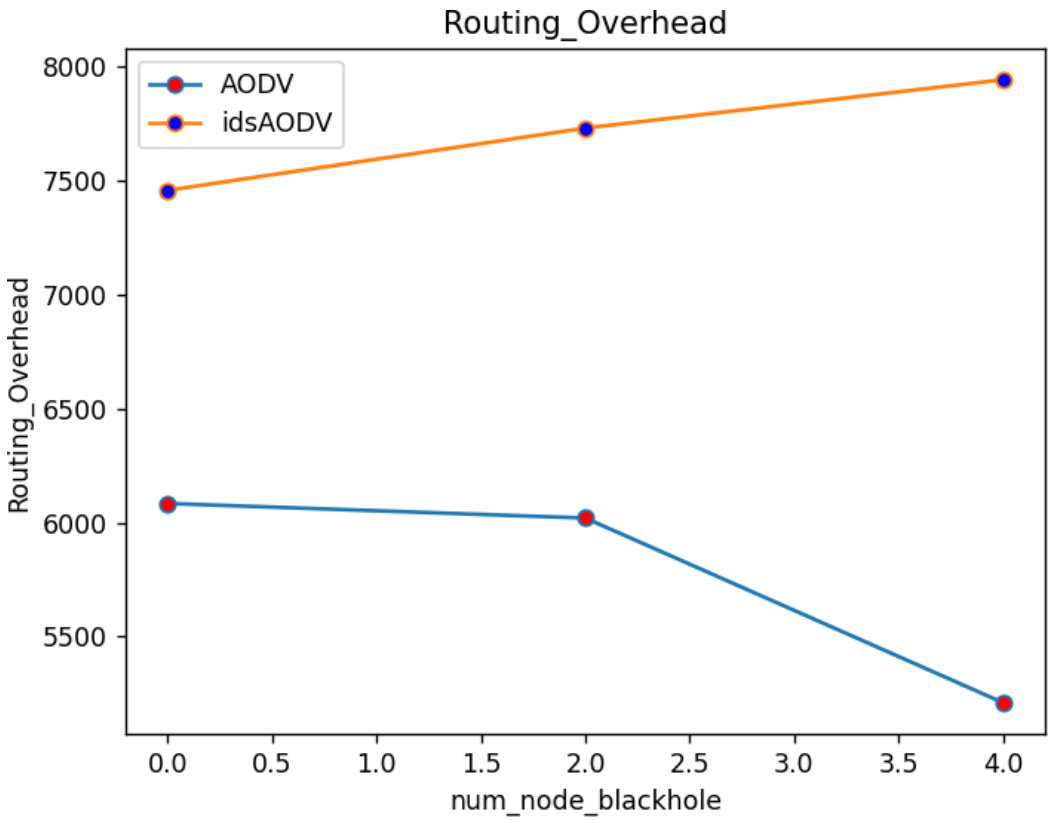


Рисунок 4 – Расходы на маршрутизацию, когда узлы перемещаются со скоростью 15 м/с

Когда в сети нет атакующих чёрных узлов. Коэффициент успешной доставки пакетов протокола AODV выше, чем у протокола IDSAODV. В случае узлов, движущихся со скоростью 15 м/с, вероятность успешной доставки пакетов для всех протоколов снижается, для протокола AODV — 74,19 %, для протокола IDSAODV — 67,53 %.

Когда в сети есть атакующие чёрные узлы. Коэффициент успешной доставки пакетов двух протоколов маршрутизации значительно снижается. Протокол IDSAODV имеет лучшую коэффициент успешной доставки пакетов, чем протокол AODV, поскольку количество узлов атаки чёрной дыры в сети увеличивается. По мере увеличения количества узлов атаки чёрной дыры, расходы на маршрутизацию протокола IDSAODV также увеличивается.

Заключение. Атаки чёрной дыры оказывают большое влияние на коэффициент успешной доставки пакетов. При атаке чёрной дырой протокол IDSAODV имеет лучший коэффициент успешной доставки пакетов, чем протокол AODV, но ненамного. Скорость движения узлов также существенно влияет на коэффициент успешной доставки пакетов в сети. Ограничение протокола IDSAODV заключается в том, что в некоторых случаях не всегда бывает так, что первый пакет RREP с наибольшим полученным значением SN также поступает из узла чёрной дыры, то есть когда узел назначения или промежуточный узел отвечает на Пакет RREP с наибольшим SN расположен ближе к узлу назначения, чем к узлу чёрной дыры.

Список использованных источников:

1. Routing Security in Wireless Ad Hoc Networks / H. Deng, W. Li and D. P. Agrawal // IEEE Communication Magazine, October 2002

2. Ad hoc wireless networks: Architecture and Protocols / C. Siva Ram Murthy, B. S. Manoj // Prentice Hall Publishers, May 2004.

UDC 621.391

SIMULATION OF ROUTING PROTOCOLS DURING A BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORKS

Nguyen T.T

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

Tsvetkov V.Y. – Doctor of Technical Sciences

Annotation. The article presents the modeling of routing protocols: AODV, IDSAODV in mobile ad-hoc networks during a black hole attack.

Keywords. IDSAODV, AODV, black hole attack.

УДК 004.3.049.77

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ПРИ РАЗРАБОТКЕ ПРОЕКТНЫХ РЕШЕНИЙ

Новиков А.А., магистрант

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Стержанов М.В. – кандидат технических наук

Аннотация. Практический опыт применения многочисленных алгоритмов тематического моделирования убеждает, что тематические модели обладают огромным «запасом решений», в том числе при разработке проектных решений в различных областях науки. При исследовании методов тематического моделирования при разработке проектных решений также исследуется возможность переноса алгоритмов некоторых методов на язык программирование Python. В рамках исследования предложена примерная последовательность шагов, необходимых и достаточных для предварительной обработки данных на примере построения тематического профиля национальных интернет-СМИ.

Ключевые слова. Интеллектуальный анализ данных, тематическое моделирование, тематическая модель, вероятностные тематические модели, эмбеддинг, токенизация.

В настоящее время, благодаря глобальному распространению сети Интернет большинство пользователей получили возможность в невиданных ранее объёмах получать и генерировать информацию. Это стало не только благом, но и породило ряд проблем, связанных со сбором, анализом и систематизацией информации. Аналитики, осуществляющие свою деятельность в различных областях, вынуждены использовать соответствующие этим условиям новые подходы к сбору, анализу и систематизации интересующих данных.

Для описания нового свойства таких данных, которые отличаются большим объёмом, высокой скоростью роста и огромным многообразием своих форм, был введён термин «большие данные» (big data). Феномен «больших данных» сформировал потребность в новых методах обработки и анализа, способных извлекать из этих, как правило, неструктурированных данных полезное «зерно», знание. Совокупность таких методов обозначается термином «интеллектуальный анализ данных» (data mining).

Из этой совокупности выделяется подмножество, специализирующееся на анализе текстовых данных - «интеллектуальный анализ текстовых данных» (text mining). Кроме того, выделяется группа методов, которые выполняют задачу тематического моделирования - построения статистических моделей, определяющих тематическую принадлежность каждого документа из корпуса.

Тематическое моделирование – это одна из современных технологий обработки естественного языка (англ. Natural language processing, NLP), активно развивающаяся с конца 90-х годов. Тематическая модель коллекции текстовых документов определяет, к каким темам относится каждый документ, и какие слова образуют каждую тему. Тематическое моделирование не претендует на полноценное понимание естественного языка (англ. natural language understanding, NLU), однако выявление тематики можно считать определённым шагом в этом направлении [1].

Тематическое моделирование принято относить к машинному обучению без учителя, поскольку темы строятся автоматически, но текстовым данным. Дня этого не требуется ни разметки, ни словарей, ни баз экспертных знаний. Существуют продвинутые тематические модели, способные учитывать такого рода данные дня улучшения тем и решения трудных задач текстовой аналитики. Такие модели тоже рассматриваются в данной книге.

Тематическая модель, как и нейросетевая, преобразует текст в векторное представление или эмбеддинг (embedding). Под эмбеддингом понимается возможность уменьшения размерности таких признаков ради повышения производительности модели. Прежде чем говорить о структурированных наборах данных, полезно будет разобраться с тем, как обычно используются эмбеддинги.

Нейросетевые эмбеддинги не интерпретируемы, мы не понимаем смысла их координат. Тематический эмбеддинг – это вектор вероятностей тем. В каждой теме есть наиболее частотные слова, и если модель построена хорошо, то они оказываются связанными по смыслу. Глядя на них, можно сказать, о чём эта тема, составить её текстовое описание, дать ей название. Наиболее ценное свойство тематических моделей в том, что коллекция сама собой кластеризуется на интерпретируемые темы.

Тематическое моделирование похоже на кластеризацию документов. Отличие в том, что при обычной «жёсткой» кластеризации (hard clustering) документ целиком относится к одному кластеру,

тогда как тематическая модель осуществляет мягкую кластеризацию (soft clustering), распределяя содержимое документа по нескольким кластерам-темам. Тематическое моделирование называют также мягкой би-кластеризацией, поскольку каждое слово также распределяется по темам.

Вероятностная тематическая модель (англ. Probabilistic topic model, PTM) определяет вероятности тем в каждом документе и вероятности слов в каждой теме. Такие модели предсказывают вероятности появления слов в документах, но делают это не настолько хорошо, как глубокие нейронные сети типа BERT или GPT-3, но и намного проще и обладают свойством интерпретируемости.

Вероятностные тематические модели находят множество применений. Это выявление трендов в новостных потоках, патентных базах, научных публикациях, многоязычный информационный поиск, классификация и категоризация документов, тематическая сегментация текстов, суммаризация текстов, поиск тематических сообществ в социальных сетях, тегирование веб-страниц, обнаружение текстового спама. В том числе, тематическое моделирование может быть успешно использовано для решения социологических задач. С их помощью, например, можно определить разницу в освещении одних и тех же событий и фактов национальными и иностранными средствами массовой информации с использованием глобальной компьютерной сети Интернет (далее – интернет-СМИ) [1] или увидеть, как менялось отношение интернет-СМИ к конкретному событию, объекту, субъекту и т.д., в определенный временной интервал.

Темой данного исследования является изучение разнообразия методов тематического моделирования при разработке проектных решений, перенос алгоритмов некоторых методов на мультипарадигменный язык программирования Python. В качестве примера показывается последовательность шагов, необходимых для предварительной обработки данных, для построения тематического профиля национальных интернет-СМИ. Обосновывается выбор количества тем для построения модели тематического моделирования.

Основные этапы необходимых для построения тематического профиля национальных интернет-СМИ.

Сбор данных

На данном этапе предполагается определить совокупность в построении тематического профиля национальных интернет-СМИ. Основу исследуемого пула составят новостные статьи интернет-СМИ, опубликованные в исследуемый период (истекший 2022 год). Интернет-СМИ, в целях построения указанного профиля, считается веб-сайт, ставящий своей задачей выполнение функции средства массовой информации в сети Интернет и ориентированный на людей, живущих в Республике Беларусь.

Новостная статья - не просто текст. Это документ в электронном виде, позволяющий установить его целостность и подлинность, который подтвержден путем идентификации его принадлежности к официальному зарегистрированному, в установленном законом Республики Беларусь порядке интернет-ресурсу, выступающим в роли интернет-СМИ, имеющий свою структуру. В его структуре интерес представляют такие элементы, как собственно текст (тело статьи), название, дата публикации, комментарии и принадлежность к национальному интернет-СМИ.

Для сбора статей будет использован парсер на мультипарадигменном языке программирования Python. Предполагаемое количество собранных таким образом статей составит более 10 тыс. единиц.

Предварительная обработка данных

Обработка данных – чрезвычайно важный этап интеллектуального анализа текста для построения тематического профиля. На этом этапе происходит удаление несущественных и вносящих помехи данных и преобразование данных к удобному для анализа виду.

Также на данном этапе осуществляется удаление из каждой статьи уникальных (специфических) признаков, свидетельствующих о её принадлежности к какому-либо источнику. Внимательное изучение получаемых текстов статей показал, что редакции каждого СМИ устанавливают собственные правила оформления статей. Эти правила касаются способа оформления источников данных, ссылок на упоминания имён авторов статей, специфических для данного СМИ условных обозначений и т.д.

После исключения уникальной (специфической) информации данные из различных источников объединяются в единый корпус и подвергаются дальнейшей обработке.

Токенизация

Токенизация – это своего рода предварительная обработка; идентификация базовых единиц, подлежащих обработке. Без этих четко разделенных базовых единиц, невозможно провести какой-

либо анализ или генерацию. Идентификация единиц, которые не нуждаются в дальнейшей декомпозиции для последующей обработки, является чрезвычайно важной. Ошибки, сделанные на этом этапе, вызовут больше ошибок на более поздних этапах обработки текста. Именно токены являются теми первичными элементами, которые непосредственно участвуют в процессе анализа.

Два основных признака токена:

лингвистическая значимость;

методологическая полезность.

Для токенизации могут использовать различные алгоритмы, например Pattern.

Лемматизация

После токенизации и удаления ненужных токенов, являющихся знаками препинания, документы будут представлены от набора неких символов к документам, представленным в виде списка слов. Дальнейшие наши шаги будут направлены на уменьшение длинны этого списка, т. е. на снижение общего количества токенов. Цель таких шагов - снижение вычислительной сложности анализа данных.

Для компьютера различные формы одного и того же слова являются совершенно разными словами. Существует два способа приведения различных словоформ к одной лексеме: стемминг и лемматизация.

Для решения задач построения тематического профиля целесообразнее использовать лемматизацию, поскольку получаемые в результате этого процесса леммы интерпретировать легче, чем усечённые основы слов (стемминг), значение которых не всегда легко восстановить.

Лемматизация – это процесс приведения словоформы к лемме – её нормальной (словарной) форме. В русском языке нормальная форма имени существительного имеет именительный падеж и единственное число, для прилагательных добавляется требование мужского рода, а глаголы, деепричастия и причастия в нормальной форме должны стоять в инфинитиве.

Удаление стоп-слов

Дальнейшие усилия по уменьшению количества токенов связаны с удалением так называемых стоп-слов. Эти слова, сами по себе почти не неся полезного смысла, тем не менее необходимы для нормального восприятия текста. Чаще всего к разряду стоп-слов относятся служебные части речи - предлоги, союзы, частицы. Будучи широко распространёнными в любых текстах, они мало могут сказать о его специфике, а следовательно, и о теме.

В качестве базы для списка стоп-слов предполагается использовать русские стоп-слова из программы NLTK (платформа для создания программ Python для работы с данными естественного языка). Однако такой список нельзя считать достаточно полным, он включает (по состоянию на 01.01.2023) в себя 301 слово, покрывая лишь самые основные случаи (*это, который, такой, некоторый, другой, тот и др.*) [3].

Тематическое моделирование

Построение тематической модели может рассматриваться как задача одновременной кластеризации документов и слов по одному и тому же множеству кластеров, называемых темами. В терминах кластерного анализа тема — это результат бикластеризации, то есть одновременно кластеризации и слов, и документов по их семантической близости. Обычно выполняется нечёткая кластеризация, то есть документ может принадлежать нескольким темам в различной степени. Таким образом, сжатое семантическое описание слова или документа представляет собой вероятностное распределение на множестве тем. Процесс нахождения этих распределений и называется тематическим моделированием.

Что касается конкретных методов тематического моделирования, то в данном исследовании будет использован метод латентного размещения Дирихле (latent Dirichlet allocation, LDA). Созданный в 2003 г. [4], сейчас LDA, безусловно, лидирует среди других вероятностных тематических моделей.

На выходе после обучения модели LDA получаются векторы, показывающие, как распределены темы в каждом документе, и распределения, показывающие, какие слова более вероятны в тех или иных темах. Таким образом, из результатов LDA легко получить для каждого документа список встречающихся в нём тем, а для каждой темы - список характерных для неё слов, т.е. фактически описание темы.

Для тематического моделирования предполагается использовать программы Gensim и Mallet.

Однако прежде, чем приступать к тематическому моделированию, необходимо произвести предварительную обработку данных, специфичную для данного этапа, а именно удаление редко встречающихся токенов. Удалённые токены представляют собой слова с ошибками, цифры,

гиперссылки, английские слова (в том числе написанные транслитом), имена собственные и просто редкие слова.

Определение оптимального количества тем

Определение оптимального числа тем – важная подзадача в тематическом моделировании, поскольку её решение существенно влияет на осмысленность получаемого набора тем. Занижение числа тем приводит к чрезмерно общим результатам. Завышение приводит к невозможности разумной интерпретации. Оптимальное число тем зависит от числа документов в анализируемом корпусе: в малых корпусах оптимальным является, как правило, меньшее число тем. Однако не существует однозначного метода определения оптимального количества тем, и часто это количество определяется «на глазок», исходя из личного мнения исследователя.

Тем не менее можно говорить о том, что самым распространённым способом является расчёт перплексии. Данная мера основана на значении правдоподобия, именно она использовалась в оригинальном исследовании [4], где впервые был представлен метод LDA.

Популярность тем у читателей

Зная количество комментариев к новостным статьям, мы можем определить самые резонансные темы, подсчитав, статьи какой тематики комментируют чаще всего, а какой - реже.

Мы можем получить показатель комментируемости темы путём сложения рассчитанных для каждого документа произведений вероятности присутствия темы в документе на количество комментариев в данном документе. Полученное таким образом значение само по себе ничего не значит, важно лишь то, как оно различается от темы к теме. Поэтому для наглядности мы можем без последствий принять наибольшее значение комментируемости за 100 %, а для остальных тем рассчитать долю, которую они составляют от этих 100 %.

Однако, построение тематической модели является некорректно поставленной оптимизационной задачей, имеющей бесконечно много решений. Согласно теории регуляризации А.Н. Тихонова, решение такой задачи возможно доопределить и сделать устойчивым. Для этого к оптимизационному критерию добавляется *регуляризатор* – дополнительный критерий, учитывающий специфические особенности данных или предметной области. Можно добавить регуляризатор, сильно улучшив один критерий качества, затем добавить второй и улучшить модель по другому критерию, и так несколько раз.

Постановка оптимизационной задачи максимума апостериорной вероятности (англ. Maximum a posteriori, MAP) позволяет интерпретировать логарифм априорного распределения как вероятностный регуляризатор, отделить его от конкретной модели и использовать в других моделях. Аддитивность регуляризаторов приводит к модульной технологии тематического моделирования, которая реализована в проекте BigARTM [5].

BigARTM — это библиотека с открытым кодом, основанная на теории ARTM. Она имеет расширяемый встроенный набор регуляризаторов и метрик качества, реализует онлайновый и оффлайновый многопоточный пакетный EM-алгоритм, обеспечивающий высокую эффективность обработки больших коллекций на одном компьютере.

Аддитивная регуляризация тематических моделей (англ. Additive regularization of topic models, ARTM) – многокритериальный подход к построению вероятностных тематических моделей коллекций текстовых документов. Охватывает наиболее известные тематические модели PLSA, LDA и многие байесовские модели. Является альтернативой байесовскому обучению тематических моделей.

Вероятностный латентный семантический анализ (англ. Probabilistic Latent Semantic Analysis, PLSA) - вероятностная тематическая модель представления текста на естественном языке. Модель называется латентной, так как предполагает введение скрытого (латентного) параметра - темы. Применяется в задаче тематического моделирования.

Latent Dirichlet Allocation (LDA) – популярный алгоритм моделирования тем реализованные в том числе в пакете Gensim. Основная задача алгоритмов ТМ, заключается в том, чтобы полученные темы были хорошего качество, понятными, самозначимыми и разделенными.

При решении прикладных задач комбинирование готовых регуляризаторов позволяет строить модели с заданными свойствами без дополнительных математических выкладок и программирования. Создание такой технологии в рамках байесовского подхода едва ли возможно. В отличие от байесовского обучения, ARTM стандартизирует реализацию тематических моделей в виде модульной расширяемой библиотеки регуляризаторов. Процедуры хранения и передачи данных, распараллеливания EM-алгоритма, оценивания качества моделей являются общими для широкого класса моделей и их композиций [6].

Заключение. Таким образом, исследование множества вероятностных тематических моделей показал высокий потенциал разнообразных вариантов их применения в практической

(прикладной) плоскости, в том числе при разработке проектных решений в различных областях науки. При этом тематические модели могут выступать универсальным базисом с гибкой структурой, адаптивной к конкретному проекту, либо задаче в различных областях (СМИ, социологические, маркетинговые и иные исследования). В качестве примера по формированию такого рода базисной структуры предложены основные этапы, необходимые и достаточные, для построения тематического профиля национальных интернет-СМИ.

Исследования по данной теме будут продолжены, в том числе в области переноса алгоритмов некоторых методов на мультипарадигменный язык программирования Python.

UDC 004.3.049.77

USING THEMATIC MODELING METHODS IN THE DEVELOPMENT OF PROJECT SOLUTIONS

Novikov A.A.[1],

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

Sterjanov M.V. – candidate of technical sciences

Annotation. Practical experience in the application of numerous topic modeling algorithms convinces us that topic models have a huge "reserve of solutions", including the development of design solutions in various fields of science. In the study of topic modeling methods in the development of design solutions, the possibility of transferring the algorithms of some methods to the Python programming language is also investigated. The study proposes an approximate sequence of steps necessary and sufficient for preliminary data processing on the example of building a thematic profile of national online media.

Keywords. Data mining, topic modeling, topic model, probabilistic topic models, embedding, tokenization.

Список использованных источников:

1. Воронцов К. В. Вероятностное тематическое моделирование: теория, модели, алгоритмы и проект BigARTM. 2020.

2. Scott Deerwester, Susan T. Dumais, George W. Furnas, Thomas K. Landauer, Richard Harshman. Indexing by Latent Semantic Analysis // JASIS (41) 1990 pp. 391-407.

3. Thomas Hofmann. Probilistic latent semantic analysis // Proceedings of the Twenty-Second Annual International SIGIR Conference on Research and Development in Information Retrieval. 1999.

4. Агеев М.С., Добров Б.В., Лукашевич Н. В. Автоматическая рубрикация текстов: методы и проблемы // Учёные записки Казанского государственного университета. Серия Физикоматематические науки. 2008. Т. 150. № 4. С. 25 40.

5. Айсина Р. М. Обзор средств визуализации тематических моделей коллекций текстовых документов // Машинное обучение и анализ данных (http://jmlda.ojy). 2015. Т. 1. № 11.С. 1584 1618.

6. Воронцов К.В., Потапенко А.А. Регуляризация вероятностных тематических моделей для повышения интерпретируемости и определения числа тем // Компьютерная лингвистика и интеллектуальные технологии: По материалам ежегодной Международной конференции «Диалог» (Бекасово. 4 8 июня 2014 г.). Вып. 13 (20). М: Изд-во РГГУ. 2014. С. 676 687.

УДК 621.391

ТОНОВОЕ ОТОБРАЖЕНИЕ НА ОСНОВЕ УПЛОТНЕНИЯ ГИСТОГРАММЫ И ЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ

Робачевский А.Д.[1], студент гр. 160801

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Цветков В.Ю. – д.т.н., профессор

Аннотация. Приведены результаты анализа чувствительности показателей качества тонового отображения к выбору алгоритмов сжатия динамического диапазона, их параметров и типов инфракрасных изображений. Показано, что интервальные показатели имеют большую чувствительность к условиям тонового отображения в сравнении с глобальными показателями.

Ключевые слова. Уменьшение динамического диапазона изображений, повышение качества воспроизведения изображений, инфракрасные изображения, выравнивание гистограммы, управление формой гистограммы.

Введение

Сжатие динамического диапазона с минимальными потерями информации о деталях инфракрасных (ИК) изображений является актуальной задачей для множества приложений. Благодаря достаточно высокому качеству формируемых ИК-изображений и относительной простоте реализации широкое распространение получил алгоритм тонового отображения на основе выравнивания гистограммы (Histogram Equalization, HE) [1]. Данный алгоритм, как и основанные на нем более сложные блочные алгоритмы адаптивного выравнивания гистограммы, не позволяют изменять параметры преобразования, кроме как через форму интегральной функции распределения яркостей. Такая функция строится по гистограмме яркости пикселей исходного ИК-изображения, но может быть видоизменена для коррекции формы гистограммы преобразованного ИК-изображения. Установление связи между необходимым преобразованием для конкретного ИК-изображения с широким динамическим диапазоном и формой интегральной функции распределения является сложной задачей. На практике часто используется заранее известная интегральная функция распределения какого-нибудь эталонного изображения. Такой подход не всегда обеспечивает приемлемое качество тонового отображения.

Целью работы является повышение качества управляемого сжатия динамического диапазона ИК-изображений при сохранении относительно низкой вычислительной сложности преобразования.

Алгоритм управляемого тонового отображения ИК-изображений

Для обеспечения возможности изменения степени сжатия динамического диапазона ИК-изображений предлагается алгоритм TCLHC (Thresholding, Compaction and Linear Histogram Compression) управляемого тонового отображения на основе пороговой обрезки, уплотнения и линейного сжатия гистограммы. Алгоритм TCLHC состоит из следующих шагов.

1) Формирование гистограммы яркости исходного ИК-изображения с широким динамическим диапазоном.

2) Определение порога TR повторяемости значений пикселей по форме гистограммы яркости исходного ИК-изображения (в ручном режиме на основе визуального контроля) с учетом того, что значения редко встречающихся пикселей будут заменены ближайшими часто встречающимися значениями.

3) Пороговая обрезка гистограммы. Значения пикселей исходного ИК-изображения, соответствующие значениям гистограммы, меньшим значения порога повторяемости, заменяются ближайшими значениями пикселей исходного ИК-изображения, соответствующими значениям гистограммы, равным или большим порога повторяемости. В результате формируется загрубленное ИК-изображение, на гистограмме которого увеличивается количество нулевых элементов.

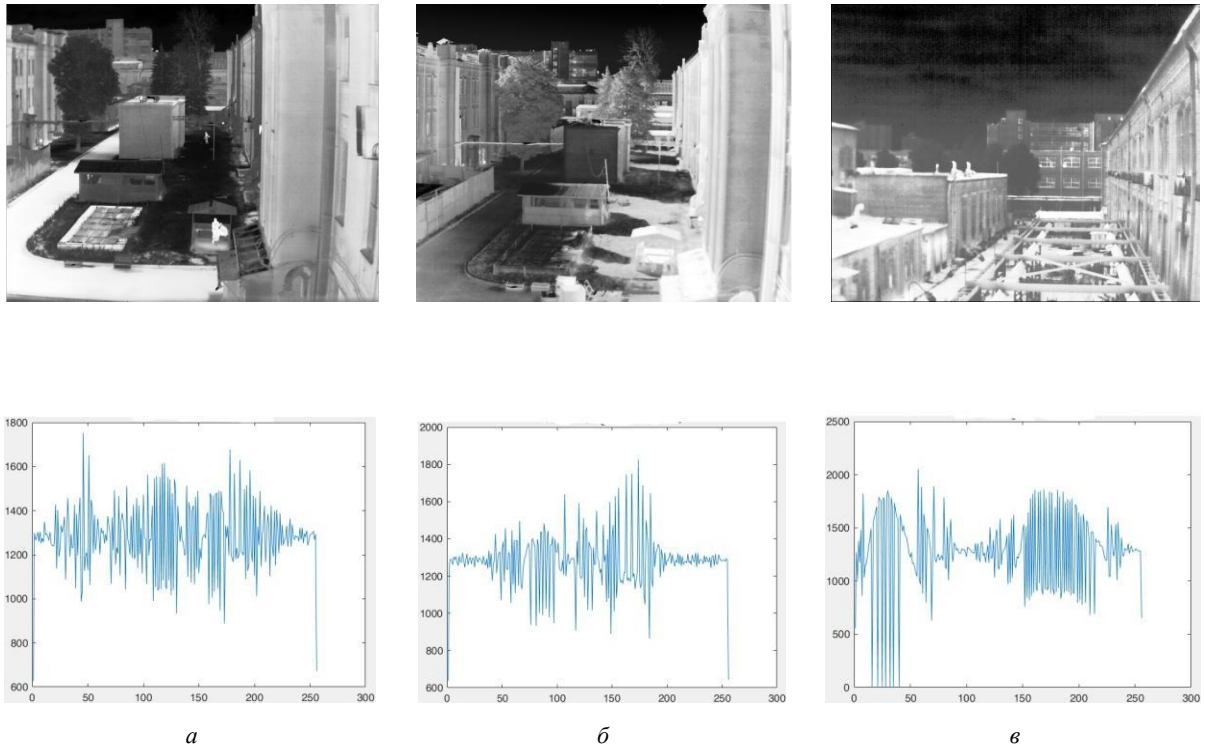
4) Поиск нулей и уплотнение гистограммы загрубленного ИК-изображения. Слева направо осуществляется поиск нулевых значений гистограммы загрубленного ИК-изображения. Если

нулевое значение гистограммы найдено, то все значения гистограммы справа от нулевого сдвигаются на одно значение влево. В результате гистограмма уплотняется за счет исключения нулевых элементов и формируется уплотненное ИК-изображение с более узким динамическим диапазоном по сравнению с исходным ИК-изображением.

5) Линейное преобразование уплотненного ИК-изображения к требуемому динамическому диапазону. Это может быть сжатие или растяжение гистограммы яркостей в зависимости от соотношения требуемой ширины динамического диапазона результирующего ИК-изображения и максимального значения яркости, уплотненного ИК-изображения.

Оценка качества тонового отображения

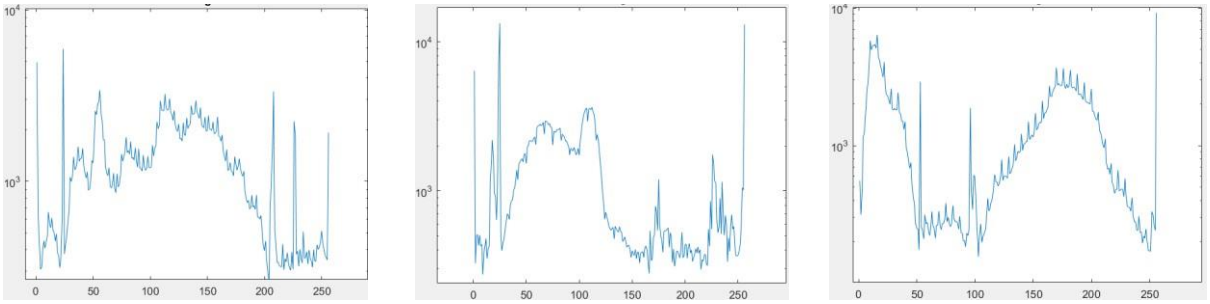
Для оценки качества тонового отображения использованы три тестовых ИК-изображения (ИК-1 – ИК-3) с динамическим диапазоном 65536 уровней яркости. На рисунке 1 приведены результаты тонового отображения этих трех тестовых изображений в динамический диапазон 256 уровней яркости с помощью алгоритма HE.



а *б* *в*

Рисунок 1 - ИК-изображения и их гистограмма после выравнивания гистограммы с помощью алгоритма HE: а – ИК-1; б – ИК-2; в – ИК-3

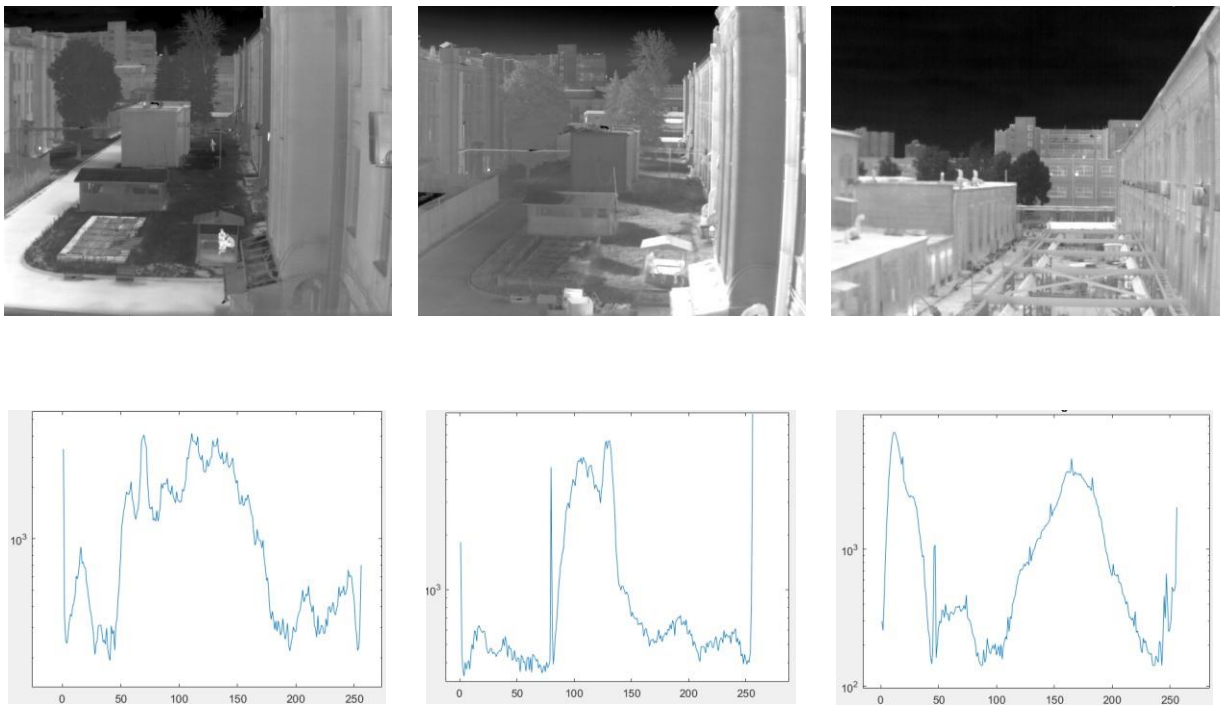
На рисунках 2 и 3 приведены результаты тонового отображения тестовых изображений ИК-1 – ИК-3 в динамический диапазон 256 уровней яркости с помощью предложенного алгоритма TCLHC при нескольких значениях порога повторяемости.



а *б* *в*

Рис. 2. ИК-изображения и их гистограмма после выравнивания гистограммы с помощью алгоритма TCLHC при значении порога повторяемости 50: а – ИК-1; б – ИК-2; в – ИК-3

В таблицах 1 и 2 приведены показатели качества преобразованных тестовых изображений с помощью алгоритмов HE и TCLHC.



а *б* *в*

Рисунок 3 - ИК-изображения и их гистограмма после выравнивания гистограммы с помощью алгоритма TCLHC при значении порога повторяемости 25: а – ИК-1; б – ИК-2; в – ИК-3

Для оценки качества тонового отображения использованы глобальные показатели, позволяющие оценить контраст (стандартное отклонение D_{ST} и средний градиент G_A), энтропия E_1, количество локальных экстремумов N_{LE}, статистическая естественность N_S [2], структурная точность F_S [3], качество тональной карты I_{TMQ} [4], а также предложенные в [5] интервальные и интервально-блочные показатели, позволяющие оценить: потенциальную различающую способность P_D на выбранном интервале динамического диапазона преобразованного изображения; потери E_D E_D различения соседних пикселей на выбранном интервале динамического диапазона преобразованного изображения, обусловленные тоновым отображением; величину E_{MS} нелинейных искажений сжатия динамического диапазона на выбранном интервале динамического диапазона преобразованного изображения относительно линейно преобразованного изображения; равномерность U_H использования динамического диапазона на выбранном интервале динамического диапазона преобразованного изображения относительно базового интервала; неоднозначность L_{DH} тонового отображения, обусловленную различиями передаточных

характеристик блоков в интервале динамического диапазона преобразованного изображения, соответствующего интервалу прореженного динамического диапазона исходного изображения; величину L_{DL} нелинейных искажений, связанных с неоднозначностью тонового отображения, в интервале динамического диапазона преобразованного изображения, соответствующего интервалу прореженного динамического диапазона исходного изображения.

Меньшие значения P_D и E_D свидетельствуют о более высокой различающей способности и меньших потерях различения соседних пикселей преобразованного изображения. Меньше значения E_{MS} говорят о приближении передаточных характеристик блоков (или всего изображения) к линейным. Близкие к единице значение U_H свидетельствуют о более равномерном распределении яркостей на выбранном интервале относительного базового интервала и близости тонового отображения к линейному при равновероятных значениях пикселей. Близость к единице значений L_{DH} говорит о меньшей неоднозначность тонового отображения. Меньшие значения L_{DL} свидетельствуют об уменьшении нелинейных искажений из-за неоднозначности тонового отображения. Значения интервальных показателей вычисляются для перекрывающихся левого (L), центрального (C), правого (R) интервалов гистограммы и всего динамического диапазона изображения (интервал T).

Табл. 1. Значения глобальных показателей качества ИК-изображений

Показатель	Значения глобальных показателей для алгоритмов											
	HE			TCLHC, TR = 50			TCLHC, TR = 25			TCLHC		
	ИК-1	ИК-2	ИК-3	ИК-1	ИК-2	ИК-3	ИК-1	ИК-2	ИК-3	ИК-1, TR=80	ИК-2, TR=60	ИК-3, TR=80
N_S	0,060	0,064	0,083	0,021	0,026	0,030	0,034	0,054	0,042	0,055	0,073	0,054
F_S	0,824	0,837	0,829	0,715	0,668	0,642	0,778	0,777	0,680	0,819	0,819	0,704
I_{IMQ}	0,782	0,787	0,791	0,736	0,724	0,717	0,760	0,767	0,733	0,779	0,785	0,745
D_{ST}	35,712	35,407	28,087	20,749	20,424	24,276	26,838	30,546	26,173	34,802	38,152	27,276
G_A	5,239	5,723	5,960	2,924	3,156	3,504	3,849	4,781	4,149	5,024	5,898	4,700
E_1	6,297	6,351	6,104	5,523	5,427	5,522	5,856	5,898	5,697	6,150	6,066	5,757
N_{LE}	34202	28360	43929	32521	24455	42001	33832	26516	42849	33438	26957	43146

Табл. 2. Значения интервальных показателей качества ИК-изображений

Показа-тель	Интер-вал	Значения интервальных показателей для алгоритмов											
		HE			TCLHC, TR = 50			TCLHC, TR = 25			TCLHC		
		ИК-1	ИК-2	ИК-3	ИК-1	ИК-2	ИК-3	ИК-1	ИК-2	ИК-3	ИК-1, TR=80	ИК-2, TR=60	ИК-3, TR=80
P_D	L	3,17	-0,27	-4,83	2,70	-1,71	-0,34	2,96	1,24	-0,10	2,43	0,43	0,36
E_D		23,89	8,52	-33,90	44,33	-78,48	-9,11	83,34	45,97	-42,04	37,55	55,08	-20,27
E_{MS}		19,91	24,95	22,77	20,09	20,32	28,94	22,84	21,46	29,69	23,39	21,56	28,04
U_H		0,99	0,99	0,99	0,55	0,27	0,81	0,72	1,16	1,21	0,78	1,27	1,32
L_{DH}		1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
L_{DL}		0,01	0,01	0,01	0,01	0,03	0,01	0,01	0,01	0,00	0,01	0,01	0,00

Показа-тель	Интер-вал	Значения интервальных показателей для алгоритмов											
		HE			TCLHC, TR = 50			TCLHC, TR = 25			TCLHC		
		ИК-1	ИК-2	ИК-3	ИК-1	ИК-2	ИК-3	ИК-1	ИК-2	ИК-3	ИК-1, TR=80	ИК-2, TR=60	ИК-3, TR=80
P_D	C	-5,85	-14,92	-0,66	-2,19	-4,53	-2,82	-4,18	-11,22	-1,40	-5,52	-14,16	-3,06
E_D		-41,33	-111,2	-10,31	-30,13	-133,5	-22,19	-81,44	-397,6	-87,20	-183,0	-585,7	-90,97
E_{MS}		4,31	8,95	6,63	8,25	6,58	2,18	6,97	10,64	2,99	5,14	7,11	3,60
U_H		1,01	1,01	1,01	2,44	3,34	1,72	1,65	1,28	0,78	1,14	1,01	0,74
L_{DH}		1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
L_{DL}		0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01
P_D	R	1,00	9,86	0,87	-1,28	6,32	2,18	-0,24	6,62	1,32	1,17	8,80	2,46
E_D		3,03	63,90	13,72	-24,71	175,5	23,56	-30,31	213,3	101,3	81,58	326,33	110,46
E_{MS}		0,57	1,11	0,73	1,16	0,91	0,56	0,99	1,09	0,71	0,84	1,23	0,75
U_H		1,00	1,00	1,00	0,28	0,33	0,36	0,49	0,40	1,34	0,97	0,70	1,37
L_{DH}		1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
L_{DL}		0,01	0,01	0,01	0,02	0,03	0,01	0,01	0,03	0,00	0,01	0,02	0,00
E_{MS}	T	10,58	9,45	10,31	9,91	7,45	13,69	10,63	12,85	13,03	9,57	12,11	12,76
L_{DH}		1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
L_{DL}		0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01

Список использованных источников:

1. Nithyananda C.R., Ramachandra A.C., Preethi // 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). – Chennai, 2016. – P. 2512–2517.

2. Mante V., Frazor R. A., Bonin V., Geisler W.S., Carandini M. // (2005) Independence of luminance and contrast in natural scenes and in the early visual system. Nat Neurosci, 8, 1690–1697.

3. Wang Z., Simoncelli E. P., Bovik A. C. // (2003) Multiscale structural similarity for image quality assessment. 37th Asilomar Conference on Signals, Systems & Computers. Pacific Grove, CA, USA, 2, 1398–1402.

4. Yeganeh H., Wang Z. // (2013) Objective Quality Assessment of Tone-Mapped Images. IEEE Transactions on Image Processing, 22(2), 657–667.

5. ПГУ

UDC 621.391

THRESHOLDING, COMPACTION AND LINEAR HISTOGRAM COMPRESSION

Robachevskiy A.D., student gr. 160801

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

V.Yu.Tsviatkou – Doctor of Engineering, professor

Annotation. The results of sensitivity analysis of tone mapping quality indicators to the choice of dynamic range compression algorithms, their parameters and types of infrared images are presented. It is shown that interval indicators are more sensitive to tone mapping conditions in comparison with global indicators.

Keywords. Image dynamic range reduction, image reproduction enhancement, infrared images, histogram equalization, histogram shape control.

УДК 621.391

АЛГОРИТМ МАТЕМАТИЧЕСКОЙ ОБРАБОТКИ РЯДА РАВНОТОЧНЫХ ИЗМЕРЕНИЙ

Устинович П.В. гр.263102

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ИКТ

Аннотация. В данной статье рассмотрена тема алгоритм математической обработки ряда равноточных измерений. Представлено поэтапное описание алгоритма. Приведены примеры применения алгоритма математической обработки ряда равноточных измерений.

Ключевые слова: математическая обработка, равноточные измерения, погрешность измерений.

Измерения – это сравнение значений определяемых параметров с эталонными при помощи специальных измерительных устройств и приборов. В маркшейдерской практике измерения играют первостепенную роль, на их основе выполняются все виды работ. Маркшейдерские измерения производятся как на земной поверхности, так и в подземных выработках. Результаты подвергаются математической обработке, которая должна улучшать их качество и ослаблять влияние погрешностей измерений.

Математическая обработка результатов представляет собой заключительный этап измерения, задачей которого является окончательное оценивание истинного значения измеренной величины, определение точности измерений и точности полученных оценок.

Целью обработки результатов измерений является установление значения измеряемой величины, и оценка погрешности полученного результата.

Задачи математической обработки результатов измерений возникают и могут решиться только при наличии избыточных измерений, выполненных сверх необходимого количества, что, с одной стороны обеспечивает контроль и надежность результатов, а с другой стороны, приводит к получению нескольких значений одной и той же величины, численно различающихся из-за влияния погрешностей измерений.

Математическая обработка результатов измерений выполняется для решения двух основных задач:

1) получения однозначных результатов, основанных на избыточной информации, наилучшим образом приближающихся к неизвестным истинным значениям измеряемых величин и их функций;

2) контроля качества и оценки точности измеренных величин и их функций.

Первая задача решается при помощи метода наименьших квадратов, который помимо нахождения оптимальных значений измеренных величин позволяет оценить их точность и качество выполненных измерений, т. е. решить вторую задачу математической обработки измерений.

По точности измеренные однородные значения подразделяются на равно- и неравноточные. Это подразделение основывается на анализе условий измерений, под которыми понимаются: объект измерений, внешняя среда, средства измерений, наблюдатель и метод измерений. Если условия измерения однородных величин были одинаковыми, то значения этих величин получаются равноточными. Практически же к равноточным относят значения, полученные при разлучающихся в некоторых пределах условиях измерений.

Равноточные измерения характеризуются одинаковой для всех результатов измерений средней квадратической ошибкой.

На рис. 1 представлен алгоритм формирования результата при прямых неравноточных многократных измерениях (на примере двух групп наблюдений). Поскольку совместная обработка результатов серий возможна при условии, что их значения однородны, что оценивается с использованием методов математической статистики. Определение «однородные» в статистике означает «являющиеся оценкой одного и того же параметра». Группы наблюдений при измерениях (серии) называются однородными, если состоят из значений, подчиняющихся одному и тому же закону распределения вероятности. В противном случае серии считаются неоднородными. Проверка однородности является обязательной при выборе способа совместной обработки результатов нескольких серий измерений. При такой проверке сравниваются между собой средние арифметические значения серии, дисперсии и рассчитывается доверительный интервал оценок среднеквадратичного отклонения.

Рисунок 1 – Алгоритм формирования результата при прямых неравноточных многократных измерениях (на примере двух групп наблюдений)

Пусть выполнен ряд многократных, независимых равноточных измерений одной величины, истинное значение X которой неизвестно. В результате измерений получены значения xi, свободные от систематических ошибок (это означает, что M(x)=X). Под математической обработкой ряда равноточных измерений, которая выполняется с использованием для оценивания основных параметров метода максимального правдоподобия, понимают:

1. определение наиболее надёжного значения измеряемой величины (наилучшей оценки неизвестного истинного значения X) — простой арифметической средины.
2. определение средней квадратической ошибки отдельного результата измерений по формуле Бесселя (оценка неизвестного параметра σx).
3. определение средней квадратической ошибки простой арифметической средины.
4. построение доверительного интервала, с заданной вероятностью β накрывающего неизвестное истинное значение X.

УДК 621.391

РАЗРАБОТКА WEB-СТРАНИЦЫ ПРОЕКТА «СОХРАНЯЯ ПАМЯТЬ О ПРОШЛОМ, СТРОИМ БУДУЩЕЕ!»

Шкред А.В. гр.260801

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ИКТ

Web-разработка сайтов и макетов сайтов заключает в себе HTML и CSS коды, а также скрипты событий на языке программирования JS. HTML и CSS являются неотъемлемой частью любой страницы. JS же используется реже, по причине его не столь существенной необходимости на сайте и нагрузке оперативной памяти устройства пользователя. HTML отвечает непосредственно за выведение информации на сайт, а также за структурирование самого сайта. CSS отвечает за определения различных свойств объектам и создание более дружелюбной среды для пользователя. JS необходим для диалога сайта с пользователем и реакцией на его действия на сайте. При разработке новой версии сайта следует учитывать то, что полное обновление всех элементов страницы может негативно отразиться на последующем дополнении и редактировании информации на сайте. По этой причине разработку новой страницы сайта следует рассматривать как обновление уже имеющихся конструкций текстовой и графической информации с созданием для нее новых форм и свойств. Новая версия сайта не является конечной версией, а представляет собой макет с уже заполненными структурами. Фотографии и текст были взяты из начальной версии сайта, либо взяты как пример с других страниц по схожей тематике (рис. 1).

Рисунок 1 – Внешний вид старой страницы (десктопная версия)

Слайдер – это специальный элемент веб-дизайна, представляющий собой блок определенной ширины, чаще всего в шапке веб-страницы. Главная его фишка в изменяющихся в ручном или автоматическом режиме элементах – картинок, текстов и ссылок. Именно интерактив слайдера помогает заинтересовать пользователя. Даже если некая содержащаяся информация будет ему не интересна, думаю, он не прочь будет "поиграться" с кнопочками и сменяющими одна одну картинками. Мной были подобраны фотографии из историографии данного проекта и собраны в слайдер, размещённый в шапке моей веб-страницы. На данный момент в нём находится 7 фото, но всегда можно что-то добавить либо убрать. Слайдер адаптивен под любой размер экрана: как десктопный, так и мобильный (рис. 2).

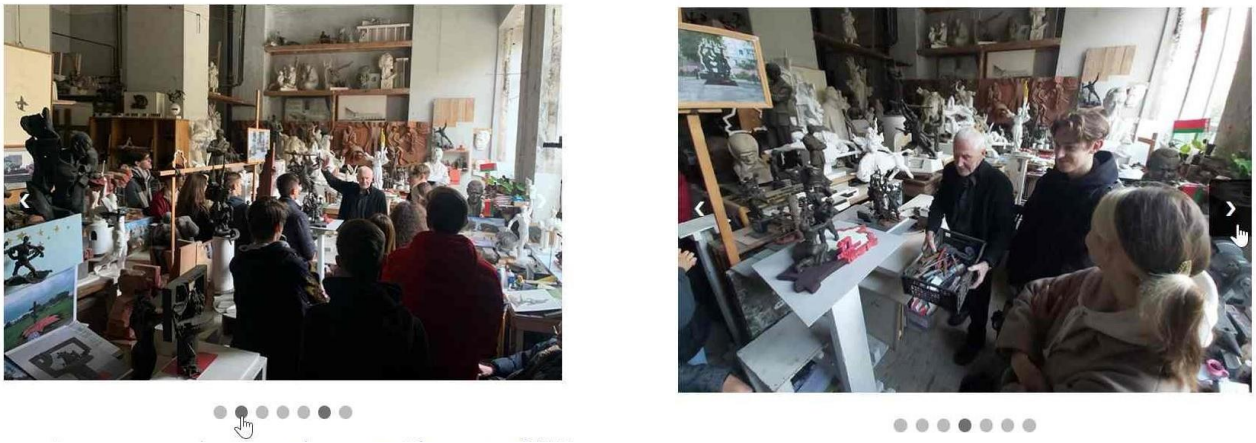


Рисунок 2 – Перелистывание фотографий производится за счёт стрелочек "назад" и "вперёд" либо точек внизу слайдера

СВЁРНУТЫЙ КОНТЕНТ

Многая информация может быть также неинтересна пользователю. Однако, есть лица, которым будет интересно её почитать. Следовательно, дабы не загружать сайт большим количеством текста, его можно свернуть. В моей работе есть два таких блока контента, они будут представлены ниже. Все блоки также адаптивны.

Блок представляет собой начало контента+многоточие и кнопку "Читать далее". После нажатия на неё многоточие пропадает, показывается всё содержание блока и надпись на кнопке меняется на "Скрыть". Также работает и в обратном порядке (рис. 3).

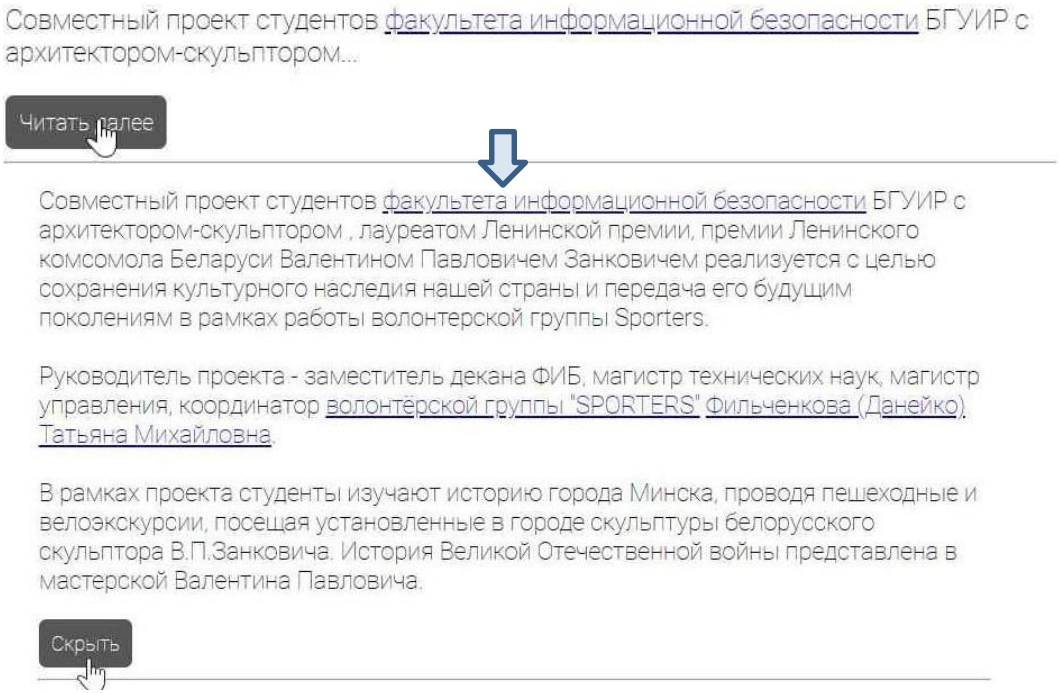


Рисунок 3 – Варианты реализации свёрнутого контента

ДОБАВЛЕНИЕ ВИЗУАЛЬНОГО КОНТЕНТА

Пользователь любит глазами. Простой текст его не очень-то интересует, а вот уже представление его вместе с изображениями как примерами либо общей тематики вероятнее заинтересуют его сильнее. Поэтому мной было принято решение показать некоторые из работ В.П.Занковича и оставить все ссылки на них.

Также я решила все ссылки на работы Валентина Павловича выделить в один блок для комфорта поиска и визуального восприятия (рис. 4).

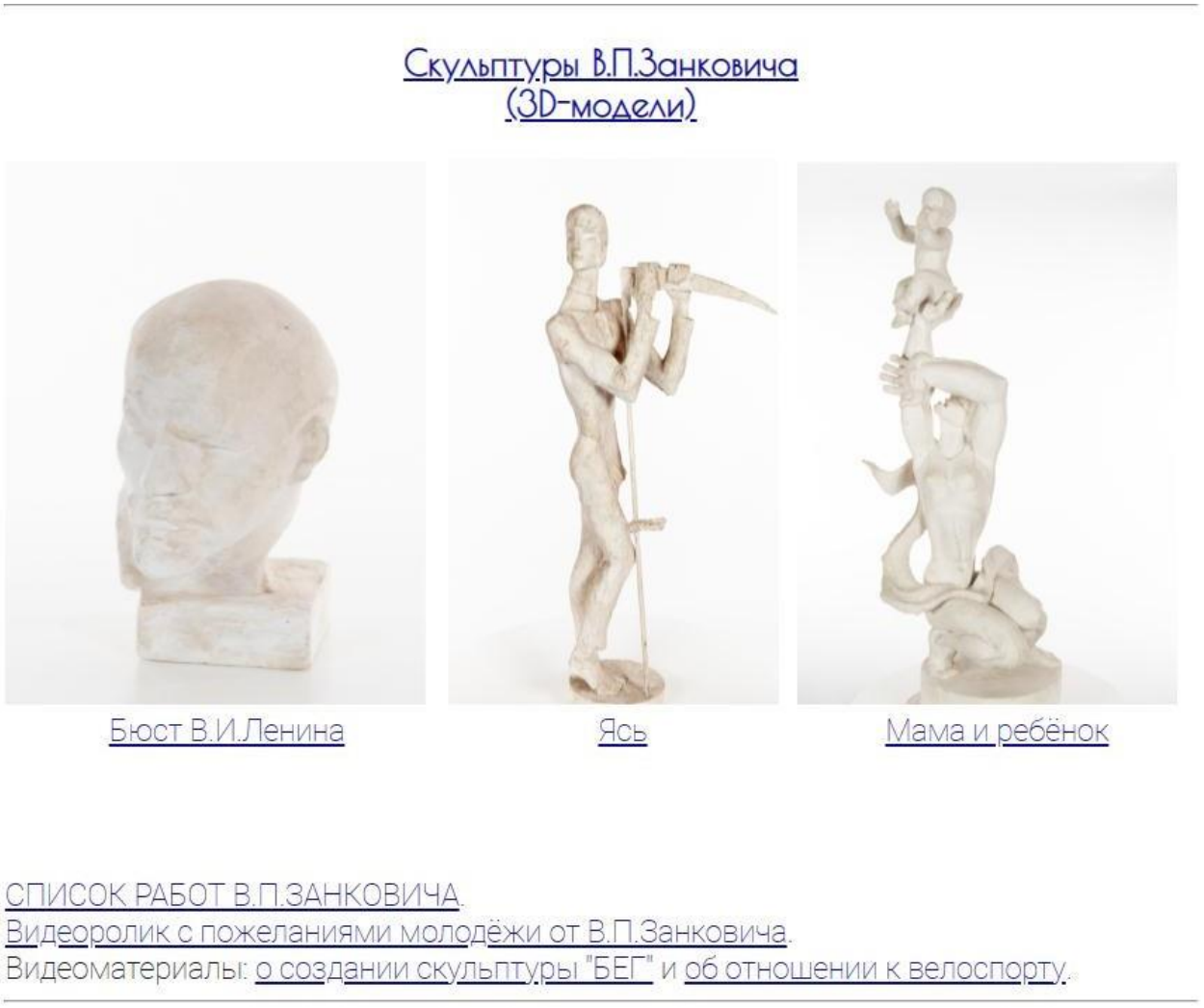


Рисунок 4 – Варианты реализации опции «добавление визуального контента»

ИНТЕРАКТИВНЫЙ КАЛЕНДАРЬ

Именно эту часть моей веб-страницы я считаю главным нововведением. Пришлось немного пораздумать над тем, во что же обернуть этот главный и самый массивный пласт текста на странице. На просторах интернета я нашла что-то подобное на то, что имею сейчас, и решила воплотить эту идею в жизнь. В итоге получился интерактивный календарь, на который можно кликать и он будет разворачиваться и сворачиваться. Только я решила немного сократить количество дат и выбрала самые на мой взгляд важные. Но, как и в случае со слайдером, всё недостающее всегда можно добавить.

Каждая из ячеек календаря представляет собой дату и начало текста, представленное полупрозрачным цветом. При наведении на верхнюю часть ячейки её верхняя граница и место по счёту изменяют цвет, появляется курсор pointer, следовательно, можно нажимать.

После нажатия начало текста пропадает и появляется полное описание события, связанное с этой датой. Также стрелочка в правом верхнем углу поменяет направление. Также всё работает и в обратном порядке.

Дивы с ячейками также адаптивны. На десктопной версии они стоят три в ряд, на мобильной одна под одной.

ЗАКЛЮЧЕНИЕ. Web-разработка – это трудоемкий процесс, который включает в себя как дизайн, так и программирование, но является одной из самых необходимых отраслей программирования в наше время. Требуются хорошие знания HTML, CSS и JS для реализации полного потенциала web-сайтов и умения адаптировать страницы под нужды всех пользователей. Создание новых версий сайтов и страниц, что по сути является их обновлением, также является очень затратным по времени и силам процессом, т.к. помимо создания новых форм и блоков информации также необходимо сохранить основную информацию сайта и его концепцию.

УДК 621.391

AN AUTOMATIC SEEDED REGION GROWING ALGORITHMBASED ON CONTOUR PROCESSING FOR GRAYSCALE IMAGES

Аль-Фурайджи О. Дж. М.[1], Аль-Мансури Х. А.[2], Цветков В. Ю.[3]

Университет Шатт Аль-Араб[1], г. Басра, Ирак

Белорусский государственный университет информатики и радиоэлектроники[2,3], г. Минск, Республика Беларусь

Аль-Фурайджи О. Дж. М. – к. т. н., доцент кафедра информатики

Цветков В.Ю. – д.т.н., профессор

Аннотация. In this paper, an automatic seeded region growing algorithm based on contour processing for grayscale images is proposed. In which, the grayscale image is first read. After that, the image is subjected to contour processing. The contour image is then segmented using simple SRG by assigning labels to each pixel in a specific segment. The segmented image is then compared to original input image to find the suitable seed in the segment depending on the average brightness of pixels forming the segment. Then these seeds are used again to generate segments using SRG algorithm. The proposed algorithm is shown that it is more accurate in finding number of segments than traditional segmentation algorithms.

Ключевые слова. Image segmentation, Seeded Region Growing, Contour processing, Region of interest, Pixel brightness.

Segmentation refers to the process of partitioning a digital image into multiple regions (sets of pixels). The goal of segmentation is to change the representation of an image into something that is more meaningful and easier to analyze. More precisely, image segmentation is the process of grouping an image into units or categories that are homogeneous with respect to one or more characteristics. The result of image segmentation is a set of segments that collectively cover the entire image, or a set of contours extracted from the image.

In 1997, C. Revol and M. Jourlin proposed an image segmentation algorithm with a homogeneity criterion based on an adequate tuning between spatial neighborhood and histogram neighborhood [1]. In 2001, I. Grinias and G. Tziritas introduced a semi-automatic method for moving object segmentation and tracking. The method is suitable when a few objects have to be tracked, while the camera moves and fixates on them [2].

In 2005, J.I. Kwak, [et al.] developed a rate-distortion (RD) based seeded region growing (SRG) algorithm for extracting an object such as breast tumors in ultrasound volumes which contain speckle noise and indistinct edges. In which, region growing proceeds in such a way that the growing cost is minimized which is represented as the combination of rate measuring the roughness of a region contour and distortion measuring the inhomogeneity of pixels in a region [3].

In 2007, O. Gomez, [et al.] suggested an automatic seeded region growing algorithm called ASRG-IB1 that performs the segmentation of color (RGB) and multispectral images. The seeds are automatically generated via histogram analysis; the histogram of each band is analyzed to obtain intervals of representative pixel values [4]. In 2009, M. del Fresno, [et al.] introduced a hybrid 3D image segmentation method which combines region growing and deformable models to obtain accurate and topologically preserving surface structures of anatomical objects of interest [5].

In 2010, J. -L. Rose, [et al.] proposed a new framework using a variational approach that is called Variational Region Growing (VRG). Variational approach is commonly used in image segmentation methods such as active contours or level sets, but is rather original in the context of region growing. It relies on an evolution equation derived from an energy minimization, that drives the evolving region towards the targeted solution [6]. In 2012, M. Mary Synthuja Jain Preetha, [et al.] presented an automatic seeded region growing algorithm for segmenting color images [7].

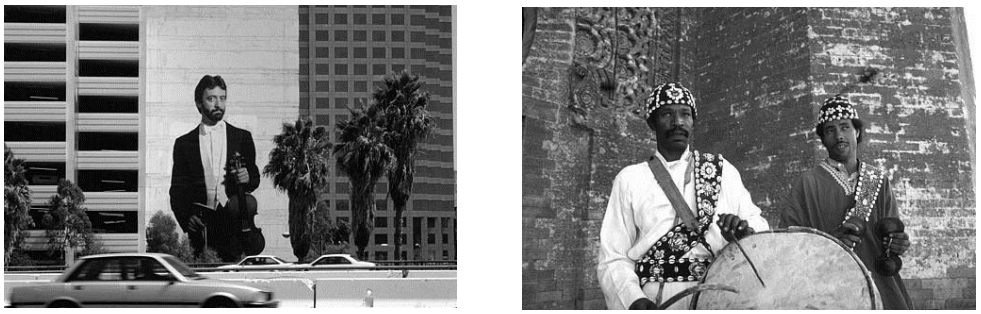
In 2015, M. Fan and T.C. M. Lee developed new modifications to SRG so that the constant grey value assumption is relaxed. Since the growing strategy of SRG does not impose any constraints or restrictions on the shapes of the growing regions, quite often SRG would produce very rough segmentation boundaries even the true boundaries were smooth. Also, they proposed a stabilized SRG that encourages smoother boundaries and prevents the so-called leakage problem [8]. In 2018, Y. Ge, [et al.] developed a modified region growing (MRG) algorithm, which is characterized by more efficient grow criterion, and was used to recognize discontinuities from the point cloud [9].

In 2020, M. F. Ramli and K. N. Tahar introduced a study to evaluate the height of oil palm tree based on crown diameter by using a multi-rotor Unmanned Aerial Vehicle (UAV). Digital Elevation Model (DEM) and orthophoto were generated by using Agisoft software, while oil palm tree crown diameter was

delineated by using seed generation with Quantum Geographic Information System (QGIS) and Seeded Region Growing (SRG) segmentation methods in the System for Automated Geoscientific Analysis (SAGA) [10].

In 2021, X. Hu, [et al.] proposed a region growing segmentation method based on microparticle color and grayscale information, in which the fuzzy contrast enhancement algorithm is used to enhance the color information of micro-particles and improve the discrimination between the micro-particles and background. In the HSV color space with stable color, the color information of micro-particles is extracted as seed points to eliminate the influence of light and reduce the interference of impurities to locate the distribution area of micro-particles accurately [11].

The aim of this paper is to automatically find the seeds which represent the center of segment, based on the average pixels' brightness of region of interest in the input image. These seeds then grow according to the simple SRG algorithm to find the segments of the input image. The grayscale image is first read, Fig. 1. After that, the image is subjected to contour processing, Fig. 2. The contour image is then segmented using simple SRG by assigning labels to each pixel in a specific segment, Fig. 3. The segmented image is then compared to original input image to find the suitable seed in the segment depending on the average brightness of pixels forming the segment, Fig.4. Then these seeds are used again to generate segments using SRG algorithm, Fig. 5. The proposed SRG algorithm described in the flowchart shown in Fig. 6, and the proposed algorithm is depicted visually as shown in Fig. 7. The resulted seeds and their pixel values are given in Table 1.



a) b)

Figure 1 – Test input grayscale images

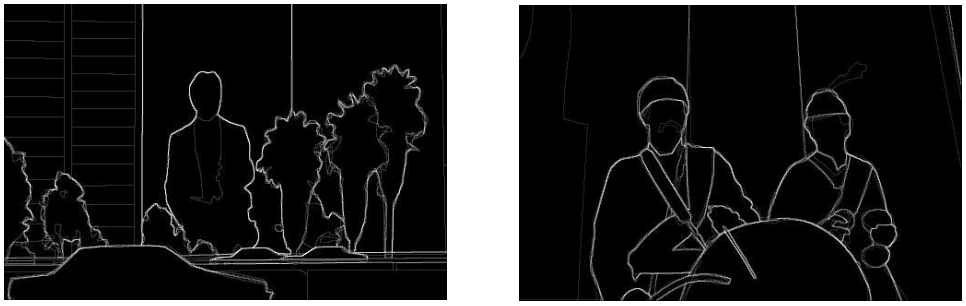


Figure 2 – Contour images

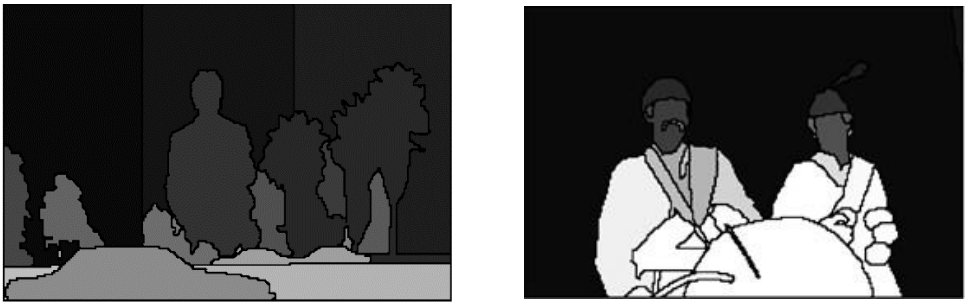


Figure 3 – Resulted labeled segmented images

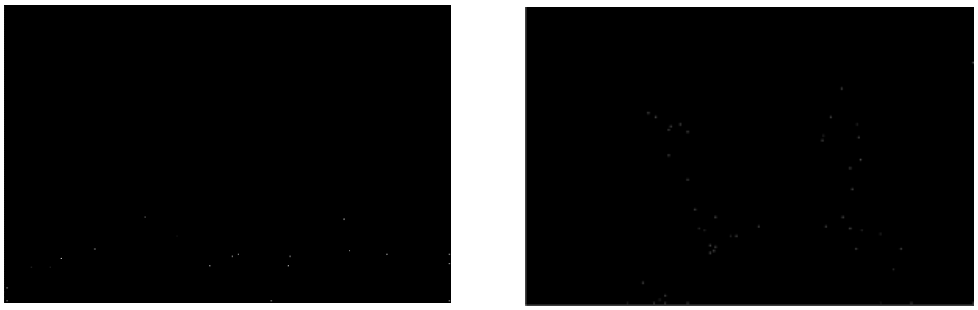


Figure 4 – Resulted seeds based on the average brightness of pixels in the segment

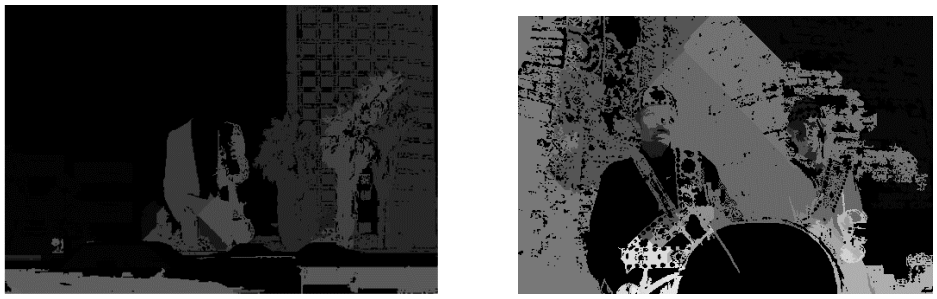


Figure 5 – Generated segments from seeds

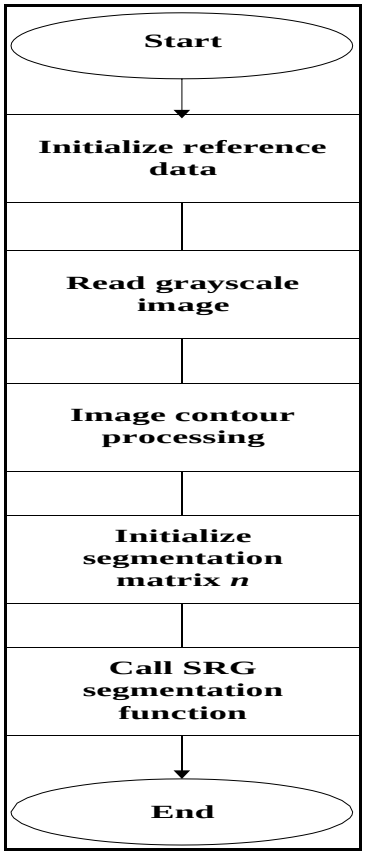


Figure 6 – The proposed SRG algorithm flowchart

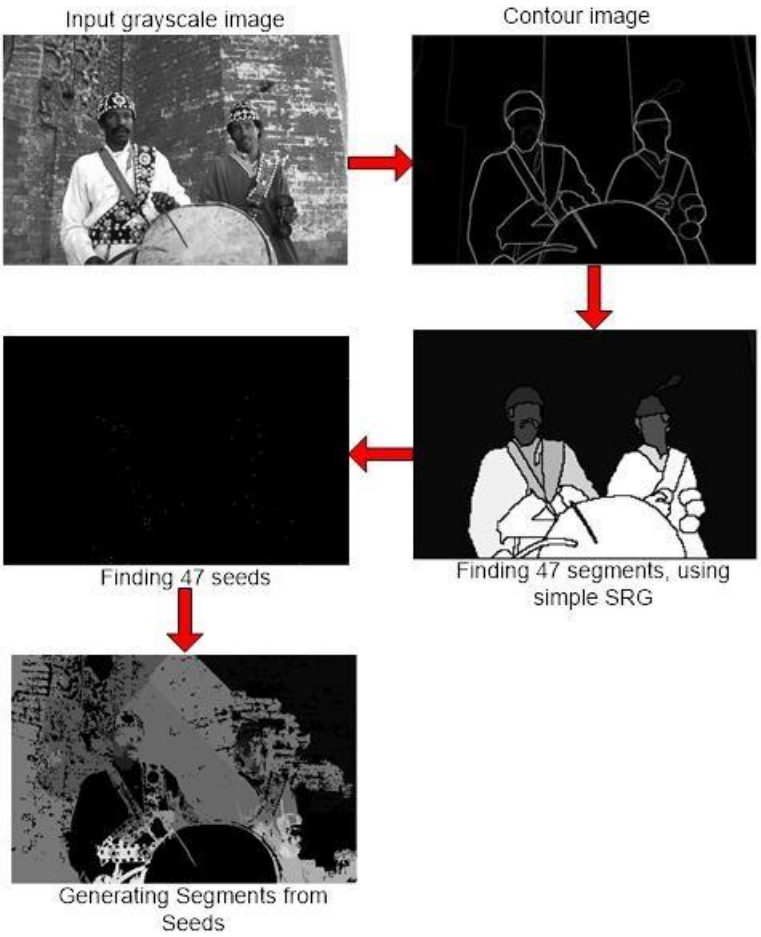


Figure 7 – The proposed SRG algorithm visual description

Table 1 – Resulted coordinates of seeds and their pixel values, for test image Fig. 1(b).

Segment number	Average pixel value in the segment	Rows	Columns
1	76	319	479
2	252	62	479
3	81	90	339
4	47	116	132
5	137	120	327
6	71	161	154
7	16	120	140
8	93	175	348
9	20	128	355
10	34	140	319
11	48	128	166
12	48	130	156

Segment number	Average pixel value in the segment	Rows	Columns
13	7	136	174
14	21	134	154
15	41	142	357
16	85	145	318
17	145	219	182
18	16	241	192
19	11	239	186
20	100	187	174
21	247	237	250
22	37	197	350
23	169	166	359
24	190	319	110
25	45	227	340
26	60	237	322
27	75	319	413
28	43	247	220
29	255	227	204
30	44	241	360
31	25	245	380
32	69	297	126
33	68	261	354
34	171	259	204
35	195	319	380
36	20	239	348
37	69	261	402
38	26	257	198
39	37	247	226
40	70	265	198
41	32	263	202
42	29	283	394
43	66	315	144
44	208	311	150
45	38	319	150
46	155	319	174

Segment number	Average pixel value in the segment	Rows	Columns
47	39	319	138

References:

1. A new minimum variance region growing algorithm for image segmentation / C. Revol, M. Jourlin // Pattern Recognition Letters, 1997. – P. 249-258.

2. A semi-automatic seeded region growing algorithm for video object localization and tracking / I. Grinias, G. Tziritas // Signal Processing: Image Communication, 2001. – P. 977-986.

3. RD-Based seeded region growing for extraction of breast tumor in an ultrasound volume / J.I. Kwak, [et al.] // Computational Intelligence and Security, 2005. – P. 799-808.

4. Image segmentation using automatic seeded region growing and instance-based learning / O. Gomez, [et al.] // Progress in Pattern Recognition, Image Analysis and Applications, 2007. – P. 192-201.

5. A combined region growing and deformable model method for extraction of closed surfaces in 3D CT and MRI scans / M. del Fresno, [et al.] // Computerized Medical Imaging and Graphics, 2009. – P. 369-376.

6. Unifying variational approach and region growing segmentation / J. -L. Rose, [et al.] // European Signal Processing Conference, Aalborg, Denmark, 2010. – P. 1781-1785.

7. Image segmentation using seeded region growing / M. Mary Synthuja Jain Preetha, [et al.] // International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Nagercoil, India, 2012. – P. 576-583.

8. Variants of seeded region growing / M. Fan, T.C.M. Lee // IET Image Processing, 2015. – P. 478-485.

9. Automated measurements of discontinuity geometric properties from a 3D-point cloud based on a modified region growing algorithm / Y. Ge, [et al.] // Engineering Geology, 2018. – P. 44-54.

10. Homogeneous tree height derivation from tree crown delineation using Seeded Region Growing (SRG) segmentation / M. F. Ramli and K. N. Tahar // Geo-spatial Information Science, 2020. – P. 195-208.

11. Research on the Region-Growing and segmentation technology of micro-particle microscopic images based on color features / X. Hu, [et al.] // Symmetry, 2021. – P. 1-17.

UDC 004.62

TEXTURE FEATURE EXTRACTION METHOD BASED ON GRAYSCALE RECOGNITION

Chen J.K., gr.167011, master

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

Tsviatkou V.Yu . – Doctor of Sciences

Аннотация. The quality of feature extraction has a great impact on the accuracy and efficiency of image recognition. Traditional image texture feature extraction consumes a long time and the efficiency is low. Therefore, a new method based on gray image is proposed in this paper. The texture feature image is collected, and then the gray processing is carried out, so the image texture feature extraction based on gray recognition is realized. Through a large number of experiments, the results shows that the new method has high speed and efficiency.

Ключевые слова. Grayscale recognition; texture features; feature extraction.

Currently, there are very many kinds of image features, and image texture features are one of the most basic ones. In image recognition technology applications, technicians can efficiently recognize images based on their texture differences. At present, image texture recognition techniques are widely used in industrial and agricultural production, etc [1]. The purpose of image texture recognition is to extract the texture features of different images. The texture features of images are very complex, and the traditional texture feature extraction methods are slow and have low extraction efficiency. Grayscale recognition is a special feature extraction technique that can greatly improve the extraction efficiency of image textures. Therefore, this paper designs a grayscale recognition based image texture feature extraction method.

The captured color image pixels are composed of 3 color components: red, green and blue. In order to reduce the complexity of the image to be processed, the acquired color image needs to be grayed out to reduce the difficulty of image processing and shorten the recognition processing time. In this paper, the grayscale transformation method is used to grayscale the image to be processed and convert it into grayscale image digital information to reduce the storage space occupied by the original image. Although the grayscale processed image reduces the difficulty of feature extraction, there is still a pixel point transformation problem. Therefore, this paper designs a grayscale co-occurrence matrix to increase the effectiveness of texture feature extraction by further judging the position relationship between pixel points. From the relationship between image pixels, it is known that there is a joint distribution factor between adjacent pixels, which can be used to determine the spatial relationship between pixels, and the quality of grayscale processing of the image can be further ensured by judging the information difference between pixels through the design of a symbiotic matrix [2].

Before the image texture feature extraction is implemented, the image needs to be binarized and edge detected. The values of the pixel points in the image are uniformly set to a fixed data format, and the binarization segmentation is performed using the thresholding method to ensure that the threshold value is within the pixel target range at this point. While retaining the original features of the image, the texture features of the image are initially extracted in order to further reduce the image complexity.

In order to verify the extraction effect of the image texture feature extraction method based on grayscale recognition, it is compared with the traditional image texture feature recognition method. The simulation experiments were conducted by Matlab 2020a software using a computer with Intel(R) Core(TM) i7-7200U@2.50 GHz CPU and 20 GB memory, and the specific experimental steps are as follows.

400 raw photos of chip images captured by industrial cameras were randomly selected for texture feature extraction test. The pixel size of the raw images was uniformly adjusted to 200×200 and normalized, and the normalized data were subsequently used as the data set. The home-made color images of the chip are selected as the data set, and uniform standard experimental parameters are set. To ensure the test images match the actual extracted information to the maximum extent, information processing is performed on the acquired images. All images are divided into grid blocks of the same pixels, and a nearest neighbor classifier is used to verify the validity of the evaluated color texture images. The experiments were cross-validated using the leave-one-out method, i.e., all the sample images were used as the training set except for one sample left as the test set image. After repeating the experiment 5 times, the average value is taken as the final result. In this experiment, three types of images are selected as the original images, the first type is the color image of the building surface cracks taken by ourselves, the second type is the image on the randomly selected color chip data set, and the third type is the image in the standard data set Colored Bordatz. The extraction results of the three types of images are compared below, and the results are shown in figure 1, figure 2, and figure 3.

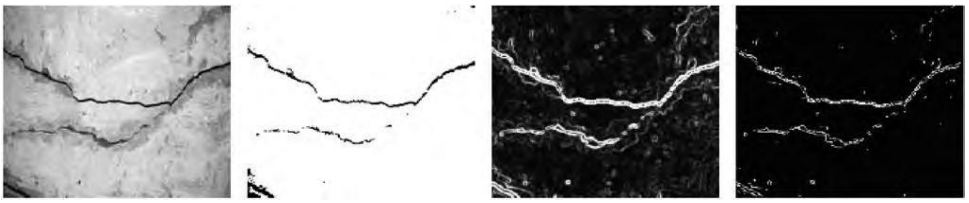


Figure 1 – Extraction results of the first type of image

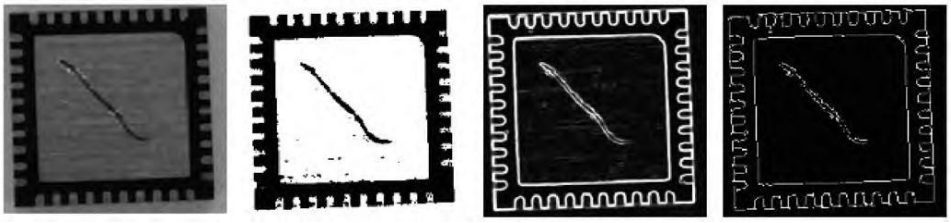


Figure 2 – Extraction results of the second type of image

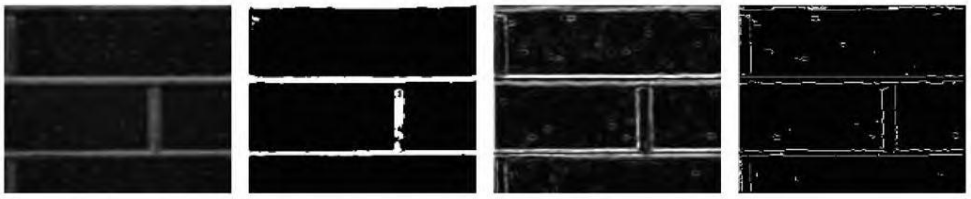


Figure 3 – Extraction results of the third type of image

Tests were performed on the standard color dataset Colored Bordatz, which contains a large amount of color and texture content. It consists of 1792 samples of size 160×160 pixels, divided into a standard data-set consisting of 112 texture classes (16 samples drawn from each class). A total of 112 image samples containing different texture classes are selected for the experiment, and 10 images to be tested are extracted for detection. If the detection length value is higher than 0.1, it is proved to meet the subsequent testing requirements. The size detection results of serial numbers 1 to 10 are 0.565, 0.366, 0.264, 0.367, 0.547, 0.632, 0.469, 0.355, 0.415 and 0.326, respectively, which are all higher than 0.1 and prove that the selected images meet the requirements of the testing experiment and the texture features are extracted reasonably.

The experiments were performed on three color images with grayscale transformation and binarization, respectively. For extraction convenience, the technicians performed edge detection on the images and feature extraction. The experimental results show that the grayscale based recognition method helps to extract the features of the images to be detected.

Список использованных источников:

1. A multi-scale partitioned Uniform LBP-based image texture feature extraction method / C. Gen [et al.] // Journal of Chengdu Normal University, 2020. – P. 98-106.

2. Image texture feature extraction based on grayscale co-occurrence matrix Feature Extraction / L. Guangyu [et al.] // Science and Technology Wind ,2021. – P. 61-64.

UDC 004.62

CODEC FOR TWO-DIMENSIONAL HAMMING CODE ON FPGA

Chen Y.M., gr.167011, master

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

Tsviatkou V.Y. – Dr. Tech. Sc.

Annotation. This work demonstrates a high-performance FPGA implementation using VHDL. The implementation includes multiple error detection and correction algorithms of Hamming product code variants, and includes selectable features such as hybrid automatic repeat request and parallel coding.

Keywords. FPGA, error correcting code, hamming code, product code.

In digital communication systems, errors can occur during data transmission due to noise, interference, or other factors. Error correcting codes are used to detect and correct these errors, ensuring the accuracy and reliability of digital communication. One popular error correcting code is the Hamming code, developed by Richard Hamming in the 1950s.

Hamming code works by adding extra parity bits to the original data bits. This creates a unique pattern of 1s and 0s that can detect and correct errors that may occur during transmission. The parity bits are added in a way that creates a unique pattern for each possible combination of single-bit errors that might occur during transmission. When the receiver receives the code, it checks the parity bits and compares them to the expected pattern. If there is an error, it can use the unique pattern to determine which bit has been flipped and correct the error.

The 2D Hamming code, also known as the Hamming product code, is an extension of the original Hamming code that is used for error detection and correction in two-dimensional arrays of data. This code adds extra parity bits to each row and column of a two-dimensional array, allowing it to detect and correct errors that may occur in both the horizontal and vertical directions. The 2D Hamming code is particularly useful in applications that require reliable transmission of data in two-dimensional formats, such as image or video data.

In this work, we implemented the Hamming product code on a Field Programmable Gate Array (FPGA). Our implementation is in a modular design, the overview of the whole system is shown as Figure 1. below.

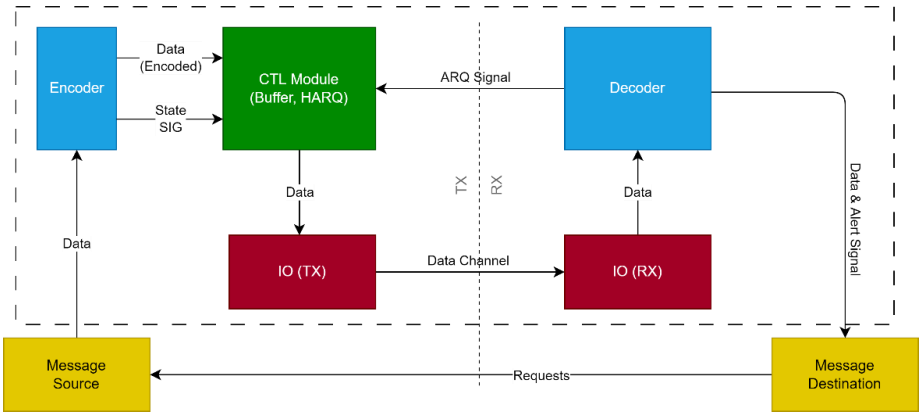


Figure 1 - System modules and structure block diagram

The decoder module plays an adapter of different algorithm, for now, the implementation come with 3 different algorithms: BaoV3, SHPC, EHPC. The different decoder algorithm has different extra feature support shown in Table 1 below.

Table 1 - Algorithm unit performance and capability

Algorithm	Codeword	Error Correcting	HARQ
BaoV3	8 Bit	4 Bit	Support
SHPC	8 Bit	4 Bit	Optional
EHPC	7 Bit	3 Bit	Optional
Encoder	8 Bit	4 Bit	-
Encoder	7 Bit	3 Bit	-

The design of this system supports installation multiple parallel workers to accelerate the decoding process. Table 2 below shows the unit resource usage and a typical performance at Fmax, which is an estimated value from four types of FPGA typical working conditions: combination of 0℃ and 85℃ at 1100mV. The average speed is calculated from the total clock cycles and the typical Fmax.

Table 2 - Algorithm unit resource usage

Algorithm	Logic utilization (in ALMs)	Total registers	Fmax	Avg. Speed
BaoV3	278	120	95 MHz	13 MB/s
SHPC	882	224	45 MHz	6.1 MB/s
EHPC	753	215	60 MHz	8.1 MB/s
ENCODE	70	141	300 MHz	40 MB/s
ENCODE	68	135	350 MHz	47 MB/s

Reference:

1. Elias P. // In Transactions of the IRE Professional Group on Information Theory. 1954. Vol. 4. P. 29–37.
2. Lin. S., Costello D.J. Error Control Coding, 2nd edition. USA, 2004.
3. Bo F., Ampadu P. // 2008 IEEE International SOC Conference. 2008. P. 59–62.

UDC 004.62

HUMAN PHYSICAL ACTIVITY RECOGNITION ALGORITHM BASED ON SMARTPHONE DATA AND LONG SHORT TIME MEMORY NEURAL NETWORK

CHEN Z.Y., YANG Z.X., LI H.

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

BARYSKIEVIC I.A. – PhD in Digital signal processing algorithm, Image Compression

Annotation. The continuous advancement of smartphone sensors has brought more opportunities for the universal application of human motion recognition technology. Based on the data of the mobile phone's three-axis acceleration sensor, using combining a double-layer Long Short Time Memory (LSTM) and full connected layers allow us to improve human actions recognition accuracy, including walking, jogging, sitting, standing, and going up and down stairs. This is helpful for smart assistive technology. It is shown that physical activity classification accuracy is equal to 98.4 %.

Keywords. Mobile acceleration sensor, long short time memory, action recognition and classification accuracy

Traditional sensor devices are bulky and expensive. With the continuous development of smart phones in recent years, the acceleration sensors of mobile phones have also continued to improve. It has the obvious advantages of small size, high penetration rate and lower price, which provides a new idea for the application of intelligent assistance technology and so on. Recognition of human activities from sensor data is at the core of intelligent assistive technologies, such as smart home, rehabilitation, health support, skills assessment or industrial environments [1]. For example, the project of Inooka et al. predicts the energy consumption of users by recognizing their activities [2], and Mathie et al. judges whether users are safe or not by recognizing their actions [3]. This work is motivated by two requirements of activity recognition: improving recognition accuracy and reducing reliance on engineered features to address increasingly complex recognition problems.

Human Activity Recognition (HAR) is based on the assumption that specific body movements translate into characteristic sensor signal patterns, which can be sensed and classified using machine learning techniques. We use data collected from accelerometer sensors. Almost every modern smartphone has a three-axis accelerometer that measures acceleration in all three spatial dimensions.

We selected the data set from the Wireless Sensor Data Mining (WISDM) project, which collected 1,098,207 experimental data generated from 29 volunteers carrying smartphones to perform specified actions every 50 ms, and each piece of data consists of 6 parts: Username, specified action, timestamp and accelerometer values for x, y and z axis.

Before feeding the raw data into the network model, we need to perform preprocessing and feature generation operations on it. Due to the impact of environmental changes in the data collection process, the data from the mobile phone accelerometer inevitably has a lot of measurement noise. The main method to eliminate these noises is to filter the original data with a low-pass filter, which helps to improve the accuracy of model recognition. The reason why the low-pass filter can be used is based on the following two conditions: 1. The noise is mainly concentrated in the high-frequency band; 2. When the human body is moving, the accelerometer measurement value is only related to gravity and human body acceleration, both of which are of small magnitude.

As a low-pass filter with a maximum flat amplitude response, the Butterworth filter has been widely used in the field of communication and electronic measurement, and can be used as a filter for detecting signals. The first-order Butterworth filter has an attenuation rate of 6 dB per octave and 20 dB per decade. A second-order Butterworth filter has an attenuation rate of 12 dB per octave, a third-order Butterworth filter has an attenuation rate of 18 dB per octave, and so on. The Butterworth low-pass filter can be expressed as the square of the amplitude $|H(jw)|$ and the frequency w as formula (1):

$$|H(jw)|^2 = \frac{1}{1+\left(\frac{w}{w_c}\right)^{2n}} = \frac{1}{1+\varepsilon^2\left(\frac{w}{w_p}\right)^{2n}}, \quad (1)$$

where w_c - cutoff frequency, that is, the frequency at which the amplitude drops to -3db, w_p - passband edge frequency, ε - damping ratio.

We experimented with Butterworth filters of different orders and cut-off frequencies. The Butterworth filter with a third-order cut-off frequency of 4 performed best. The graphs before and after filtering the raw

data of 200 three-axis accelerometers with label of sitting in the dataset using a Butterworth filter with a third-order cutoff frequency of 4 are shown in Fig. 1 and Fig. 2. After filtering, the graph is visibly flattened.

Figure 1 - Three-axis accelerometer plot labeled as sitting before filtering using a third-order 4 Hz Butterworth filter

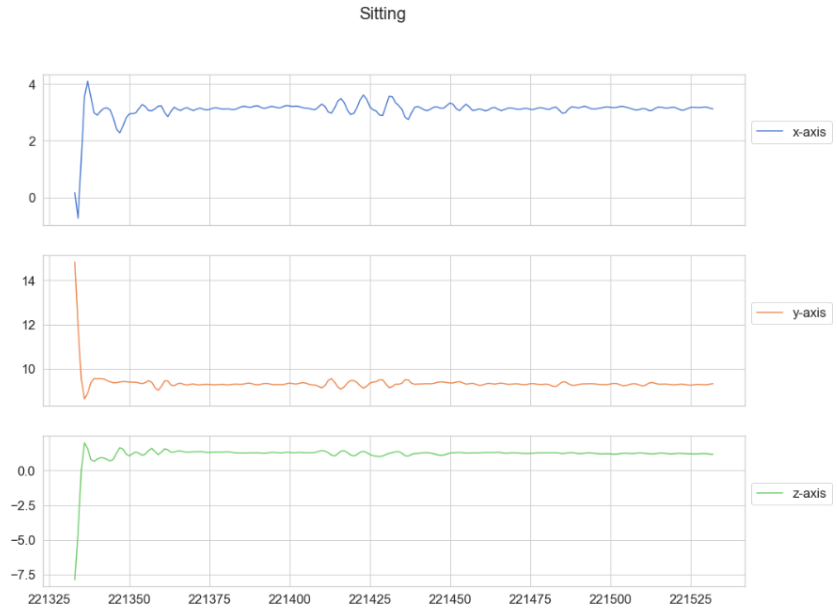


Figure 2 - Three-axis accelerometer plot labeled as sitting after filtering using a third-order 4 Hz Butterworth filter

We use a window of size 200 with an overlap of 90 % to divide the x, y and z axis accelerometer and label part in the original data, store them as acceleration data and label data respectively for preprocessing. We get 54901 windows and split both data into a training set (80 %) and a test set (20 %).

We trained a double layer LSTM neural network (implemented in TensorFlow) for HAR from accelerometer data with the purpose of providing an algorithm with higher recognition accuracy. The trained model will be exported/saved and added to the Android app. The network model consists of double layer

LSTM network layers and double fully connected layer (FCL), and predicts the corresponding human actions from the x, y and z axis acceleration count values from the data set. The proposed algorithm achieved 98,4 % accuracy and a loss of 0,2 on the test set.

Reference:

1. Tracking and sharing daily activity levels with unaugmented mobile phones. / I. Anderson. [et al.] // Mobile Networks and Applications, 2007. – P. 12.

2. Development of advanced portable device for daily physical assessment. / H. Inooka. [et al.] // SICE-ICASE International Joint Conference, 2006. – P 5878-5881.

3. Classification of basic daily movements using a triaxial acceler ometer. / M. Mathie. [et al.] // Medical & Biological Engineering and Computing, 2004. – P. 42

UDC 004 62

SYNTHESIS ALGORITHM OF MULTI-EXPOSURE IMAGES

J.X. FU, gr.167011, master

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

V.YU. Tsviatkou – PhD in Processing and image coding, infocommunications

Annotation. An effective way of synthesizing high dynamic range images is to shoot the same scene under a set of different exposure time conditions to obtain a set of multi-exposure images, and then extract, organize, and analysis to synthesize a luminance image that represents the original scene light distribution.

Keywords. High dynamic range image synthesis, Multiple exposure images.

The images taken by ordinary digital cameras are very different from the real scene, but it is difficult to generate images with high dynamic range by using ordinary digital cameras. Properly use the camera's exposure time to take multiple shots of the same scene, and each shot has a different exposure. By adjusting the ISO setting, a group of images with different exposures can be captured at different exposure times, and high dynamic range images can be effectively synthesized by using the full details of each image.

The details of the synthesized high dynamic range image are fully preserved, and the details of the high-exposure image and the low-exposure image can be well blended in one image. The visual effect of the synthesized image is enhanced, the recognition of the image is improved, and the details of the image can be better observed with the naked eye. This method of image synthesis can be widely used in digital video surveillance, remote sensing technology, real-time railway surveillance, medical imaging equipment, etc.

In a specific scene, the exposure area of a digital image is different, divided into three areas: overexposure, underexposure and normal exposure. Different exposure times will affect the shooting effect of the image. For an image with a long exposure time, the image shooting effect of the low-exposure area is better. Conversely, for an image with a short exposure time, the image shooting effect of the over-exposed image area is better. Taking advantage of this phenomenon, a series of exposure images can be obtained by changing the exposure time by shooting the same scene. Based on such a group of exposure images, the image information of different brightness regions can be extracted for each image, and finally a high dynamic range image is synthesized by using the detail information of this group of images [1].

To synthesize an HDR image, we divide the LDR image into the same region according to the exposure time, and then sum the normalized image pixels in the relevant range, however this is not straightforward to do because most cameras pass the sensor The process of collecting incident light by the circuit is nonlinear [2]. Such a nonlinear process of the camera is called the camera response function. By inverting it, the response function of the synthetic high dynamic range image can be obtained.

If the response function of the camera is known, then the nonlinear response function of the camera can be negated, and the response function of the camera is usually kept secret, and the camera manufacturer will not publish it [3]. Then in recent years, some algorithms have been developed to restore the response function of the camera. These algorithms use multiple images of the same scene with different exposure times to create the response function. Once the response function is restored and reconstructed through an image sequence, it can be Used to linearize other images taken with the same camera.

After calculating the camera's response function f and weight function w, the final irradiance I_p of the pixel p is obtained by calculating the weighted average of the pixel values in the relevant area of N consecutive frames [4]. As shown in Formula 1:

$$I_p = \sum_{a=1}^{N} \frac{f^{-1}(p_a)w(p_a)}{t_a} / \sum_{a=1}^{N} w(p_a) \quad (1),$$

In the formula, f^{-1} represents the inverse of the camera's response function, p_a is the pixel value in image a, and t_a is the exposure time of image a. If the HDR synthesis process based on the exposure value is accompanied by noise, then the synthesis process of the high dynamic range image may produce

a noisy image. In fact, the weight function is applied to the HDR synthesis process. In many cases, this is not unsatisfactory. And the resulting image will be rendered unusable. Therefore, in order to improve the quality of HDR, it is necessary to remove the noise in the synthesis process, further play the role of the weight function, and analyze the noise influence mode and principle of the high dynamic range image synthesis process, which is very important for the following work.

For the noise problem of HDR images, there are two types of methods to solve it: the first type of method is to perform noise processing after HDR image synthesis, treat HDR images as ordinary images, and use classic image denoising algorithms, such as mean filtering, etc. . The disadvantage of this type of method is that the details of the image are sacrificed, making the image blurred, and even this cannot completely remove the noise. Since the noise processing occurs after image synthesis, a large amount of image information has been lost, and the real information of the original image cannot be restored, and denoising will cause the image to further lose information. The second type of method is to perform noise reduction processing on the image group before HDR synthesis, and then obtain the noise-filtered image and then synthesize the HDR image. This method can greatly improve the quality of the image.

Reference:

1. High dynamic range image and color scale mapping operator / K. H. Yang, J. Ji, J. J.Guo // Acta Automatica Sinica, 2009. – P. 113-122.

2. Research on conversion algorithm between color and grayscale images / Q. X. Liu, T. F. Jiang // Journal of Wuhan University of Technology, 2003. – P. 344-346.

3. Abnormal tone rate forensics technology of blur operation in image forgery / B. Wang, L. L. Sun, X. W. Kong // Electronic Journal, 2006. – Vol. 34.

4. A robust camera response function calibration algorithm for HDR images / W. X. Zhang, B. F. Zhou // Journal of Computer Science, 2006. – P. 658-663.

UDC 004.62

HEART RATE ESTIMATION FROM PHOTOPLETHYSMOGRAM AND ACCLERATION SMARTPHONE DATA BASED ON CONVOLUTIONAL NEURALNETWORK AND LONG SHORT TIME MEMORY NETWORK

Qiu G.W., gr.167011, master

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

Baryskievic A.A. – PhD in Technical Sciences

Annotation. The wearable reflective photocapacitance plethysmograph (PPG) sensor can be integrated into the watch or strap to provide instantaneous heart rate (HRs), causing minimal inconvenience to users. However, the existence of motion artifacts (MAs) leads to inaccurate heart rate estimation. In order to solve this problem, I propose a new deep learning neural network to ensure accurate estimation of HR in high-intensity exercise.The average absolute error of the algorithm for all training data sets and test data sets is less than 1.5 bpm, including 1.09 bpm for training data sets and 1.46 bpm for test data sets.

Keywords. PPG, LSTM, Convolution,Concatenation,Heart rate and motion artifacts

Reflective photoplethysmography (PPG) sensor measures the intensity change of skin reflected light and provides PPG signal representing the change of arterial blood volume between systolic and diastolic phases of the heart cycle. The reason why the sensor is concerned is that it can be installed in a watch or wrist strap to measure and monitor instantaneous heart rate (HRs), minimizing the inconvenience to users. However, the sensor is sensitive to motion artifacts (MAs), which come from the pressure and motion exerted on the wrist of the PPG sensor. Motion artifacts will eventually lead to inaccurate heart rate estimation. A few years ago, Zhang and others shared the data set of acceleration and PPG signals measured simultaneously in [1] motion, which prompted people to study the use of acceleration signals to eliminate motion artifacts in PPG sensors. However, despite the efforts and progress of algorithms, these methods do not always provide accurate results.

In this paper, the purpose is to measure heart rate more accurately,so I propose a new deep neural network based on multi-class and non-uniform multi-label classification for human heart rate estimation. In the proposed algorithm, I consider two power spectra from the input layer of PPG and acceleration signals. In addition, I use the acceleration signal strength in the input layer. I assume that the acceleration signal strength can provide information about the recent HR changes: high intensity represents intense exercise, which may change HR. The proposed algorithm includes two convolution layers, two LSTM layers, one connection layer and three full connection layers (including one softmax layer). In the proposed algorithm, the power spectrum from PPG and acceleration signals is fed to two convolutions to provide MA cancellation in the PPG power spectrum. The output is flattened and connected to a fully connected layer, which is then connected to the acceleration signal strength. Then, the output is fed to two LSTM layers, and then to other full-connection layers including softmax.

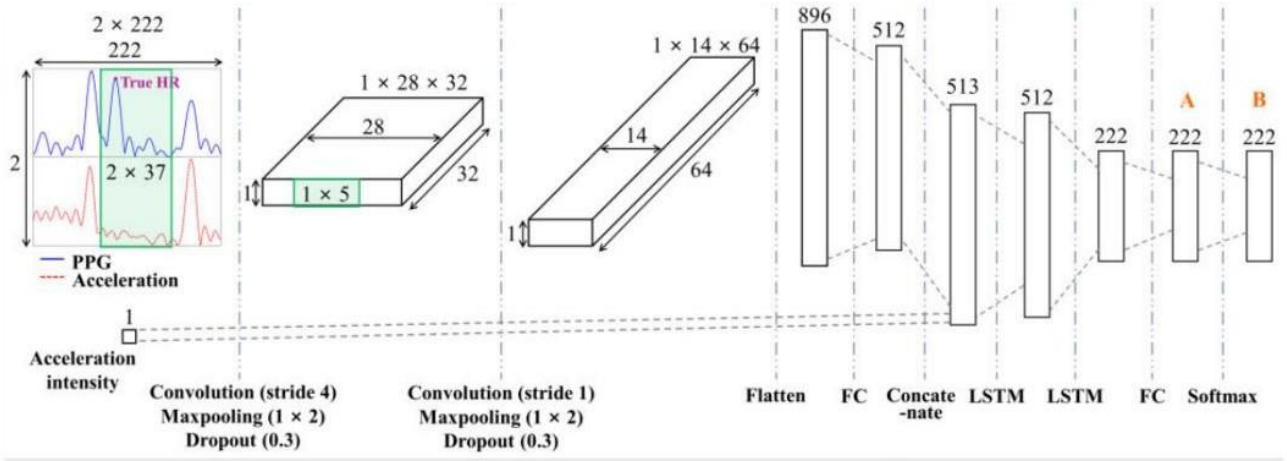


Figure 1. The architecture of the proposed algorithm; 2D convolution layer, 1D convolution layer, a full connection layer,a concatenation layer two LSTM layers and a full connection layer are structured in sequence

The LSTM layer uses minimum outliers to track HR tracking. In this algorithm, I also propose a new scheme to modify the real HR value to Gaussian distribution to evaluate the loss value. The performance of the proposed algorithm is evaluated by comparing with the results of [1] - [18] previously reported.

I used two data sets to evaluate the proposed HR estimation algorithm - the IEEE Signal Processing Cup (ISPC) 2015 data set (n=23) and the direct measurement data set obtained by the developed equipment (n=48). These two sets of data include multi-channel PPG signal and three-axis accelerometer signal, which are measured by the equipment on the wrist during high-intensity physical exercise. At the same time, ECG signals ire measured in the chest as real HR reference.

The data includes 12-minute three-channel PPG signal and 50-Hz sampling three-axis acceleration signal. The dataset is divided into two groups, BAMI-I and BAMI-II.

During every 4 minutes of running and walking, the subjects walked or ran with a treadmill stick in the last two minutes. I designed this link to reflect the heart rehabilitation exercise of patients with heart disease who have poor exercise ability. They usually walk or run with a treadmill stick. There are 17 males and 6 females, with an average age of 22.0 ± 1.7 years. The whole exercise process is also carried out on the treadmill. For these two data sets, the reference real heart rate was measured by ECG data recorded simultaneously by 24-h the ambulatory ECG monitor (SEER Light, GE Medical, Milwaukee, WI, USA).

In this study, I selected the ISPC data set (n=23) as the training data, because it includes various movements, such as waking up, running, resting, jumping, push up, shaking hands, stretching, pushing and boxing. I also added the own dataset BAMI-I (n=25) to the training data to increase the size of the training data, and used another dataset named BAMI-II (n=23) to test the training algorithm. For all data sets, the ecg-based HRs are calculated using an 8-second window, with a 2-second offset (6-second overlap) to obtain the HRs every 2 seconds. In the whole study, the same window length (8 seconds) and shift (2 seconds) are used to evaluate the performance of the proposed algorithm relative to the existing algorithm.

Figure 1 summarizes the architecture of the proposed algorithm. It consists of eight layers: two convolutional layers, two LSTM layers, one tandem layer and three full connection layers, including a softmax layer. More specifically, a 2D convolution layer, a one-dimensional convolution layer, a flat layer, a splice layer, a fully connected layer, two LSTM layers, and a fully connected layer folloid by a softmax.

For the input layer, the power spectrum from PPG signal and acceleration signal is divided into two (size 2×222): the top signal is from PPG (Ps (i)), and the bottom signal is from acceleration (Pa (i)). Note that the power spectrum is based on each 8-second window and then shifted for 2 seconds (6-second overlap). Input layer input to 32 2×37 cores, two-dimensional convolution with a step of 4, and then perform the nonlinear function leaky corrected linear unit (ReLU) and 1×2 max pooling, in steps of 2. The resulting size is $1 \times 28 \times 32$.The characteristic diagram of 32 shows the intermediate PPG power spectrum after MA cancellation.

Send characteristic map into 64 1×5-core, one-dimensional convolution with a side of 1, and then carry out leaky ReLU and 1 with a side of 2×2 max pooling, get other sizes of $1 \times 14 \times 64$, showing the PPG power spectrum of MA elimination. The resulting feature map is spread evenly to 896 nodes, which are fully connected to 512 nodes with leaking ReLU.

Subsequently, the acceleration intensity (I) is connected with 512 activations. I assume that the acceleration intensity represents how the current HR value will change in the near future. For example, high acceleration intensity means high intensity exercise, which may increase HR. 513 connected nodes are sent to two LSTM layers. These two LSTM layers act as HR tracking algorithms by considering the local HR tracking mode. Due to the existence of LSTM layer, even if the signal to noise ratio (SNR) of PPG signal is extremely low, the dominant frequency corresponding to HR will not deviate seriously in the continuous window. The first layer LSTM contains 512 nodes, each node has 6 time steps, and all nodes are connected to the second layer LSTM. Note that six time steps provide the best accuracy. The numerical analysis of the effect of time step will be introduced. The second LSTM layer also includes six time steps, each of which provides an output with a length of 222. Then, only the output from the last time step is fed to the full connection layer, which is connected to 222 nodes with leaking ReLU. In the frequency range of 0.6-3.3 Hz, the frequency resolution is 0.012 Hz, and the result of the final PPG power spectrum after MA cancellation is 222 activations. The activation is input to the softmax layer, which provides the final probability of the real HR value.

To avoid over-fitting, I applied dropout to two convolution layers and two LSTM layers. For convolution layer, the exit rate is set to 0.3. For LSTM layer, the drop rate of input linear transformation is 0.3, and the drop rate of loop state is 0.2.

List of used sources:

1. TROIKA: A general framework for heart rate monitoring using wrist-type photoplethysmographic signals during intensive physical exercise. / Z. Zhang, Z. Pi, B. Liu // IEEE Trans. Biomed. Eng. Feb. 2015. Vol. 62, no. 2, pp.

2. Photoplethysmography-based heart rate monitoring in physical activities via joint sparse spectrum reconstruction. / Z. Zhang // IEEE Trans. Biomed.Eng. Aug. 2015. Vol. 62, no. 8, pp.

3. A novel time-varying spectral filtering algorithm for reconstruction of motion artifact corrupted heart rate signals during intense physical activities using a iarable photoplethysmogram sensor./ S. Salehizadeh, D. Dao, J. Bolkhovsky, C. Cho, Y . Mendelson, K. Chon. // Sensors, 2016. Vol. 16, no. 1, p. 10.

UDC 004.62

RESEARCH ON GESTURE RECOGNITION BASED ON SUPPORT VECTOR MACHINE

Z.M. LIAO, gr.167011, master

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

Tsviatkou V.– PhD in Technical Sciences

Annotation. In response to the problems of low recognition accuracy and large computation of traditional neural network algorithms, a gesture recognition detection model is designed by using human skin color features and SVM model with gesture classification recognition as the target. The method adopts bilateral filtering and other graphical processing to smooth the edges of the palm, detect and binarize the skin color of the region, and filter the binarized image to smooth the edges. The skin color space is transferred from the RCB space to the YUV space under which the gesture region is separated from the background, and morphological processing techniques are introduced in terms of gesture integrity to effectively fill the black hole region and remove the white dot region in the gesture picture, and directly edge the gesture picture. After obtaining the standardized image, the feature values are obtained. The experimental results show that the method improves the accuracy of gesture recognition compared with traditional algorithms.

Keywords. Gesture recognition, OpenCV library, Support vector machines.

Introduction

The main purpose of gesture recognition is to make it easier for users to communicate with machines, especially for people with disabilities who are physically challenged. Early scholars mainly used sensors to collect gesture data, and although this method can obtain a high accuracy rate, the hardware is generally expensive. In recent years, the technology in the field of computer vision has developed rapidly, and scholars from various fields have started to flock to the embrace of computer vision. Research can be broadly divided into two categories, one is based on artificial feature extraction gesture recognition "", this method requires human to extract gesture features, and then processing, this method is susceptible to the impact of external factors, the background color changes will also bring a large error on the results; the other is based on deep learning gesture recognition research P, using deep convolution and recurrent neural network to achieve, the method uses four deep convolutional layers to automatically perform feature learning in the original data.

System Design

The first step of the gesture recognition system is to extract the contour lines of the hand after recording the gesture from the computer camera, and then program the image pre-processing process by using the OpenCV computer vision library to improve the API to denoise the image. The denoised gesture images are subjected to skin color detection and color space conversion, as well as binarization of the images, and then further processing such as erosion and expansion is done to finally extract the overall contour of the target object. The overall flow chart is shown in Figure 1.

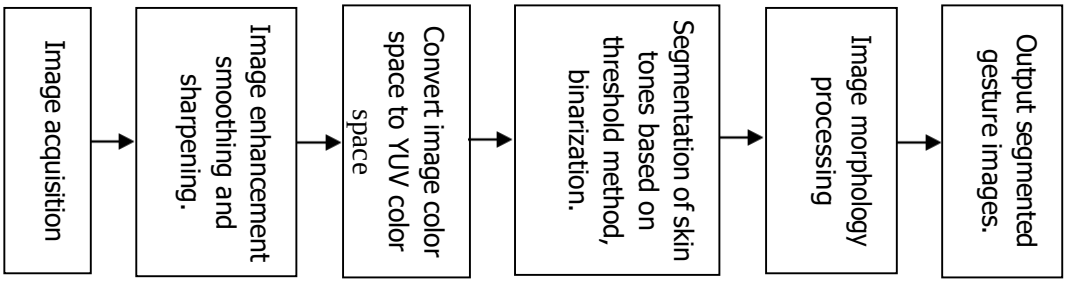


Figure 1. Flow chart of gesture segmentation

Get gestures and denoising

Due to the complex and diverse background environment of the captured images and the different performance of the capture devices, the raw gesture images captured directly from the computer camera

contain a lot of noise interference, and usually need to perform pre-processing operations to maintain the integrity of the raw image information.

The OpenCV environment is configured in the PyCharm compiler, and the gesture image is recorded in the main.py source file, and the video Capture function is called to capture the camera and obtain a live gesture image from the camera. The directly acquired gesture images are affected by environmental factors, such as light intensity, gray background, etc., and need further processing to ensure that the images have valid information and key feature points, as well as to remove features from the original images [1] that have an impact on the effect or are not relevant to our target information. The noise reduction of the original image is also called filtering, and the more commonly used filtering algorithms in current research are mean filter, Gaussian filter, bilateral filter and so on. Here, the bilateral filtering algorithm is chosen to perform noise reduction on the original image.

The essence of bilateral filtering is to combine the space of pixel fields and intervals with similar pixel values to achieve the purpose of edge preservation and denoising. The closer to the center point of the coordinates of the pixel point of the gray value accounted for a greater weight, to ensure that the boundary will not be blurred out, it is a simple, non-iterative and local algorithm. Bilateral filtering method achieves the purpose of edge pixel point keeping and noise reduction by setting the corresponding function internally.

Gesture Skin Tone Detection and Binarization

To achieve the ultimate gesture recognition, one of the more important steps is gesture segmentation, which is a prerequisite for gesture recognition. Here, we use the method of skin color detection to segment the gestures. There are many gesture features [2], among which hand color is an important feature and has strong robustness, which is an inherent feature of the hand.

OpenCV uses the cvColor() function to convert to RCB space, and then uses the split() function to obtain the RGB value of each pixel in the image, which is a two-dimensional matrix split into a three-dimensional matrix. If not, the mask is set to black. In addition to the RGB color space model, there is also a more common color space is YUV, OpenCV cvtColor function parameters to CV_YUV2BGR_I420, the color space will be converted to YUV space.

SVM model-based gesture recognition

For a limited number of learning samples, by continuously reducing the structure of the problem, the learning machine can obtain the best classification ability and finally can use statistical methods to successfully predict unknown outcomes. The generalized world can find the best function in the same kind of function set, but it is difficult to find other kinds of functions. The above problem can be better solved by choosing a partial set SVM of the eigenvectors of the sample group instead of the SVM of the sample group partition [3]. The SVC classification is trained as follows.

SVC function parameters are used.

'kernel':('linear', 'rbf'), 'C': [1, 3, 5, 7, 9, 11, 13, 15, 17, 19].

'gamma':[0.00001,0.0001,0.001,0.1,1,10,100,1000] which, C is the penalty term, the larger its value, the more it will directly affect the penalty value, the training samples will also get higher accuracy; kernel indicates different kernel function types; gamma indicates kernel function coefficients, the parameters are not fixed.

Comparative analysis of experimental results

The dataset and training set are imported into the SVM model and ANN for training and testing, and the accuracy of each round and the final average accuracy are obtained as shown in Table 1 and Table 2.

Table 1- Recognition accuracy of the training and data sets for SVM

Round/Accuracy	Round1	Round2	Round3	Round4	Round5	Round6	Round7	Round8	Round9	Round10
Training accuracy	0.987	0.984	0.991	0.987	0.997	0.987	0.987	0.987	0.987	0.987
Test accuracy	0.972	1.0	0.944	1.0	0.943	1.0	1.0	1.0	0.971	1.0

Table 2- Recognition accuracy of the training and data sets for ANN

Round/Accuracy	Round1	Round2	Round3	Round4	Round5	Round6	Round7	Round8	Round9	Round10
Training accuracy	0.997	0.997	0.997	0.991	0.997	0.997	0.997	0.771	0.997	1.0
Test accuracy	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.771	1.0	0.971

From Table 1 and Table 2, the recognition accuracy of SVM is 0.983 and 0.988 for training and test sets. 0.974 and 0.973 for training and test sets of ANN. SVM has higher recognition progress than ANN.

Conclusion

The experimental results show that the method has improved the accuracy of gesture recognition compared with the traditional algorithm. The gesture segmentation using the skin color recognition technique is susceptible to interference in complex real-world situations, and objects with similar skin color and shapes similar to the gestures are likely to appear in complex environments, which affects the accuracy rate to a certain extent. Only nine common hand gestures were analyzed, and there are limitations in the application scope. In the future research, the model can be further improved and extended to train more gestures to improve the adaptation range.

References

1. Haralick R M, Zhuang X, Lin C, et al. The digital morphological sampling theorem[J]. IEEE Transactions on Acoustics, Speech, and Signal Processing, 1989, 37(12): 2067-2090.

2. Saravanan G, Yamuna G, Nandhini S. Real time implementation of RGB to HSV/HSI/HSL and its reverse color space models[C]//2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2016: 0462-0466.

3. Yin X, Xie M. Hand gesture segmentation, recognition and application[C]//Proceedings 2001 IEEE International Symposium on Computational Intelligence in Robotics and Automation (Cat. No. 01EX515). IEEE, 2001: 438-443.

UDC 004.62

A REVIEW OF RESEARCH ON THE CONSTRUCTION AND DECODING OF MULTIPLE LDPC CODES

Liu F. Y., gr.167011, master

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

Salomatin S.B. – PhD in Technical Sciences

Annotation. With the continuous progress of communication technology, LDPC codes have become one of the key technologies in channel coding with their superior error correction performance and efficient decoding algorithms. Among them, multivariate LDPC codes perform better in high-order modulation and burst error channels, especially in short to medium code length conditions, but there are also shortcomings [3]. In order to better reconcile band utilization with BER and reduce decoding complexity, this paper discusses the construction and decoding of multivariate LDPC codes, focusing on their development history and research status.

Keywords. Channel coding, LDPC codes, multiple LDPC codes, construction, decoding

Around the 1960s, Gallagher started to construct multivariate LDPC codes using finite fields while proposing binary LDPC codes, but only from the idea of multivariate codes. It was not until 1998 that Mackay and Davey successfully demonstrated that LDPC codes constructed randomly based on finite fields outperformed binary LDPC codes, with good iterative decoding performance in both Gaussian white noise (AWGN) channels and binary erasure channels (BEC).

In fact, the construction methods of multivariate LDPC codes can be divided into two categories, namely randomized construction methods and structured construction methods. The PEG [1] algorithm is one of the commonly used randomized construction methods, where the connection between the check node and the variable node can be established step by step under a known degree distribution, and is used to build Tanner graphs of multivariate LDPC codes with large ring lengths. The approximate extra-ring message degree (ACE) algorithm is also one of the well-known computer-based stochastic construction algorithms, which increases the influence of overlapping rings on the decoding code by considering the rings as a way to improve the flow of extra messages during decoding iterations. The above random construction method requires a large number of computer search operations, and the constructed code words are irregular. Although the randomly constructed LDPC codes have good performance, the coding complexity is high.

Using algebraic theory, knowledge of finite geometry and the theory of matrix operations as the main structured construction method can be used to construct a class of multiplexed LDPC codes with regular structure of the check matrix. The structured construction method can be used to construct a class of multiple LDPC codes whose check matrices have a regular structure. By using sets of special structures, such as perfect difference sets, prime sets and good codes, a class of LDPC codes with regular structure can be constructed, which This effectively improves the performance of the waterfall region and brings some performance gains. Constructing multivariate LDPC codes can be combined with "good" codes to bring structural optimization, including generalized RS codes (GRS) [2] and Irregular Repeated Accumulation (IRA) codes. By combining other code The optimization of the checksum matrix of multivariate LDPC codes, in combination with other code features, allows for efficient encoding and easy to implement in hardware and further increase encoder throughput. Finite geometric knowledge is one of the most important ways to construct LDPC codes is to use the relationship between points and lines at the earliest. It is possible to obtain code word structures with a minimum distance and a better trap set, with a very low error leveling. The mask technique is used more often in matrix operation theory, and the mask technique is mainly The mask technique is mainly used by multiplying a check matrix of known structure with a certain mask matrix to change the original matrix structure, reducing the number of short loops while making the degree distribution better and the sparsity The mask technique is mainly used to change the structure of the original matrix by multiplying the known structure with a certain mask matrix, reducing the number of short loops while making the degree distribution better and sparser.

In addition, there are many measures of code word merit, including ring distribution, minimum distance, trap set, etc. Several of the structured construction methods mentioned above also start from these measures. One of them is for the existence of rings, especially short rings, which tend to bring about correlation between variable nodes, making the outer information return to its own node after only a few passes, which is not conducive to accurate decoding, such as the PEG algorithm which focuses on designing code words with larger ring lengths. The greater the minimum distance, the less it is affected by noise and the easier it is to decode, which is also one of the key factors affecting the decoding threshold and performance curve waterfall area. As multivariate LDPC codes are defined over a finite domain, their

check matrix consists of elements within the domain, so optimization of measures such as the ring can be achieved from the perspective of optimizing the set of coefficients.

In summary, for the problem of constructing multivariate LDPC codes, the core objectives are optimize the metrics that measure the structure of the code word so as to quickly and accurately construct a structured checksum matrix, which facilitates accurate decoding at the receiver. For the decoding of multivariate LDPC codes the core objective is to optimize the metrics for measuring the code word structure so that a well-structured check matrix can be constructed quickly and accurately to facilitate accurate decoding at the receiver. The decoding problem of multi-dimensional LDPC codes requires an analysis of the decoding rules of the two types of nodes to reduce the algorithm of the two types of nodes can be reduced without degrading the error correction performance.

List of used sources:

1. Low-complexity decoding for non-binary LDPC codes in high order fields. / A. Viola, F. Vernier // IEEE Transactions on Communications, 2010. – P. 1365–1375.

2. A simplified min-sum decoding algorithm for non-binary LDPC codes. / Wang C.L, Chen X // IEEE Transactions on Communications, 2013. – P. 23–32.

3. Generation and decoding of non-Binary LDPC codes using MSA decoding algorithm. / J.C. Babu, C.C. Reddy // Singapore : Micro-Electronics Springer, 2018.

UDC 004.62

NOISE AND INTERFERENCE IN TRANSMISSION OF SPEECH SIGNALS IN THE COROPORATE NETWORK

C. Uzor-Ejikeme, gr.167011, master

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Khatskevich O. A ., Ph.D, Assoc. Prof.

In signal processing, noise is a general term for unwanted (and, in general, unknown) modifications that a signal may suffer during capture, storage, transmission, processing, or conversion.
Sometimes, it can also mean signals that are random (unpredictable) and carry no useful information; even if they are not interfering with other signals or may have been introduced intentionally, as in comfort noise. Noise reduction, the recovery of the original signal from the noise-corrupted one, is a very common goal in the design of signal processing systems, especially filters. The mathematical limits for noise removal are set by information theory, namely the Nyquist–Shannon sampling theorem.
Noise may arise in signals of interest to various scientific and technical fields, often with specific features:
Noise is unwanted sound considered unpleasant, loud or disruptive to hearing. From a physics standpoint, noise is indistinguishable from desired sound, as both are vibrations through a medium, such as air or water. The difference arises when the brain receives and perceives a sound.
Acoustic noise is any sound in the acoustic domain, either deliberate (e.g., music or speech) or unintended. In contrast, noise in electronics may not be audible to the human ear and may require instruments for detection.

Background noise or ambient noise is any sound other than the sound being monitored (primary sound). Background noise is a form of noise pollution or interference. Background noise is an important concept in setting noise levels.
Background noises include environmental noises such as water waves, traffic noise, alarms, extraneous speech, bioacoustics noise from animals, and electrical noise from devices such as refrigerators, air conditioning, power supplies, and motors. The prevention or reduction of background noise is important in the field of active noise control. It is an important consideration with the use of ultrasound (e.g. for medical diagnosis or imaging), sonar, and sound reproduction.
Comfort noise (or comfort tone) is synthetic background noise used in radio and wireless communications to fill the artificial silence in a transmission resulting from voice activity detection or from the audio clarity of modern digital lines.

Some modern telephone systems (such as wireless and VoIP) use voice activity detection (VAD), a form of squelching where low volume levels are ignored by the transmitting device. In digital audio transmissions, this saves bandwidth of the communications channel by transmitting nothing when the source volume is under a certain threshold, leaving only louder sounds (such as the speaker's voice) to be sent. However, improvements in background noise reduction technologies can occasionally result in the complete removal of all noise. Although maximizing call quality is of primary importance, exhaustive removal of noise may not properly simulate the typical behaviour of terminals on the PSTN system.
The result of receiving total silence, especially for a prolonged period, has a number of unwanted effects on the listener, including the following:
- the listener may believe that the transmission has been lost, and therefore hang up prematurely;
- the speech may sound "choppy" (see noise gate) and difficult to understand;
- the sudden change in sound level can be jarring to the listener.

To counteract these effects, comfort noise is added, usually on the receiving end in wireless or VoIP systems, to fill in the silent portions of transmissions with artificial noise. The noise generated is at a low but audible volume level, and can vary based on the average volume level of received signals to minimize jarring transitions.

Electromagnetically induced acoustic noise (and vibration), electromagnetically excited acoustic noise, or more commonly called coil whine, is audible sound directly produced by materials vibrating under the excitation of electromagnetic forces. Some samples of this noise include the mains hum, hum of transformers, the whine of some rotating electric machines, or the thrill of fluorescent lamps. The hissing of high voltage transmission lines is because of corona discharge, not magnetism.
The phenomenon is additionally called audible magnetic noise, electromagnetic acoustic noise, lamination vibration or electromagnetically-induced acoustic noise, or more rarely, electrical noise, or "coil noise",

looking on the application. The term electromagnetic noise is usually avoided because the term is employed within the field of electromagnetic compatibility, managing radio frequencies. The term electrical noise describes electrical perturbations occurring in electronic circuits, not sound. For the latter use, the terms electromagnetic vibrations or magnetic vibrations, that specialize in the structural phenomenon are less ambiguous.

Acoustic noise and vibrations due to electromagnetic forces can be seen as the reciprocal of microphonics, which describes how a mechanical vibration or acoustic noise can induce an undesired electrical perturbation [1].

In telecommunications, an interference is that which modifies a signal in a disruptive manner, as it travels along a communication channel between its source and receiver. The term is often used to refer to the addition of unwanted signals to a useful signal.

Noise is a form of interference but not all interference is noise.

A solution to interference problems in wireless communication networks is interference alignment, which was crystallized by Syed Ali Jafar at the University of California, Irvine. A specialized application was previously studied by Yitzhak Birk and Tomer Kol for an index coding problem in 1998. For interference management in wireless communication, interference alignment was originally introduced by Mohammad Ali Maddah-Ali, Abolfazl S. Motahari, and Amir Keyvan Khandani, at the University of Waterloo, for communication over wireless X channels. Interference alignment was eventually established as a general principle by Jafar and Viveck R. Cadambe in 2008, when they introduced "a mechanism to align an arbitrarily large number of interferers, leading to the surprising conclusion that wireless networks are not essentially interference limited." This led to the adoption of interference alignment in the design of wireless networks.

In many cases noise found on a signal in a circuit is unwanted. There are many different noise reduction techniques that can reduce the noise picked up by a circuit.

Faraday cage – A Faraday cage enclosing a circuit can be used to isolate the circuit from external noise sources. A faraday cage cannot address noise sources that originate in the circuit itself or those carried in on its inputs, including the power supply.

Capacitive coupling – Capacitive coupling allows an AC signal from one part of the circuit to be picked up in another part through the interaction of electric fields. Where coupling is unintended, the effects can be addressed through improved circuit layout and grounding.

Ground loops – When grounding a circuit, it is important to avoid ground loops. Ground loops occur when there is a voltage difference between two ground connections. A good way to fix this is to bring all the ground wires to the same potential in a ground bus.

Shielding cables – A shielded cable can be thought of as a Faraday cage for wiring and can protect the wires from unwanted noise in a sensitive circuit. The shield must be grounded to be effective. Grounding the shield at only one end can avoid a ground loop on the shield.

Twisted pair wiring – Twisting wires in a circuit will reduce electromagnetic noise. Twisting the wires decreases the loop size in which a magnetic field can run through to produce a current between the wires. Small loops may exist between wires twisted together, but the magnetic field going through these loops induces a current flowing in opposite directions in alternate loops on each wire and so there is no net noise current.

Notch filters – Notch filters or band-rejection filters are useful for eliminating a specific noise frequency. For example, power lines within a building run at 50 or 60 Hz line frequency. A sensitive circuit will pick up this frequency as noise. A notch filter tuned to the line frequency can remove the noise.

The noise level in an electronic system is typically measured as an electrical power N in watts or dBm, a root mean square (RMS) voltage (identical to the noise standard deviation) in volts, dBμV or a mean squared error (MSE) in volts squared. Examples of electrical noise-level measurement units are dBu, dBm0, dBrn, dBrnC, and dBrn(f1 – f2), dBrn(144-line). Noise may also be characterized by its probability distribution and noise spectral density N0(f) in watts per hertz.

A noise signal is typically considered as a linear addition to a useful information signal. Typical signal quality measures involving noise are signal-to-noise ratio (SNR or S/N), signal-to-quantization noise ratio (SQNR) in analogue-to-digital conversion and compression, peak signal-to-noise ratio (PSNR) in image and video coding and noise figure in cascaded amplifiers. In a carrier-modulated passband analogue communication system, a certain carrier-to-noise ratio (CNR) at the radio receiver input would result in a certain signal-to-noise ratio in the detected message signal. In a digital communications system, a certain Eb/N0 (normalized signal-to-noise ratio) would result in a certain bit error rate. Telecommunication systems strive to increase the ratio of signal level to noise level in order to effectively transfer data. Noise in telecommunication systems is a product of both internal and external sources to the system.

Noise is a random process, characterized by stochastic properties such as its variance, distribution, and spectral density. The spectral distribution of noise can vary with frequency, so its power density is measured in Watts per hertz (W/Hz). Since the power in a resistive element is proportional to the square of the voltage

across it, noise voltage (density) can be described by taking the square root of the noise power density, resulting in volts per root hertz. Integrated circuit devices, such as operational amplifiers commonly quote equivalent input noise level in these terms (at room temperature).

UDC 004.62

HUMAN PHYSICAL ACTIVITY RECOGNITION ALGORITHM BASED ON SMARTPHONE SENSOR DATA AND CONVOLUTIONAL NEURAL NETWORK

Wan Z.W., gr.167011, master

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

Baryskievic A.A. – PhD in Technical Sciences

Annotation. Human activity recognition (HAR) is a prominent application of advanced Machine Learning (ML) and Artificial Intelligence (AI) techniques that utilizes computer vision to understand the semantic meanings of heterogeneous human actions. This paper describes a supervised learning method that can distinguish human actions based on data collected from practical human movements. This study proposes a HAR classification model based on a Convolutional Neural Network (CNN) and uses the collected human action signals. The model was tested on the WISDM dataset, which resulted in a 92 % classification accuracy. This approach will help to conduct further researches on the recognition of human activities based on their biomedical signals.

Keywords. Human activity recognition, machine learning, convolutional neural network

There are several approaches to collect HAR data from the participating subjects; broadly, they fall into one of the two categories – namely camera-based recording or sensor-based recording [1]. In the former approach, one or more video cameras are set up to record the activities of a subject for a certain amount of time, and then the recognition is performed using video analysis and processing techniques. The later one utilizes various types of sensors to track the movements of the subject. This approach can be further classified based on the type of sensors used, whether they involve wearable body sensors or the external ones [2]. External sensors are placed in predetermined points of interest on the subjects' body, whereas wearable sensors require to be attached to the subject while collecting data. Each of these techniques has its advantages, shortcomings, and apposite applications. Some recognition techniques even combine multiple recording techniques to collect more relevant data and make the corresponding actions more interpretable to the machines. The applications of HAR include intelligent surveillance, haptics, human-computer interaction, motion or gesture-controlled devices, automatic health-care monitoring systems, prosthetics, and robotics. Despite many advancements, HAR is still a challenging task because of the articulated nature of human activities, the involvement of external objects in human interactions, and complicated spatiotemporal structures of the action signals [3]. Success in recognizing these activities requires advanced signal and image processing techniques, as well as sophisticated ML algorithms. Since the absolute performance is yet to be achieved, HAR remains a tending field to the researchers.

The WISDM dataset contains mobility information that was collected from 30 people of different ages (ranging from 19 to 48 years), genders, heights and weights using a wrist-mounted smartphone. The smartphone has integrated accelerometer and gyroscope. Action data was recorded using these sensors while each of the subjects was performing six predefined tasks, which according to the jargon of ML, represent six different classes. Three-axial linear acceleration and three-axial angular velocity data were acquired at a steady rate of 20 Hz. The collected samples were labeled manually afterward. Before putting in the dataset, the samples were pre-processed using a median filter for noise cancellation and a thirdorder low-pass Butterworth filter having a 20 Hz cutoff frequency.

This study aims to classify the HAR signals of the WISDM dataset employing a CNN model, as shown in Figure 1. The training stage requires a set of data samples containing various attributes measured from subjects while performing various predefined activities. The supervised learning technique then try to make some "sense" out of the data, find out how the samples that belong to the same class are similar to each other while samples from different classes are diverse, then builds one or more internal models focusing on the crucial attributes that can highlight those contrasting properties to carry out the classification [1]. In the training stage, a preordained portion of the dataset is used to train the machine and build a feasible model, which is then evaluated over the remaining samples.

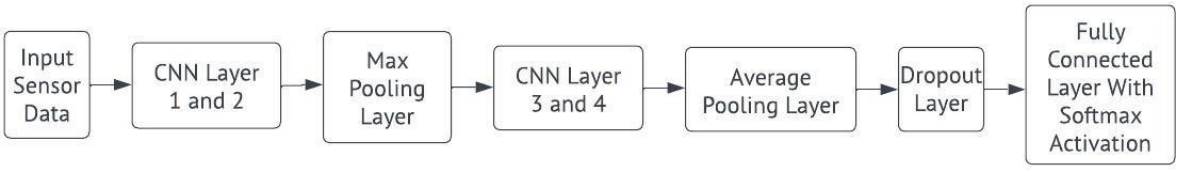


Figure 1. Block diagram of the proposed CNN-based HAR algorithm

The data has been preprocessed in such a way that each data record contains 80 time slices (data was recorded at 20 Hz sampling rate, therefore each time interval covers four seconds of accelerometer reading). Within each time interval, the three accelerometer values for the x axis, y axis and z axis are stored. This results in an 80×3 matrix. The data must be passed into the neural network as a flat vector of length 240. The first layer in the network must reshape it to the original shape which was 80×3. The model is tested on the human behavior pose dataset WISDM. We selected 80 % of the data in the WISDM dataset for model training and 20 % for model testing. Using Adam as optimizer, batch size equals to 400, epochs equal to 50 (training for 50 rounds).

Accuracy is a measure for how many correct predictions your model made for the complete test dataset. It is measured by the following formula:

$$\text{Accuracy} = (TP + TN)/(TP + TN + FP + FN), \quad (1)$$

where TP – True Positives, FP – False Positives, FN – False Negatives, and TN – True Negatives.

The model learns well with accuracy reaching above 92 % and loss hovering at around 0,39.

List of used sources:

1. Human activity recognition: using wearable sensors and smartphones. / M. Labrador, Y.O. Lara // CRC Press, 2013.
2. Human activity recognition and prediction. / Fu Y // Springer, 2016.
3. Human Action Recognition with Depth Cameras. / J. Wang [et al.] // Springer International Publishing, 2014.

UDC 004.62

PHOTOPLETHYSMOGRAPHY AND ACCELEROMETER SENSOR SIGNALS FOR THE DETECTION OF PHYSICAL ACTIVITY

Wei S.S.

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

Wei S.S. – Master in Systems and Networks of Infocommunications

Annotation. Wearable devices for monitoring human physiological parameters have become popular, and due to their low cost, the most common method of monitoring human information in such devices is the use of photoplethysmography (PPG) signals. Nevertheless, the accurate estimation of the PPG signal recorded from the subject's wrist during various physical exercises is often a challenging problem because the initial PPG signal is heavily corrupted by motion artifacts. Long Short Time Memory (LSTM) is built to recognize activities.

Keywords. Photoplethysmography, Accelerometer, LSTM.

Accurate estimation of the wrist-recorded PPG signal is often a difficult problem when the patient is wearing the wearable device during exercise, because the original PPG signal is strongly affected by motion artifacts (MAs), mainly due to the relative motion between the PPG springs and the skin of the wrist [1]. To reduce MAs, a number of signal processing techniques based on data from different types of sensors, especially ACC data, have proven to be very useful.

ACC provides information about the acceleration of the human body during motion. In smartphones and smartwatches, the integrated three-axis ACC is probably the most commonly used sensor for activity tracking. A combined approach to retrieve PPG and acceleration data is available directly on smartphones and smartwatches [2]. HAR can be viewed as a pattern recognition problem where machine learning techniques have been particularly successful. Several machine learning models have been developed for HAR. The main goal of this paper is to maintain the good performance of the RNN framework in terms of detection accuracy [3], and an RNN for human activity detection using four-dimensional ACC and PPG data has been developed.

PPG signals are continually captured during activities from the wrist using Maxim Integrated MAXREFDES100 device. To guarantee a perfect fit of the sensor unit to the skin surface, a specific weightlifting cuff, adjustable by tear-open closure, is used to hold the sensor in place by fully tightening the strap with a cable protruding from the back end of the strap. The PPG signal value is equivalent to the output of an ADC (Analog to Digital Converters) photodetector with a pulse width of 118 μs, a resolution of 16 bits and a full scale of 8192 nA, illuminated by a green LED (Light-Emitting Diode). The ACC signal values on the three axes correspond to MEMS (Micro-ElectroMechanical System) outputs with 10-bit resolution, left-aligned, and a scale of ±2 g.

For analysis, a recently published data set consisting of 105 PPG signals (15 per subject) and 105 corresponding triaxial ACC signals recorded at 400 Hz from seven different subjects was used. The seven adult subjects were three males and four females, ranging in age from 20 to 52 years, who performed five sets of resting, squatting, and stepping activities. The signals were recorded simultaneously and the dataset contains 210 audio clips with a total duration of 17,201 seconds.

The individual PPG signal values for the same subject are highly variable from series to series, and vary considerably over short periods of time within the same series. Normalization allows for better separation of the PPG signal from motion artifacts using the following equations:

$$\boxed{\mathrm{PPG}_{\mathrm{cal}} = \frac{\mathrm{PPG} - \mu_{\mathrm{PPG}}}{\sigma}}, \quad (1)$$

$$\boxed{\mu_{\mathrm{PPG}} = \frac{1}{N}\sum_{i=1}^{N}\mathrm{PPG}_i} \quad (2)$$

where $\boxed{\mathrm{PPG}_{\mathrm{cal}}}$ is the calculated PPG data, $\boxed{\mathrm{PPG}_i}$ means PPG value of the i-th data.

The accelerometer is affected by the low noise level, the gravitational acceleration is in three spatial axes, so the data usually has some bias, remove it by subtracting the average from the data, the procedure gives a fine filtering of the signal with the following equation:

$$\mathrm{ACC}_{\mathrm{cal}} = \mathrm{ACC} - \mu_{\mathrm{ACC}} \tag{3}$$

$$\mu_{\mathrm{ACC}} = \frac{1}{N}\sum_{i=1}^{N}\mathrm{ACC}_i \tag{4}$$

where $\mathrm{ACC}_{\mathrm{cal}}$ is the calculated ACC data, ACC_i means ACC value of the *i*-th data.

The network model used in the publication is shown in Figure 1. It is based on a widely used architecture for time-based sensor data and consists of a combination of fully connected layers and LSTM modules [4]. The input data has three acceleration axes, and PPG generates a four-dimensional timeline. The data is then transmitted to the network in a window, where the parameter is the time point size of one data window.

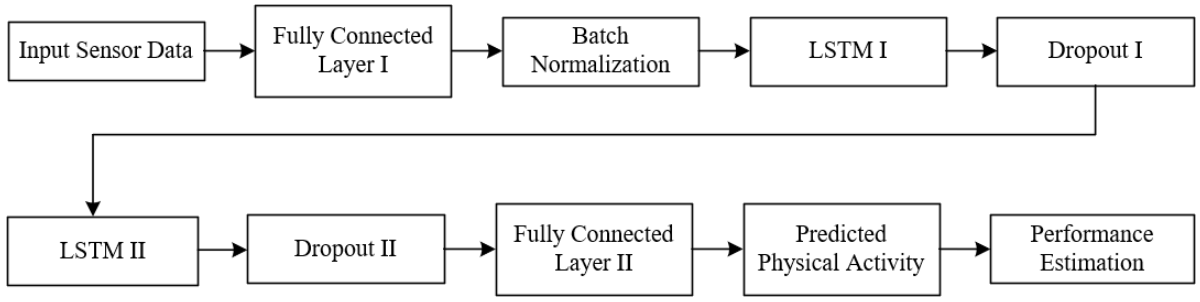


Figure 1-The network model for training dataset

The first layer is fully connected layer and aims to identify the relevant features in the input data. In this layer, the general neuron produces an output value y.

$$y = f\left(\left[w_1, w_2, \ldots, w_n\right]\left[x_1, x_2, \ldots, x_n\right]^T + b\right), \tag{5}$$

where the x_n inputs to the layer and the w_n neuron weights in association with each input, f is the activation function and b is the bias value.

The batch normalization layer, which normalizes the mean and standard deviation of the global data, operates on individual batches of data with training. Then, the recurrent neural network is represented at its core by two cascaded LSTM layers, with the LSTM followed by a dropout layer that randomly discards some of the inputs to reduce overfitting.

In the end, there is a fully connected layer of size 3 which, together with the sparse class cross-entropy loss function assigned to the network, classifies one of these three classes of layers. The loss function represents the error that must be minimized by the training process. The representation of the error varies upon the given function of the network allotted to it. For a categorical cross-entropy function $J(w)$, the error function is as follows:

$$J(w) = -\frac{1}{N}\sum_{i=1}^{N}\left[y_i \log y_i + (1-y_i)\log(1-y_i)\right], \tag{6}$$

where w is the set of model parameters, N is the number of input test features, y_i and y_i are the true and predicted classes respectively, expressed numerically.

The virgin PPG signal has been severely corrupted by MAs, mainly due to the relative motion between the PPG source and the wrist skin. In order to reduce MAs, the ACC data and PPG were integrated into four-dimensional data, which were processed and analyzed. In an investigation of Python based data analysis of PPG and ACC signals, the study completed the design of functions such as importing data and analysis of signals.

List of sources used:

1. Temko, Andriy. "Accurate heart rate monitoring during physical exercises using PPG." IEEE Transactions on Biomedical Engineering 64.9 (2017): 2016-2024.
2. Seok, Dongyeol, et al. "Motion artifact removal techniques for wearable EEG and PPG sensor systems." Frontiers in Electronics 2 (2021): 685513.
3. Sherstinsky, Alex. "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network." Physica D: Nonlinear Phenomena 404 (2020): 132306.
4. Shewalkar, Apeksha, Deepika Nyavanandi, and Simone A. Ludwig. "Performance evaluation of deep neural networks applied to speech recognition: RNN, LSTM and GRU." Journal of Artificial Intelligence and Soft Computing Research 9.4 (2019): 235-245.

UDC 004 81

HUMAN PHYSICAL ACTIVITY RECOGNITION ALGORITHM BASED ON SMARTPHONE DATA CONVOLUTIONAL NEURAL NETWOrK AND LONG SHORT TIME MEMORY

Z.X YANG., Z.Y CHEN., H LI, gr.167011, master

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

BARYSKIEVIC I.A. – PhD in Digital signal processing algorithm and image compression

Annotation. A deep learning framework for activity recognition based on smartphone acceleration sensor data, convolutional neural network (CNN) and long short-term memory (LSTM) is proposed in the paper. The proposed framework aims to improve the accuracy of human activity recognition (HAR) by combining the strengths of CNN and LSTM. The CNN is used to extract features from the acceleration data and the LSTM is used to model the temporal dependencies of the features. The proposed framework is evaluated on the publicly available dataset, it includes 6 different actions: walking, walking upstairs, walking downstairs, sitting, standing, laying. The physical activity recognition accuracy has reached 94 %.

Keywords. HAR, CNN, LSTM, Acceleration sensor.

With the rapid popularity of smartphones and the rapid development of micro sensors, various MEMS sensor devices are embedded in people's smartphone. The main advantages of MEMS sensors are small size, light weight, low power consumption, high reliability, high sensitivity, easy integration, etc. And the research on human behavior recognition based on sensor-based intelligent devices has become an emerging research topic in recent years, traditional machine learning algorithms extract feature vectors from data to distinguish between classes of activities, and researchers have done a lot of research work in this area. FGD Silva [1] used two methods, FDR and PCA, to extract 19 features from the data and used SVM method to classify the activities, VNT Sang [2] applied KNN, ANN and SVM algorithms for classification and recognition of human behavior, R Singh [3] et al. proposed an algorithm for human state recognition activity using decision tree C4,5 by data mining algorithm. Since traditional machine learning algorithms require manual extraction of features in the data, and it is difficult for non-professionals to extract effective feature sets, manual extraction is also subject to human error and time-consuming, all of these methods which will reduce the accuracy of classification and recognition, but neural networks greatly compensate for the lack of manual feature extraction in traditional machine learning by building a multi-level automatic feature extraction architecture.

Data acquisition for human behavior recognition is basically divided into two categories, video image-based data acquisition and wearable sensor-based data acquisition. In this paper, we focus on human activity recognition based on wearable sensing data. This paper uses the built-in acceleration sensor of a smartphone for data collection.

The network model consists of three convolutional layer and LSTM network layers, fully connected layer, and one Softmax layer, and predicts the corresponding human actions from the data set. The proposed algorithm's accuracy achieved 94 % and the loss is about 0,02 at the test set.

The algorithm which we proposed consists of six different layers: three 1D convolutional layers, LSTM network layer, fully connected layer, and Softmax layer. The structure diagram of the algorithm is shown in Figure 1.

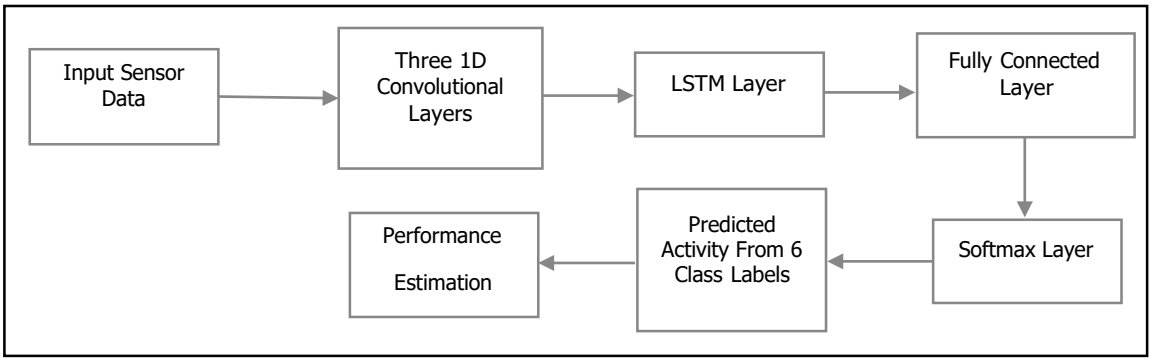


Figure 1 – The block scheme of physical activity recognition algorithm based on CNN-LSTM neural network

We tested the recognition accuracy of the algorithm using data from the publicly available dataset UCI-HAR. In this dataset, 70 % of the volunteers was selected for generating the training data and the remaining 30 % is used to test the data. We set the training set to 100 and train on the training set for 50 epochs. The loss value and the accuracy values are shown in Figure 2.

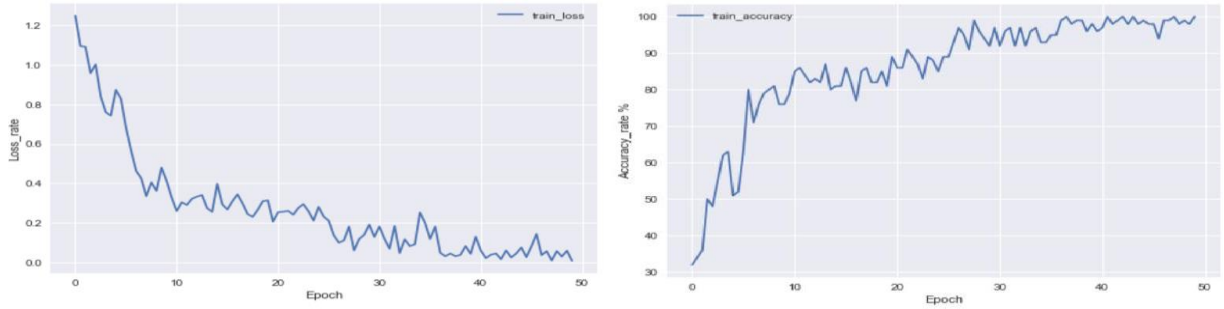


Figure 2 – Loss and accuracy rate of the CNN-LSTM model

In the second experiment, to predict human activities, we used only a pure LSTM algorithm for comparison with our algorithm. This choice was made because human activities are sequences of actions, and LSTMs are known for their effectiveness with time series sensor data. By capturing temporal dependencies from this data, the LSTM model was able to achieve an accuracy of 92.98%. The experimental results are illustrated in Figure 3, which displays the training and validation loss.

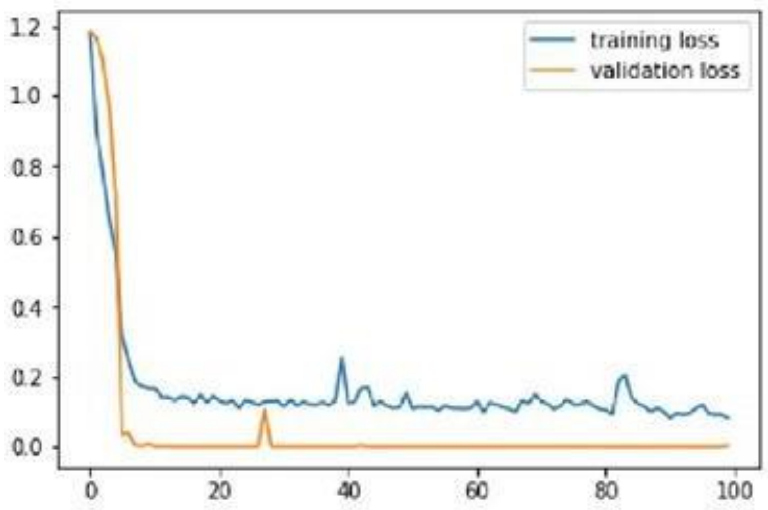


Figure 3 – Training and validation loss of LSTM

We conducted experiments using different optimizer such as stochastic gradient descent (SGD), Adagrad, RMSprop and Adam. We decided to use Adam as an optimizer based on our preliminary results. Experimental results showed the accuracy of 94 % which outperformed different forms of LSTM models used in this dataset. The adding of additional layers did not show any significant accuracy improvement but only increased the computational cost. Therefore, we decided to keep our CNN-LSTM algorithm simple by keeping three 1D convolutional layers and one LSTM network. The experimental results showed the advantages of using hybrid model over pure and other forms of LSTM models. We also compared our

results with state-of-the art LSTM models proposed on same dataset. The comparison of performance of other LSTM models on UCI HAR dataset is given in the Table 1.

Table 1 – Performance comparison on UCI HAR dataset

Algorithm	Accuracy
LSTM-CNN	94,00 %
LSTM	92,98 %
Bidirectional LSTM [4]	92,67 %
Res-LSTM [5]	91,60 %
Baseline LSTM [5]	90,80 %

The performance comparison table shows the effectiveness of our CNN-LSTM model compared to state-of-the-art methods used for LSTM, Bidirectional LSTM, Res-LSTM and Baseline LSTM model on same UCI HAR dataset. The CNN-LSTM model yield better recognition score than applied LSTM model and outperformed other forms of LSTM used for activity recognition in the same dataset.

Reference:

1. Accelerometer based intelligent system for human movement recognition / Silva F G., Galeazzo E // 2013. P. 20-24.
2. Human activity recognition and monitoring using smartphones / VNT Sang., Vu Ngoc Thanh // 2015. P. 481-485.
3. Analysis of Feature Selection Techniques for Network Traffic Dataset / Singh R., Kumar H., Singla R K // 2014. P. 42-46.
4. Human activity recognition on smartphones using a bidirectional lstm network / F Hern´andez., L F Su´arez., J Villamizar // 2019, pp. 1–5.
5. Deep residual bidir-lstm for human activity recognition using wearable sensors. / Y Zhao., R Yang., G Chevalier., X. Xu // Mathematical Problems in Engineering. vol. 2018.

UDC 004.62

NOISE REDUCTION METHOD FOR SKELETONIZED IMAGES

Yuan Liu, Master student

Belarusian state university of informatics and radioelectronics

г . Minsk, Republic of Belarus

Salomatin S.B – PhD in Technical Sciences

Annotation. Scale-space-based denoising approaches adopt scale space filters before the binarization stage to smooth the potential noise. These kinds of methods can simultaneously suppress both inner noise and border noise. 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 information can be used in many fields, such as image matching [1], sketch-based modeling [2], and medical image segmentation [3]. And in recent years, hand gesture recognition and human action recognition based on skeletons are attracted much focus. For the task of recognition or classification, since the later recognition depends on the extracted skeleton, it is very important to extract a stable skeleton. There are two main approaches to obtaining skeletons, which are hardware approaches and software approaches. The hardware approach uses a depth camera such as Kinect. These skeletons obtained from Kinect are robust to lighting, shade, and color changes, so these skeletons can be deemed stable. The software approaches use traditional skeletonization to extract the skeleton from the normal camera. Since existing skeletonization methods are sensitive to noise, the skeleton may be altered according to the noise; it is necessary to adopt denoising strategies to make the skeleton more stable.

Conventional skeletonization algorithms extract skeletal images from input binary images composed of foregrounds and backgrounds. Skeletons are extracted from those foregrounds area. Generally, images obtained from a standard camera are colorful images instead of binary images. Therefore, several preprocessing is needed before skeletonization, including converting the RGB images to grayscale images and then following binarization on grayscale images to acquire binary images. From the perspective of binary image, there are two types of cases in which even tiny changes may significantly alter the result of the skeletonization algorithm; since stable skeletons are expected to reflect the overall structure instead of small structures, these two cases are considered as border noises and inner noise according to their position, respectively.

Pruning methods [4] 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.

A scale-space method for thinning both grayscale and binary images has proposed by Hoffman and Wong [5]. 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.

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 σ_{init}.

Output: The best skeleton I_{best}

Step 1: Initialize the scale of the Gaussian filter σ 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;

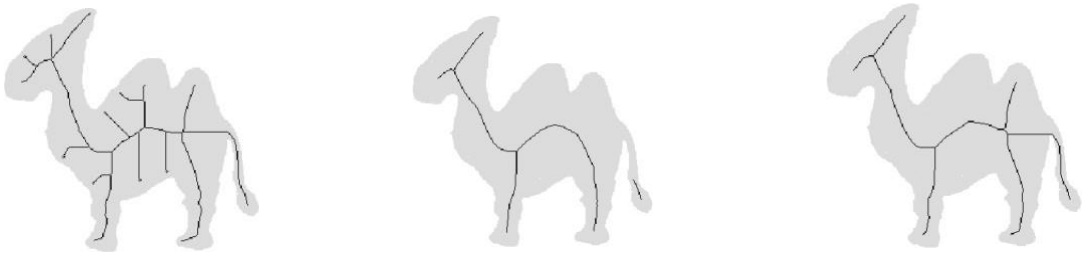
Step 5: Calculate the sensitivity measure S_σ of the skeleton I_{th} and record it in the memory;

Step 6: If the sum of σ and the σ_{init} is less than σ_{max}, increase σ with a given step σ_{init} and go to the step 2; Otherwise, go to step 7;

Step 7: Find the smallest S_σ and then obtain corresponding skeleton I_{best}

Experiments and results

Obviously, in the figure below, the skeleton extracted by FPSA has many redundant branches caused by internal noise. Both Houssem's method and the proposed method can eliminate this branch very well. But Houssem's method cannot preserve the original topology because some important skeletons are lost. The method proposed in this paper can basically get 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 Yang C, Tiebe O, Shirahama K and Grzegorzek M 2016 Pattern Recognition 55 183–197

2 Mourot L, Hoyet L, Le Clerc F, Schnitzler F and Hellier P 2022 A survey on deep learning for skeleton-based human animation Computer Graphics Forum vol 41 (Wiley Online Library) pp 122–157

3 Ma J, Wang J, Li J and Zhang D 2022 Computers and Graphics 102 56–66

4.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.

5.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.

UDC 621.391

RESEARCH ON CHINESE SIGN LANGUAGE RECOGNITION BASED ON SKELETON FEATURES

Qiu Yuepeiyan, post-graduate student

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

Abstract. The hearing-impaired people in China account for about 20% of the world 's hearing-impaired people, and increase year by year. Chinese sign language is an important auxiliary tool for communication between the hearing impaired and the outside world. Finger language is a part of sign language, the number of it is not large and it is easy to learn and remember. Therefore, this thesis takes Chinese letter sign language as the research object, studies Chinese letter sign language in different backgrounds, and researches the skeleton extraction of gesture images, the presentation and recognition of skeleton descriptors based on computer vision.

The main research content of this thesis is Chinese letter sign language recognition based on skeleton features. Firstly, gestures are extracted. Secondly, on the basis of the extracted binary image of gestures, an improved gesture skeleton extraction method based on distance change is proposed to make the extracted skeletons have connectivity.

Keywords*:* sign language recognition; skeleton; probabilistic neural network.

Introduction

The main research content of this thesis is Chinese letter sign language recognition based on skeleton features. Firstly, gestures are extracted. Secondly, on the basis of the extracted binary image of gestures, an improved gesture skeleton extraction method based on distance change is proposed to make the extracted skeletons have connectivity; then, an improved invariant moment is proposed to describe the skeleton; finally, probabilistic neural network is used to classify the value of the obtained invariant moment to achieve the purpose of recognizing gestures. To sum up, this thesis mainly conducts research work from the following two aspects:

(1) A gesture skeleton extraction method combining distance transformation and morphological watershed algorithm is proposed. This method uses the distance field and watershed algorithm to obtain the skeleton potential map containing the gesture skeleton, uses the active contour model to determine the skeleton endpoint, and trims the redundant skeleton through the A * algorithm to obtain the final skeleton. Experimental results prove that the skeleton obtained by this method not only solves the problem of disconnection of the skeleton extracted by the skeleton extraction method based on distance transformation, but also ensures the single pixel of the skeleton and conforms to the target topology.

(2) An improved invariant moment is proposed to describe the gesture skeleton and apply it to the field of gesture recognition. First, it proves that Hu invariant moments are not fully scale invariant in digital images. Then, on the basis of Hu invariant moments, circumvent the limited invariant moments, eliminate their regional factors, and derive Iimproved invariants moment describing the skeleton of the gesture, and finally combined with probabilistic neural network for sign language recognition. The experiment proves that the improved invariant moment proposed in this thesis changes the eigenvalue of the gesture skeleton when it rotates and scales. The accuracy is improved by 5% when it is combined with probabilistic neural network for sign language recognition.

Sign Language Recognition Research

Sign language is a "language" spoken by people who are hard of hearing or otherwise unable to communicate verbally. In sign language recognition research, researchers usually use different kinds of algorithms to recognize sign language. Sign language can not only be expressed through hand movements alone, but also can be expressed with the help of external things, such as directions. Generally, sign language recognition can be divided into static sign language

recognition and dynamic sign language recognition. Static sign language recognition refers to the recognition of the information expressed by individual sign language gestures at a certain point in time; compared with static sign language recognition, the recognition of dynamic sign language is more complicated, and dynamic sign language recognition needs to recognize the information expressed by gestures within a certain period of time , for dynamic sign language recognition, the information to be expressed must be recognized under the premise of correctly capturing dynamic gestures.

Gesture Segmentation

Compared with the computational complexity of converting an RGB image to the HSV color space, the computational complexity of converting an RGB image to the YCbCr color space is lower.[1] The conversion method of YCbCr is more direct and convenient, and there is no need to consider the calculation method according to the situation. Also, in the YCbCr color space, the distribution of skin tones is tighter and less sensitive to light. Therefore, in this article, the RGB image is converted to the YCbCr color space.[2]

Basic Idea Of Skeleton

Regarding the skeleton, it can be approximately regarded as the central axis of the object. After the skeleton theory was proposed, because the skeleton of the object is not only concise and clear, but also can represent the topological structure of the object very well, especially when there is a cavity inside the object (such as a water cup with a handle), the contour information cannot represent the water cup and the handle. There are holes between them, and in the case that the topological structure of the object can also be represented, the number of pixels required by the skeleton is much less than the number of pixels required by the outline, so the skeleton is often applied to life Not only the image field, but also other fields, such as: archaeology [3], literature [4], sorting of materials [5] and information storage and retrieval [6], etc.

Skeleton Recognition

Skeleton recognition is the last step of object recognition.Comparing the processed skeleton with the skeleton in the library,it can retrieve the graphics corresponding to the graphics library by the matching degree of object skeleton. Therefore, the key step of shape retrieval is to perform effective bone matching[7].At present, there are several common skeleton matching methods,such as skeleton graph matching based on path similarity,skeleton matching based on clustering and affine invariant of image feature matching algorithm.

Conclusion

The research in this paper adopts sign language recognition based on computer vision: the image of sign language gestures is captured by the camera, the image is preprocessed to extract the binary image of the gesture, and then the skeleton features of the gesture are extracted, and the skeleton features of the gesture image are extracted using the improved invariant moments. It is represented by feature quantity, and finally, the calculated feature quantity information is classified (that is, recognized) by using a probabilistic neural network.

References

1. Wu Y , Huang T S . Human hand modeling, analysis and animation in the context of HCI[C]// International Conference on Image Processing. IEEE, 1999.
2. Davis, J, Shah, M. Visual gesture recognition[J]. IEE Proceedings-Vision, Image and Signal Processing, April1994:321-332.

3. Dong J , Lin W , Huang C . An improved parallel thinning algorithm[C]// 2016 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR). IEEE, 2016.
4. Martin Manak, Ivana Kolingerova. Extension of the edge tracing algorithm to disconnected Voronoi skeletons[J]. Information Processing Letters, 2016, 116(2):85-92.
5.Wang Pengfei, Zhao Fan, Ma Shiwei. Skeleton extraction method based on distance transform[C]// 2013 IEEE 11th International Conference on Electronic Measurement & Instruments (ICEMI). IEEE, 2013.
6. Shen, W., Bai, X., Hu, R., Wang, H., & Latecki, L. J. (2011). Skeleton growing and pruning with bending potential ratio. Pattern Recognition, 44(2), 196-209.
7. Wang H, Chai X, Hong X, et al. Isolated sign language recognition with grassmann covariance matrices[J]. ACM Transactions on Accessible Computing (TACCESS), 2016, 8(4): 1-21

СВЕДЕНИЯ ОБ АВТОРАХ

1. Цю Юпейян – аспирант кафедры инфокоммуникационных технологий БГУИР

2. Цветков Виктор Юрьевич – д.т.н., заведующий кафедрой инфокоммуникационных технологий БГУИР

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сборник материалов 59-ой научной конференции аспирантов, магистрантов и студентов

Ответственный за выпуск *В.И. Брилевский*

Компьютерная верстка *Шкред А.В.*

Дизайн обложки *Кайдак Д.Н.*