ISSN 2409-1677

ВЫСШАЯ ШКОЛА

раскрытие научной новизны исследований

июль (13) 2017

В номере:

ВЫСШАЯ ШКОЛА

Научно-практический журнал
№ 13 / 2017

Периодичность – два раза в месяц

Учредитель и издатель:
Издательство «Инфинити»

Главный редактор:
Хисматуллин Дамир Равильевич

Корректура, технический редактор:
А.А. Силиверстова

Компьютерная верстка:
В.Г. Кашапов

Контакты редакции:
Почтовый адрес: 450000, г.Уфа, а/я 1515
Адрес в Internet: www.ran-nauka.ru
E-mail: mail@ran-nauka.ru

ISSN 2409-1677

Тираж 500 экз. Цена свободная.

СОДЕРЖАНИЕ

ТЕНДЕНЦИИ РАЗВИТИЯ ЛЕГКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ УЗБЕКИСТАН

Мухаммадалиева Наргиза Баходировна

ТУИТ

Легкая промышленность Узбекистана имеет многовековые традиции по переработке местного сырья: хлопкового волокна – национального богатства страны, шелка, шерсти и кожи, каолинов. Через Узбекистан проходил Великий шелковый путь и производимые узбекскими ремесленниками хлопковые и шелковые ткани, нарядная и повседневная одежда, национальная обувь, сюзане с оригинальными рисунками были известны во многих странах мира.

После обретения независимости перед нашей страной встала серьёзная задача – нужно было строить отрасль практически с нуля, так как Узбекистан долгое время являлся сырьевым придатком. Хлопковое волокно вывозилось как сырьё в другие республики, а потом уже приходилось завозить из-за пределов страны по более высоким ценам готовую продукцию из него с высокой добавленной стоимостью. Таким образом, республика теряла огромную прибыль и фактически не имела никакой производственной базы для переработки собственного хлопкового сырья. К примеру, в 1990-95 гг. лишь около с 7% производимого хлопка-сырца перерабатывалось внутри республики.

Стимул развитию легкой промышленности, в частности текстильной, была способна дать только целенаправленная системная государственная промышленная политика, нацеленная на поддержку приоритетных проектов, в том числе и инновационных, а также борьба с контрафактом, который стал серьезной проблемой в первые годы существования республики. И здесь хорошо себя показала модель взаимодействия бизнеса и государства, когда они совместными усилиями вытеснили нелегальную продукцию с рынка, замещая ее собственными товарами и законным импортом, создавая прозрачный рынок и повышая на нем уровень конкуренции.

Тогда, в середине 1990-х, специалисты определили круг основных проблем, с которыми было необходимо бороться в кратчайшие сроки. Это были техническая и технологическая отсталость отрасли, низкий уровень инновационной и инвестиционной деятельности, высокая энергоемкость, трудоемкость и сырье, что в конечном итоге приводило к слабой конкурентоспособности отечественных товаров. В то время эту ситуацию можно было увидеть, даже не проводя специализированные маркетинговые исследования. Достаточно было выйти на рынки, где покупателю предлагали импортную продукцию откровенно плохого качества.

Для изменения сложившейся ситуации акцент был сделан на уникальные для Узбекистана факторы, которые давали отечественным предприятиям и созданным здесь СП ряд преимуществ, в частности, это низкая стоимость энергоресурсов, квалифицированный персонал, развитая инфраструктура, наличие собственной научной базы, налоговые и таможенные льготы. Перечисленные факторы на сегодняшний день обеспечивают отрасли одно из ведущих мест в реальном секторе экономики.

Благодаря проделанной работе за годы независимости объем внутренней переработки хлопкового волокна с 7 % в 1991 году увеличился до 35 % в 2016 году от общего объема производства. По прогнозам экспертов, в 2017 году показатель внутренней переработки хлопкового волокна должен вырасти еще больше1.

Отметим, что на данном этапе развития страны легкая промышленность Узбекистана – это важнейший многопрофильный и инновационно привлекатель-ный сектор экономики. Согласно программе, в 2015-2020 годах ГАК «Узбеклегпром» направит около 1 млрд. долларов США на увеличение внутренней переработки хлопка-волокна и сокращение его экспорта. Программа предусматривает увеличение объемов внутренней переработки хлопка-волокна с 44 до 70% в 2020 году с соответствующим увеличением экспорта текстильной продукции с $800 млн. до $1,5 млрд.

[1] World Trade report, 2016. – P 55.

Разработанная программа развития легкой промышленности Узбекистана позволит повысить уровень внутренней переработки хлопкового волокна и увеличить экспортный потенциал текстильной промышленности.

С такими хлопковыми возможностями Узбекистан просто обязан производить товар, а не сырье. Но для этого необходимо развитие и сопутствующих отраслей. Они способствуют получению эффективного результата от масштабного производства экономически выгодных и экологически безопасных товаров, импортозамещению, повышению экспортного потенциала страны.

Вместе с тем, отрасль содействует гармоничному развитию областей, снижению социальной напряженности, обеспечению занятости населения и улучшению его благосостояния, оказывает помощь в становлении и развитии малого бизнеса. Так, на сегодняшний день существенная часть предприятий легкой промышленности республики приходится на Государственно-акционерную компанию «Узбекенгилсаноат», в составе которой более 300 предприятий и объединений, имеющих сеть филиалов.

Сегодня еще одним показателем привлекательности отрасли является и уровень осваиваемых в ней инвестиций. Так, в период с 1995 года по настоящее время в отрасль привлечено иностранных инвестиций в объеме свыше двух млрд. долларов с организацией новых рабочих мест, что имеет высокое социальное значение. За эти годы создано более 150 предприятий с участием иностранных инвесторов из Германии, Швейцарии, Италии, Южной Кореи, Японии, Турции, США, Индии и других стран. Введены в эксплуатацию современные текстильные предприятия, включающие отделочное, вязальное и швейное производства.

Только за последние четыре года введены в эксплуатацию 92 промышленных предприятия общей стоимостью 575,3 млн. долларов и с экспортным потенциалом 215,8 млн. долларов, создано более 11,6 тысяч рабочих мест.

В настоящее время производственные мощности отрасли составляют 450 тысяч тонн пряжи, 296 млн. квадратных метров тканей, 90 тысяч тонн трикотажного полотна и 270,2 млн. единиц швейно-трикотажных изделий в год. Современный дизайн наряду с высокими техническими характеристиками делает продукцию предприятий легкой промышленности наиболее привлекательной и позволяет занимать собственную нишу на международном рынке, конкурировать на самом высоком уровне с мировыми брендами2.

Легкая промышленность занимает существенную нишу в общем объеме экспорта республики. Вызов за рубеж продукции предприятий отрасли за годы независимости значительно увеличился не только по объемам. Расширилась география экспорта, а также количество предприятий-экспортеров. Наряду с этим увеличивается с каждым годом и доля новых предприятий-экспортеров от общего объема экспорта.

Если обратить внимание на процесс развития отрасли, то в 1994 году объем привлеченных иностранных инвестиций в предприятия легкой промышленности составлял всего лишь 5,2 млн. долларов. В 2001 году этот показатель достиг уже 649,6 млн. долларов, в 2010 году - 1,8 млрд. долларов, а по итогам 2016 года - 2,4 млрд. долларов. В нынешнем году ожидается прирост прямых иностранных инвестиций еще на 117 млн. долларов.

Таким образом, общий объем иностранных инвестиций в отрасль за годы независимости превысил 2,5 миллиарда долларов, благодаря чему реализовано более 290 крупных инвестиционных проектов.

Динамика роста определяется ежегодным обеспечением ввода не менее 30 новых производств и модернизации имеющихся мощностей по производству, в том числе новой текстильной продукции, как, например, пряжа из бамбука и меланжевая пряжа, а также готовые изделия из них, шелковые ткани и изделия, жаккардовое и рингельное полотно, большой ассортимент готовой швейной и трикотажной продукции с применением оригинальных решений отечественных дизайнеров, соответствующих мировым тенденциям индустрии моды под маркой «Сделано в Узбекистане».

В республике появились крупные современные текстильные комплексы, включающие в себя отделочные, трикотажные и швейные производства. Установлены красильно-отделочные мощности, позволяющие осуществлять покраску и отделку полотна в соответствии с современными требованиями для дальнейшего производства качественной готовой швейно-трикотажной продукции3.

Сегодня благодаря внедрению в отрасль современных высокопроиз-водительных технологий вывоз продукции возрос в 120 раз – до одного миллиарда долларов против семи млн. долларов в 1991 году. В настоящее время продукция с торговой маркой «Сделано в Узбекистане» экспортируется уже в 50 стран мира, из них освоены пять новых рынков сбыта – Венгрия, Шри-Ланка, Кения, Марокко и Тунис. Также узбекский текстиль вывозится в такие страны, как Аргентина, Бразилия, Венесуэла, Колумбия, Перу, Чили и ЮАР. На сегодняшний день отраслью создано свыше 60 дилерских подразделений предприятий - экспортеров в странах ЕС, СНГ и Азии.

За рассматриваемый период легкая промышленность республики и ее система управления прошли долгий путь совершенствования и развития. Были достигнуты значительные результаты и приняты необходимые меры по расширению присутствия текстильной продукции Узбекистана на мировом рынке.

[2] МИД РУз. http://www.mfa.uz/ru/press/news/2016/07/7983/

[3] Рахимов Ш. АО «Узбекенгилсаноат». http://www.narodnoeslovo.uz/index.php/homepage/i-tisodijot/item/ 7392-legkaya-promyshlennost-uzbekistana-tsentr-prityazheniya-investitsij

Тем не менее, с учетом развития тенденций внешнеэкономической деятельности Республики Узбекистан и выхода ее на новые рынки сбыта задаются определенные предпосылки и требования для дальнейшего совершенствования отечественной легкой промышленности.

ПОЧТА АЛОҚАСИ КОРХОНАЛАРИДА ТАДБИРКОРЛИК ФАОЛИЯТИНИ ТАШКИЛ ҚИЛИШ ИСТИҚБОЛЛАРИ

Худойбердиев Раҳматилло Фозиллиддинович
Почта алоқаси технологияси кафедраси ассистенти
Мухаммад Ал-Хоразмий номидаги Тошкент Ахборот Технологиялари Университети

Барчамизга маълумки, 2016 йил 29 декабрь куни Ўзбекистон Президенти Шавкат Мирзиёев «Тадбиркорлик фаолиятининг жадал ривожланишини таъминлашга, хусусий мулкни ҳар томонлама ҳимоя қилишга ва ишбилармонлик муҳитини сифат жиҳатидан яхшилашга доир қўшимча чора-тадбирлар қабул қилинганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида»ги қонунни имзолади. Шу муносабат билан Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси қабул қилинган бўлиб унга асосан **2017 — 2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегияси қабул қилинди.** Ҳаракатлар стратегиясининг учунчи бўлимида иқтисодиётни янада ривожлантириш ва либераллаштиришга йўналтирилган макроиқтисодий барқарорликни мустаҳкамлаш ва юқори иқтисодий ўсиш суръатларини сақлаб қолиш, миллий иқтисодиётнинг рақобатбардошлигини ошириш, қишлоқ хўжалигини модернизация қилиш ва жадал ривожлантириш, иқтисодиётда давлат иштирокини камайтириш бўйича институционал ва таркибий ислоҳотларни давом эттириш, хусусий мулк ҳуқуқини ҳимоя қилиш ва унинг устувор мавқеини янада кучайтириш, кичик бизнес ва **хусусий тадбиркорлик ривожини рағбатлантириш**, ҳудудлар, туман ва шаҳарларни комплекс ва мутаносиб ҳолда ижтимоий-иқтисодий тараққий эттириш, инвестициявий муҳитни яхшилаш орқали мамлакатимиз иқтисодиёти тармоқлари ва ҳудудларига хорижий сармояларни фаол жалб этиш каби йўналишларни ривожлантириш кўзда тутилган.

Ўзбекистон почтаси АЖга тадбиркорлик фаолиятини кенгайтириш мақсадида чет эл сармоялар оқими кенгайиши муносабати билан, инвестиция фаолиятини давлат томонидан тартибга солишни асосий вазифаси оммавий ва хусусий манфаатлар, хорижий мамлакатлар, компаниялар, муайян инвесторлар манфаатларини самарали нисбатини белгилаш ҳисобланади. Иқтисодиёт эркинлаша боргани сари, инвестиция фаолиятини давлат тартиблаши кўпроқ кичик бизнес ва хусусий тадбиркорлик соҳибларини инвестиция фаолиятига кенгроқ жалб этилишига ҳамда бу борада уларни рағбатлантиришга қаратилади.

Хорижий мамлакатларини почта алоқаси объектлари фаолиятини асосий йўналишлар ва олинган самарадорлик (1-жадвал)

№	Хорижда почта соҳасини ривожланиш йўналишлари	Олинаётган самарадорлик
1.	Ахборот коммуникация технологиялари асосида янги хизмат турларини кўрсатиш	Почта алоқаси объектларини компьютер технологиялари билан тўлиқ жихозлашга ва ахборотлаштириш натижасида янги хизмат кўрсатишга эришилди
2.	Почта соҳаси энг йирик иш берувчи соҳа	Мамлакатда ишсизлар сонини камайишига ва почта соҳаси нуфузини оширишга эришилди
3.	Почта соҳаси катта молиявий манбаларга эга инвестор	Соҳадаги ислоҳатлар натижасида соҳа катта молиявий манбаларга эга булди ва мамлакатдаги бошқа соҳаларни ривожланишига амалий ёрдам бермоқда
4.	Почта алоқаси объектлари томонидан ижтимоий дастурларни ташкил этиш	Давлатнинг ижтимоий вазифаларини бажаришга амалий ёрдам берилмоқда
5.	Почта соҳасида маркетинг ва реклама фаолияти, жумладан, директ-маркетинг фаолияти	Бозор муносаботлари ва механизмларини ривожлантиришга замин яратилмоқда
6.	Почта соҳасида инновацион жараёнлар	Иқтисодиёт усишга янги ғоялар ва хизматлар билан эришилмоқда
7.	Почта бозорида кучли рақобат муҳити	Хусусий секторни почта бозоридаги фаолият кучли рақобат муҳитини шакллантирди. Бунинг натижасида соҳа миллий иқтисодиётнинг барқарор ривожланаётган соҳаларидан бирига айланди.
8.	Почта алоқаси объектларида экспресс-элтиш ва курьерлик хизматлари	Хизмат кўрсатиш ва сервис соҳасини ривожланишига ижобий таъсир кўрсатди.
9.	Янги хизматлар билан қаторда анъанавий хизматларни ривожлантириш	Почта соҳасини нуфузи ва хизмат турлари ортиб бормоқда

Сўнги йилларда тадбиркорлик фаолиятини ва тадбиркорларни қўллаб қувватлаш борасида қабул қилинаётган қарорларнинг моҳияти шуни кўрсатиб турибдики ривожланган давлатлар тажрибаси ўлароқ тадбиркорлик фаолияти ҳар бир давлатнинг иқтисодиётини жадал суръатларда ривожланишига олиб келадиган энг асосий омиллардан бири ҳисобланади.

Ўзбекистон почтаси аксиядорлик жамиати аксиядорларининг 2016 йил 30 июндаги умумий йиғилишининг 3-сонли баённомаси билан тасдиқланган "Ўзбекистон почтаси" аксиядорлик жамиатининг уставида почта алоқаси соҳасининг тадбиркорлик йўналишида кўрсатиши мумкин бўлган хизматлари келтириб ўтилган. Биз юқорида ушбу фаолият турига кирадиган хизматларни қўриб ўтган едик. Тадбиркорлик фаолиятини қисқача ўрганиб чиқишим натежасида қуйидаги тадбиркорлик фаолиятига тегишли бўлган хизмат турларини почта алоқасига ташкил етиш фойдадан ҳоли бўлмайди деган фикрдаман:

турли хил қурилиш материаллари, хом-ашёларини сотиш;

буюртмаларга асосан ташкилот, корхона ва муассасаларга турли хилдаги бинолар қуриб бериш, ижарага бериш ҳамда сотиш;

автомашиналар учун ёқилгъи қуйиш шаҳобчаларини очиш, ижарага бериш, сотиш;

Жамиятга тегишли бўлган транспорт воситаларини ижарага бериш, хизмат кўрсатиш, сотиш;

қимматли қоғозлар чиқариш, сотиш ва сақлаш, улар билан бошқа операцияларни ўтказиш;

ускуна ва мол-мулк лизинги, прокат ёки ижарага берилиши;

қонун ва бошқа меъёрий ҳужжатлар билан рухсат етилган тижорат ва воситачилик фаолиятни амалга ошириш, шу жумладан банк ҳисоб рақамларидаги бўш пул маблағларни қўшимча даромад олиш мақсадида депозитларга қўйиш;

хусусий ва ташқи савдо тармоғи орқали нақд пулга ва пул ўтказиш ҳисоб-китоби бўйича тамаки маҳсулотлари, вино-ароқ маҳсулотлари ҳамда бошқа халқ истеъмоли маҳсулотларини улгуржи, майда улгуржи, чакана савдо орқали сотиш;

савдо-воситачилик фаолиятини ташкил етиш, маркетинг ва реклама хизматлари кўрсатиш;

глобал, локал ва ички компьютер тармоқлари коммуникация ҳамда алоқа воситалари, шу жумладан интернет соҳасида провайдерлик ва операторлик фаолияти;

радио, телефон, телевизор, компьютерларни таъмирлаш устахоналарини очиш ҳамда уларни таъмирлаш;

риелторлик фаолияти, кўчмас мулк объектлари, ускуналар ва мулкни сотиб олиш, експлуатация қилиш, ижарага бериш ва сотиш;

автомобилларни таъмирлаш хизматини ташкил етиш ва амалга ошириш, автомобиллар, транспорт воситалари, қишлоқ хўжалиги ва бошқа техникаларни таъмирлаш ва техник хизмат кўрсатиш;

лотереялар таъсис етиш, чоп етиш, сотиш ҳамда лотерея ва кўрик-танловларни ўтказиш;

улгуржи ва чакана савдо;

автомобил транспортида йўловчиларни ва юкларни шаҳарда, шаҳар атрофида, шаҳарлараро ва халқаро йўналишлар бўйича ташиш (Логистика хизмати);

аудиовизуал асарларни, фонограммаларни ва ЕҲМ учун яратилган дастурларни такрорлаш, реализация қилиш, прокатга бериш;

турли ташкилотлар фойдасига тўловларни қабул қилиш (ДСИ мисол);

авиа – темир йўл чипталарини сотиш ва Жамият қонунчилик билан тақиқланмаган, шу жумладан Уставда кўрсатилмаган ҳар қандай фаолиятни амалга оширишга ҳақлидир. Махсус рухсат (лицензия)ни талаб қиладиган фаолиятнинг алоҳида турлари билан Жамият фақат лицензияни олгандан сўнггина шуғулланишга ҳақлидир. Юқорида кўриб ўтганимиздек почта алоқаси корхоналари тадбиркорлик соҳасида кўрсатиши мумкин бўлган бир қанча фаолиятлар келтириб ўтилган.

Ушбу фаолиятларни амалга ошириш учун энг аввало чуқур ўйланган маркетинг тадқиқотларини олиб бориш зарур бўлади. Биламизки, почта алоқаси тармоқлари бутун Республика ҳудудида ёйилган бу почта алоқасининг имкониятларини оширишга хизмат қилади. Бу кенг ёйилган тармоқлардан самарали фойдаланиш учун албатта жамиат имкониятларини чуқур мухокама қилган ҳолда иш олиб бориши мақсадга мувофиқдир. Бугунги кунда тадбиркорлик соҳасида ушбу фаолиятларни амалга қўллаш орқали жамиат даромадини ва ишчи кучини ошириш мумкин.

РОЛЬ СОЦИАЛЬНОГО ПАРТНЁРСТВА В ОКАЗАНИИ СОДЕЙСТВИЯ ЗАНЯТОСТИ И ТРУДОУСТРОЙСТВУ ВЫПУСКНИКОВ ПРОФЕССИОНАЛЬНЫХ КОЛЛЕДЖЕЙ

Гаппаров Ш.Х.

ассистент, Термезский государственный университет

Хусанбоева Х.С., Турсунова З.Э.

студенты Ташкентского института инженеров ирригации и механизации сельского хозяйства (ТИИИМСХ, Ташкент, Узбекистан)

Важным условием развития Узбекистана является формирование совершенной системы подготовки кадров на основе богатого интеллектуального наследия народа и общечеловеческих ценностей, достижений современной культуры, экономики, науки, техники и технологий» Содействие занятости и трудоустройству молодежи может быть организовано по нескольким направлениям:

1. Образование молодежи.

- проблема комплексная, ее решение предполагает взаимодействие и сотрудничество разных структур: государственных органов власти, службы занятости населения, сферы образования и комитетов по делам молодежи.Одним из направлений деятельности является содействие дополнительному образованию молодежи через организацию и функционирование и центров дополнительного образования. Чтобы предотвратить надо, корректми написать “ые трудоустроенных” необходимо вести систематическую проф ориентационную работу с абитуриентами, которая должна содействовать личности в профессиональном самоопределении с учетом не только потребностей и возможностей, но и ситуации на рынке труда.

Программа «Эффективное поведение на рынке труда» рассчитана уже на более взрослую категорию молодежи (18-23 года), т.е. на выпускников профессиональных учебных заведений. Она предлагает активные формы обучения навыкам эффективного поведения на рынке труда. Основная проблема выпускников не в том, что они получили несоответствующее образование, а в том, что они не умеют грамотно строить отношения с работодателем при трудоустройстве. Известно, что работодатели охотнее берут на работу коммуникабельных, уверенных в себе, инициативных людей, а самой главное - умеющих творчески подходить к решению проблем. Данная программа определяет не только практический опыт трудоустройства, но и повышает личные качества молодых людей, т.е. делает их более конкурентоспособными на рынке труда.

Реализация данных программ дает молодежи возможность эффективно адаптироваться к современным условиям рынка труда.

2. Содействие профессиональной подготовке молодежи. В системе мер социальной защиты населения от безработицы важное место занимает право молодежи на бесплатную профессиональную подготовку, повышение квалификации и переподготовку по направлению органов службы занятости.

Профессиональная подготовка, переподготовка и повышение квалификации безработной молодежи осуществляются в образовательных учреждениях профессионального и дополнительного образования, учебных центрах органов службы занятости, образовательных подразделениях организаций или в иных учебных заведениях в соответствии с заключаемыми

органами службы занятости договорами. Право в приоритетном порядке пройти профессиональную подготовку, переподготовку и повышение квалификации имеют молодые инвалиды, длительно не работающие граждане (по истечении шестимесячного периода безработицы), уволенные с военной службы, выпускники образовательных учреждений, а также граждане, впервые ищущие работу (ранее не работавшие) и при этом не имеющие профессии (специальности), и др. Эффективность системы профессионального образования молодежи подтверждается высокой долей трудоустройства по окончании обучения граждан.

3. Изменение порядка приема молодежи на работу. Работодатели сегодняпредъявляют завышенные требования к молодым специалистам. Многие компании не видят перспектив применения труда подростков и молодежи и относятся к их способностям и возможностям с большим неуважением, не ви-

дят для них условий карьерного роста в рамках своего предприятия. Следовательно, основной мерой по социальной поддержке молодежи может стать смягчение критериев приема на работу, трудоустройство без опыта работы, создание гибкого графика работы для студентов дневной формы обучения и др. Сегодня есть возможность совместить вторичную занятость несовершеннолетних с ориентацией на будущую профессию. При разумной организации данная форма занятости молодежи может быть экономически выгодна компаниям и предприятиям и ориентирована на выполнение социальных функций. Социальный эффект от реализации программы вторичной занятости подростков может полностью оправдать экономические затраты на ее реализацию, поскольку приобщение подростков к трудовой деятельности, безусловно, оказывает позитивное влияние.

Развитие предпринимательской деятельности. В системе занятости молодежи характерной является частичная или скрытая безработица, когда работодатель дает возможность трудиться неполный рабочий день, неделю или официально не регистрирует работника. По мнению многих специалистов, для нормализации ситуации в области занятости населения требуется развитие предпринимательства, особенно в малых городах и сельской местности. Малый и средний бизнес во многом инициирует появление дополнительных рабочих мест, способствует деловой активности граждан, в том числе и тех, кто менее конкурентоспособен на рынке труда.

Организация ярмарок вакансий.

В целях оказания гражданам дополнительных услуг по содействию в трудоустройстве в ходе сотрудничества с работодателями служба занятости организует ярмарки вакансий. Данная форма работы дает возможность любому желающему ознакомиться с банком данных свободных рабочих мест, самостоятельно подобрать себе работу и в ходе непосредственного общения с работодателем выяснить варианты и условия трудоустройства. В последнее время широкое распространение получили мини-ярмарки, специализированные ярмарки для определенных групп населения (молодежи, инвалидов, специалистов в определенной сфере трудовой деятельности, высококвалифицированных работников и т.д.).

Создание специальных молодежных организаций для решения проблемы занятости. Сегодня социальные предприятия для молодых людей – реальное явление на молодежном рынке труда. Несмотря на то, что действуют они в различных секторах и отраслях экономики, решаемые ими задачи дают основание выделить данные предприятия в отдельную категорию.

При создании социальных предприятий приходится преодолевать целый ряд проблем, связанных с неопределенностью их правового статуса. Вместе с тем одной из задач создания данных организаций является выполнение важнейших социальных функций (увести подростков с улиц, снизить напряженность в молодежной среде и др.). Создание рабочих мест для подростков и молодежи дает им возможность сочетать работу с учебой, определиться с выбором профессии, приобрести опыт трудовой деятельности. Организуя подготовку и обучение молодых работников, предприятие как бы включается в реализацию социальной молодежной политики. Поэтому важно создавать и развивать такие механизмы, которые позволили бы молодежи не только зарабатывать, но и учиться новой, интересной профессии, приобретать знания и опыт. Когда подросток приобретет необходимые навыки, сформируется и профессионально, и психологически, он может стать полноценным участником рынка труда.

Применяются разнообразные формы организации рабочих мест для учащихся, такие как создание некоммерческих предприятий и организация социальных производств на базе учебных заведений.

Правовое регулирование молодежной политики.

Необходимость формирования современной законодательной базы в области государственной молодежной политики определяется сохранением, а нередко и нарастанием целого ряда социальных проблем молодежи, что негативно отражается на социально-экономическом и культурно-духовном аспектах ее жизнедеятельности и перспективах ее развития. Предпринимаемые меры по повышению образовательного уровня молодежи, ее трудоустройству, решению жилищных проблем, развитию разносторонних способностей молодых людей недостаточно эффективны в силу слабой координации этих мер, их частичного характера и недостаточной правовой обеспеченности.

INVESTIGATION OF TECHNOLOGICAL UNIVERSITY STUDENTS' USE OF METACOGNITIVE READING STRATEGIES IN FIRST AND SECOND LANGUAGES

Курбанова Мунаввар Эсоналиевна

Ассистент кафедры иностранные языки

Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Abstract*: Reading, whether the reader's First language, L1 or Second language, L2, is a cognitive enterprise, and it can be treated as a result of the interaction among the reader, the text, and the context. Metacognitive strategies refer to the behaviours applied by learners to plan, arrange, and evaluate their learning.*

Reading is referred as a decoding process for the purpose of extraction of meaning from written texts (McDonell, 2003). Whether in L1 or L2 context, reading includes readers, texts, and the interaction between readers and texts (Seng & Fatimah, 2006) and all the activities are defined to as reading strategies or reading skills. Readers are required to use their prior knowledge, culture background, and skilled readers typically know how to identify the strategies they use and what kinds of strategies they use in certain conditions (Carrel, 1988; Pritchard, 1990). The awareness and monitoring in learning is often defined to in the literature as "Metacognition". More and more studies have focused on the significant role of metacognitive strategies in reading (Lengkanawati, 2004; Oxford, 1990; Phakiti, 2003; Taraban, Rynearson, & Kerr, 2004). Metacognitive strategies refer to the behaviours applied by learners to plan, arrange, and evaluate their learning (Oxford, 1990). The awareness and use of these strategies is regarded as one of the significant elements in upgrading reading comprehension and successful learning (Alexander & Jetton, 2000). In Taiwan, Chinese is the native and first language while English is the second language which is taught from elementary school up to high school. In comparison to the familiarity in the students' use of Chinese, the language which the students grew up with and has been practicing in everyday lives, most students' English learning experiences and usage focus only on the preparation for examinations.

Reading, whether in L1 or L2, is a cognitive enterprise; however, comparing the reading activities in L1 and L2 reading, Singhal (1998) stated that "reading in a second language was often viewed as a slower version of doing the same task in the native language. Such comparisons, however, imply that second language tasks are mapping tasks – that is, replacing one mode of behavior with another." Readers are inclined to apply the strategies they are familiar with in reading their native language (L1) to second or foreign languages (L2) reading. Singhal (1998) discussed the differences and similarities of L1 and L2 reading in terms of three cultural differences: content (background knowledge) schema, formal (textual) schema, and linguistic (language) schema. Enright, Grabe, Koda, Mosenthal, Mulcahy-Ernt, and Schedl (2000) described that L2 reading differs from L1 reading in three ways: firstly, L2 readers establish prior L1 reading experience; secondly, learners' reading processes are cross-linguistic, involving two or more languages; thirdly, the reading instruction usually starts before adequate oral proficiency in the target language has developed.

Metacognition was first introduced by Flavell (1976), and defined as one's ability to understand, control, and manipulate his own cognitive process to maximize learning. Flavell (1979) described the process of cognitive monitoring as occurring through the actions and interactions of four interrelated phenomena: metacognitive knowledge, metacognitive experiences, goals (or tasks), and actions (or strategies). In terms of metacognitve knowledge, Wenden (1998) underscores its important role in the self-regulation of learning as language learners plan, monitor, and evaluate their learning. It is believed that metacognition is basically essential in various aspects of language learning, such as oral, reading, writing, and language acquisition. As metacognition relates to reading process and self-control mechanism for monitoring and enhancing comprehension, studies proved that it was the significant component in L1 as well as L2 reading (Guo & Roehrig, 2011; Sheorey & Mokhtari, 2001).

Reading in both L1 and L2 involves the interaction of many variables, and readers use mental activities to develop reading skills or strategies to construct meaning from the text. As previous studies suggested that the

reading comprehension can be enhanced through systematic instruction of metecognitive reading strategies (Cubukcu, 2008), instructors might consider designing the specific training programs to meet the individual's needs for improving the learning outcome. Besides that, learning motivation is certainly another important factor influencing the application of reading strategies; how to encourage the low-achieving learners to develop the reading strategies systemically and appropriately challenges all the language educators. Furthermore, with the limitation of the small sample used in this research, it might not be able to represent the real situation. We hope to repeat the survey with larger samples and conduct individual interview for more detailed investigation. Future study will also evaluate if there is any correlation between learners' application of metacognitive reading strategies and their learning performance in L1 and L2 academic reading.

THE USE OF FIRST LANGUAGE IN THE SECOND-LANGUAGE CLASSROOM: A SUPPORT FOR SECOND LANGUAGE ACQUISITION

Курбанова Мунаввар Эсоналиевна

Ассистент кафедры иностранные языки

Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

***Abstract**: This action research project was carried out in order to identify the role of first language in the second-language classroom. This study was conducted in a Colombian international school with an English immersion program for kindergarten students attending their first year of school. The purpose of this study was to identify if the use of the mother tongue in the classroom increases comprehension and facilitates the second language acquisition process. Two lesson plans were designed: the first one using only English as the language of instruction, and the second one using both languages, Spanish and English. The results demonstrate that students do benefit from the use of the first language in the classroom, transferring concepts from their mother tongue to the new language.*

As globalization and population movements are increasing, different cultures come into greater contact with each other, resulting in the need for communication between societies (Hamers & Blanc, 2000). Thus, being bilingual has become a vital aspect for becoming a successful professional, making bilingualism the main component in education. In fact, a bilingual person has more opportunities to obtain a better job and to have more achievements than a monolingual person. Therefore, elementary schools, high schools, and universities have to face the need for bilingualism by educating students who are able to work in these multicultural societies. If students receive bilingual education from their first years of school, the level of proficiency in the second language should increase.

That is why today, teachers in bilingual schools and language teachers are challenged to teach children to help them reach the level of proficiency required for learning demanding academic content and ensuring complete cognitive development. Cognitive development is understood in this study as the construction of thought processes, including problem-solving, decision-making, reasoning, and language development (Piaget & Inhelder, 1969).

Furthermore, as we are talking about kindergarten students starting their literacy process, it is important to take into account the stages of language development. In fact, during the first stages of language acquisition it is important to constantly refer to the mother tongue in order to make connections (Cummins, 2001). Previous knowledge in kindergarten students is a starting point for acquiring a new language, leading to language transfer (Baker, 2001). Language transfer is understood as the use of the first language during the second language acquisition, which represents the first stage of language acquisition (Krashen, 2003).

Moreover, during the first year of school it is vital that the first language is developed in students. In fact, first

language development is required in order to have good strategies to transfer to the new language. If students do not have good strategies in their mother tongue, they will not have good strategies to transfer to the new language, and therefore the cognitive development will be reduced (Friedlander, 1997). Due to the importance of first language development, the school in this study has now increased the number of Spanish hours in kindergarten.

First of all, students were more engaged during the activity that used code switching. Their level of participation was higher, which made room for teachers to connect with other activities and deepen understanding. When students are engaged, the lesson runs in a smoother and positive way, and therefore the teacher and students can make the most of every activity, thus enriching learning.

This study focused on the importance that the first language has during the second language acquisition process. Nowadays, bilingualism is a key factor in becoming a successful professional, and thus, bilingualism has become the main component in education. Many theories debate the way in which a second language should be taught. This study was conducted at an immersion international school in Bogotá, and the results demonstrated and supported Cummins' theory: the development of the first language during the first year of immersion school benefits the second language acquisition process. In fact, the theory suggests that even if the two languages are visually different, they do operate through the same processing system. In all learning situations, previous knowledge is a starting point for acquiring a new language (Cummins, 2000). However, even if there were no main differences in students' understanding between the two activities, it was demonstrated by teachers' opinions that students with a more developed mother tongue and with more concrete concepts seem to transfer their experiences to the new language, making the second language acquisition process easier.

References

1. Baker, C. (2001). Cognitive theories of bilingualism and the curriculum. In Baker, C. (3rd ed.) Foundations of bilingual education and bilingualism,163-180. Clevedon: Multilingual Matters Ltd.
2. Benson, C. (2002). Transfer/cross-linguistic influence. English Language Teachers Journal, 56(1, 68-70.
3. Beardsmore, H. B. (1986). Bilingualism: Basic principles. Clevedon: Multilingual Matters.
4. Burchinal, M., Field, S., López, M. L., Howes, C., & Pianta, R. (2012). Instruction in Spanish in pre-kindergarten classrooms and child outcomes for English language learners. Early Childhood Research Quarterly, 27, 188-197.
5. Cárdenas-Hagán, E., & Carlson, C. D. (2007). The cross-linguistic transfer of early literacy skills: The role of initial L1 and L2 skills and language of instruction. Language, Speech, and Hearing Services in Schools, 249–259.
6. Cummins, J. (2000). Language, power and pedagogy: Bilingual children in the crossfire. Clevedon: Multilingual Matters.
7. Dixon, Q. L., Zhao, J., Shin, J. Y., Su, J. H., Burgess-Birgham, R., Gezer, M. U. & Snow, C. (2012). What we know about second language acquisition: a ynthesis from four perspectives. Review of Educational Research, 82(5), 5-60

ОРГАНИЗАЦИЯ ВИРТУАЛЬНОГО СПРАВОЧНО-БИБЛИОГРАФИЧЕСКОГО ОБСЛУЖИВАНИЯ В УЗБЕКИСТАНЕ

Ануфриева Юлия Геннадьевна

ассистент кафедры "Информационно-библиотечные системы" Ташкентского университета информационных технологий им. М.Ал-Хорезмий

Традиционные формы обслуживания в информационно-библиотечных учреждениях не теряют свою актуальность, но внедрение информационных технологий способствует постоянному изменению информационной среды и средств доступа к информации.

Свидетельством изменений в традиционном справочно-библиографическом обслуживании являются создаваемые в информационно-библиотечных учреждениях виртуальные справочные службы (ВСС). Они ориентированы на обслуживание удалённых пользователей и предоставление в ответ на запросы готовой информации как в виде ссылок на имеющиеся сетевые ресурсы, так и в привычной для пользователей форме - в виде библиографических списков и фактографических данных. Создание таких справочных служб объясняется объективными причинами: увеличением Интернет-ресурсов, которые используются при выполнении запросов пользователей; формированием новой пользовательской аудитории, испытывающей потребность в круглосуточном доступе к электронным каталогам информационно-библиотечных учреждений, получении электронных копий документов и помощи высококвалифицированных библиографов.

Виртуальное справочно-библиографическое обслуживание (ВСБО) как инновационный метод оказания библиотечных услуг в информационно-библиотечных учреждениях (ИБУ) является одним из приоритетных направлений организации деятельности ИБУ.

Виртуальное библиотечное обслуживание – программно-технологический комплекс, размещенный на web-сайте библиотеки и предназначенный для предоставления услуг по индивидуальным запросам пользователей, находящихся за ее пределами. [1]

С учетом сложившейся практики можно констатировать, что в настоящее время по целевому назначению виртуальное обслуживание может быть ориентировано на решение следующих задач в сфере обслуживания пользователей: приоритетное выполнение запросов и информирование по социально значимым темам; предоставление библиографической и фактографической информации по персонифицированным запросам; предоставление электронных копий документов.

Каждая из указанных задач решается с помощью определенного типа виртуального обслуживания. (рис. 1)

Рис. 1. Соотношение задач обслуживания и типов виртуального обслуживания

Наряду с международными документами в Узбекистане применяются и национальные нормативные документы (законы, постановления, указы, положения):

Закон Республики Узбекистан “Об информационно-библиотечной деятельности” от 13 апреля 2011 г. № ЗРУ- 280, целью которого является регулирование отношений в области информационно-библиотечной деятельности. [2]

Закон Республики Узбекистан «Об авторском праве и смежных правах», целью которого является регулирование отношений, возникающих в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), исполнений, фонограмм, передач организаций эфирного или кабельного вешания (смежные права). [3]

Внедрение ИКТ в деятельность информационно-библиотечных учреждений, создание цифровых библиотек, которые в ближайшее время позволят сформировать глобальный информационный ресурс, стимулирование поэтапного развития онлайнового открытого доступа к научным знаниям и культурному наследию послужило Постановление Президента Республики Узбекистан «О мерах по дальнейшему качественному развитию информационно-библиотечного и информационно-ресурсного обслуживания на базе информационно-коммуникационных технологий на 2011–Положение «О виртуальной справочной службе Национальной библиотеки Узбекистана имени Алишера Навои». Настоящее положение содержит в себе 6 разделов: общие положения, основные принципы обслуживания, содержание обслуживания, режим и порядок работы, ресурсная база, контроль и ответственность за выполнение работ.

Положение «О службе координации электронных заказов и дистанционной доставки ресурсов в Национальной библиотеке Узбекистана», в нем изложены общие положения, задачи и функции службы, показана структура и права службы, определены обязанности руководителя службы, и взаимоотношение с другими подразделениями библиотеки.

Основополагающие документы по виртуальному справочному обслуживанию носят рекомендательный характер, обозначают общие стандарты организации виртуального справочно-информационного обслуживания, предлагают модель виртуальной справочной службы, окажут неоценимую помощь при разработке собственного проекта виртуальной службы ИБУ. В Узбекистане в последние годы в крупных информационно-библиотечные учреждениях организована работа виртуального справочного библиографического обслуживания. (рис. 2.)

Рис. 2. Виртуальное справочно-библиографическое обслуживание в ИБУ Узбекистана

Изучая отечественный опыт можно отметить, что на сайте Национальной библиотеки представлены для пользователей ресурсы библиотеки в виде виртуальной выставки, такие как: Книги – юбиляры 2017 года, Тематические виртуальные выставки

Сборник уникальных произведений узбекского поэта Алишера Навои, Сборник трудов первого Президента И. А. Каримова, Труды и доклады Президента Республики Узбекистан Ш. М. Мирзиёева. Также в Национальной Библиотеке функционирует Виртуальная справочная служба. Пользователи могут получить ответ на любой интересующий его вопрос, ответ на вопрос отправляется в течение 2-3 рабочих дней на указанную почту пользователя. [5]

Ферганский областной информационно-библиотечный центр (далее ИБЦ) им. А. Фаргони организовал работу виртуального справочно-библиографического обслуживания и постоянно совершенствует работу в этом направлении. На сайте ИБЦ функционирует раздел «Интерактивные услуги», который включает в себя: Виртуальную справочную службу «Спроси библиотекаря», «Онлайн консультацию», «Заказ электронной копии документа», «Онлайн - информирование пользователей» и «Виртуальную приёмную директора ИБЦ». В разделе Виртуальной справочной службы можно задать вопрос о наличии в фонде ИБЦ определенного издания, узнать, в каком отделе ИБЦ оно хранится, уточнить данные о книге или статье, выяснить конкретные фактографические сведения. В зависимости от сложности вопроса ответ пользователю может прийти в течение 1-3 дней.

В разделе Онлайн консультации можно обратиться к дежурному библиографу за консультацией в режиме реального времени. Раздел Заказ электронной копии документа позволяет заказать электронные копии печатных документов из фонда библиотеки. Услуга работает на платной основе. В разделе Виртуальная приёмная директора ИБЦ у пользователей есть возможность высказывать свое мнение, оставлять комментарии, пожелания и предложения в адрес ИБЦ и сайта, посетив раздел "Гостевая книга".[6]

В заключении активное использование пользователями ИБУ услугами виртуального справочного библиографического обслуживания позволит расширить сферу деятельности ИБУ, оптимизировать условия взаимодействия с пользователями и другими учреждениями и удовлетворять их запросы.

Использованные источники:

1. Долгополова, Е. Е. Обслуживание пользователей в электронной информационной среде / Е. Е. Долгополова // Інфармацыйныя рэсурсы Нацыянальнай бібліятэкі Беларусі: праблемы фарміравання і выкарыстання : зб. арт. / Нац. б-ка Беларусі ; [склад. Т. В. Кузьмініч ; рэдкал.: Л. Г. Кірухіна і інш.]. – Мінск, 2008. – С. 82–89.
2. Об информационно-библиотечной деятельности: Закон Республики Узбекистан от 13 апреля 2011г. № ЗРУ- 280. // Новости Узбекистана. – 2011. - 14 апреля.
3. Об авторском праве и смежных правах: Закон Республики Узбекистан от 20 апреля 2006 г. № ЗРУ-42. // Новости Узбекистана. – 2006. - 21 июля.
4. О мерах по дальнейшему качественному развитию информационно-библиотечного и информационно-ресурсного обслуживания на базе информационно-коммуникационных технологий на 2011–www.natlib.uz - Сайт Национальной библиотеки Узбекистана имени Алишера Навои.
5. www.ru.ferlibrary.uz – Сайт Ферганского областного информационно-библиотечного центра имени Ахмада Фаргоний.

ОБРАЗОВАНИЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Абдурахимова С.В.

Ст.препод.каф.АВТ ТУИТ

Применение компьютерной технологии обучения в учебном процессе на современном этапе заключается в использовании компьютеров как средства обучения не эпизодически, а систематически с самого начала обучения и до последнего занятия при изучении любого предмета. Основная проблема при этом заключается в методике компьютеризации курса, который предстоит освоить обучаемому. Возможна либо полная перестройка и ориентация на создание новых компьютеризованных курсов, либо реализация методики с частичной компьютерной поддержкой курса.

Когда речь идет об освоении аудиовизуальных дисциплин все приобретает еще большую значимость. Необходимость в слуховом и визуальном контроле материалов, представляемых преподавателем, просто обязательна. Что влечет за собой необходимость дополнительного оборудования: Звуковых карт, устройств видеозахвата, более мощное программное обеспечение и процессор.

При освоении лекционного материала наряду с информационно-познавательным содержанием интерактивная лекция имеет эмоциональную окраску благодаря использованию в процессе ее изложения компьютерных слайдов. Заранее готовясь к лекции, преподаватель разрабатывает на компьютере в приложении «Power Point» программы «Office» необходимое количество слайдов, дополняя видеоинформацию на них звуковым сопровождением и элементами анимации. Естественно, что это значительно повышает требования к квалификации преподавателя. Он должен обладать необходимым уровнем знания компьютерной техники и владеть навыками работы с программным обеспечением. Важным условием проведения интерактивной лекции является также наличие специализированной аудитории, оснащенной компьютерной техникой и современными средствами публичной демонстрации визуального и звукового учебного материала. В процессе изложения лекции преподаватель эпизодически представляет информацию на слайде в качестве иллюстрации. Это способствует лучшему усвоению учебного материала студентами.

Таким образом, участие в процессе обучения одновременно педагога и компьютера значительно улучшает качество образования. Использование предложенной методики активизирует процесс преподавания, повышает интерес студентов к изучаемой дисциплине и эффективность учебного процесса, позволяет достичь большей глубины понимания учебного материала. С одной стороны, сотрудничество преподавателя и компьютера делает учебную дисциплину более доступной для понимания различными категориями студентов, улучшает качество ее усвоения. С другой — оно предъявляет более высокие требования к уровню подготовки преподавателя и его квалификации, который должен уже не только владеть традиционными методиками преподавания, но и уметь модернизировать их в соответствии со спецификой обучаемых, используя современные достижения науки и техники.

Прежде всего, повышается интерес студента к такому занятию. Психологи отмечают, что современная молодежь информационного общества – это дети экранной динамичной информации. Информация на экране монитора, проектора или телевизора воспринимается ими намного лучше, чем печатная книжная информация. Конечно, печально осознавать, что современные студенты очень мало читают, однако, при подготовке к занятию необходимо учитывать данный фактор.

Компьютер, укомплектованный звуковой картой, колонками, видеопроектором, позволяет сделать занятие живым и красочным. На качественно новом уровне реализуется принцип наглядности обучения.

Анимация, видеоизображение, звук делают изучаемые события и явления более наглядными, а, значит, и доступными, таким образом превращая процесс обучения в более комфортный для ученика. Использование ИКТ на занятии позволяет рационально организовать рабочее время преподавателя и студентов на уроке, т.к. преподавателю не потребуется писать на доске мелом, отвернувшись от студентов, развешивать иллюстрации, менять демонстрируемый материал и т.д. Заранее подготовленная информация к занятию появляется в нужно время, в эстетической форме, в заранее продуманном темпе и объеме. Время, сэкономленное на занятии, может использоваться для увеличения объема информации или тренировочных упражнений.

Проблемой является и создание видеопособий по технологиям производства аудио видео продукции. Одному преподавателю сложно создать необходимое количество электронных уроков по несколь-

ким предметам и на все количество тем, входящих в курс. Поэтому на нашем факультете мы стараемся создавать такие уроки с помощью наших студентов, задавая им в качестве выпускной работы создание электронных пособий или видео уроки, которые в последующем пригодятся при обучении следующих поколений студентов.

Каждый год перед нами вплотную стоит вопрос по созданию новых тем для выпускных работ, а каждая такая тема дает толчок в создании новых технологий создания аудио видео продукции, новых направлений развития и обучения студентов.

Сейчас теоретики высшего образования считают, что термин «образовательные технологии» сегодня не совсем адекватен. Чаще, как правило, говорят об информационных технологиях, о компьютерных технологиях, чуть реже — о коммуникационных технологиях, и совсем редко — это уже предмет специальных обсуждений — об аудиовизуальных технологиях. Представляется необходимым рассматривать информационные, коммуникационные и аудиовизуальные технологии в совокупности, как подчиненные решению более важной задачи — созданию новой образовательной среды, где информационные, коммуникационные и аудиовизуальные технологии органично включаются в учебный процесс для реализации новых образовательных моделей.

Сегодня проблема образования в целом — это проблема не технологий, а человека, преподавателя, который приходит в аудиторию. Именно преподаватель является слабым звеном с точки зрения информационных технологий. Кроме того, большинство из работающих в вузах специалистов часто вообще не имеют педагогического образования.

В нашем университете это связано с необходимостью специальных знаний, преимуществом же является изучение именно информационных и, в частности, телевизионных технологий. То есть и студент и, конечно, преподаватель в этой области уже подкован.

Создавая видео и аудио продукцию наши студенты должны освоить приемы монтажа изображения и звука, освоить приемы съемок и звукового оформления. Научиться работе с музыкой, начиная от умения подобрать подходящую к изображению и, кончая, умением создавать какие- то мелодии в компьютерных программах, которые мы изучаем на наших занятиях.

Интересным нам кажется создание видеоряда под определенную музыку, а не наоборот, как обычно бывает, подбирается или пишется музыка под уже смонтированное изображение. Здесь же мы сначала подбираем понравившуюся музыку, а затем представляем видео образы, навеянные данным музыкальным произведение. При таком способе мы полностью зависим, а значит и развиваем образное мышление студентов.

Объединить творчество и технику, технологии при создании аудио и видео продукции наша задача. Заинтересовать студентов творчеством, а создавать аудио и видео продукцию, при нынешнем развитии техники, можно чем угодно, вплоть до личного телефона.

Конечно, освоить все эти дисциплины без компьютера и программ нелинейного монтажа было бы абсолютно невозможно.

Поэтому главное внимание в системе образования должно быть в первую очередь направлено на педагогическую подготовку преподавателей предметников. Совместив педагогическое образование и образование в области новых информационных технологий, можно будет обеспечить прорыв в создании новой образовательной среды.

INFORMATION MODEL FOR ARCHIVES

Ishniyazov Odil Olimovich

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

assistant, Basic of Informatics

Anufriyeva Yuliya Gennadevna

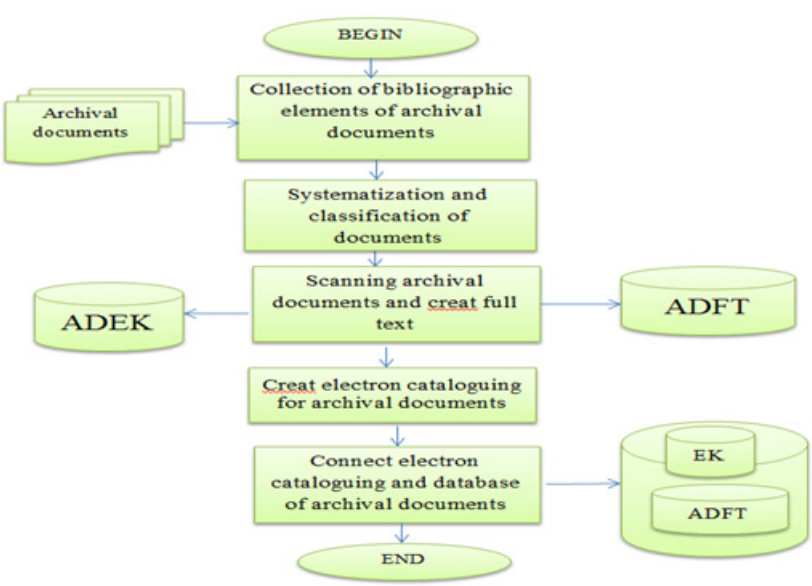
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

assistant, information and library science

In order to present the information models and algorithms for processing of archival documents, we introduce some basic concepts.

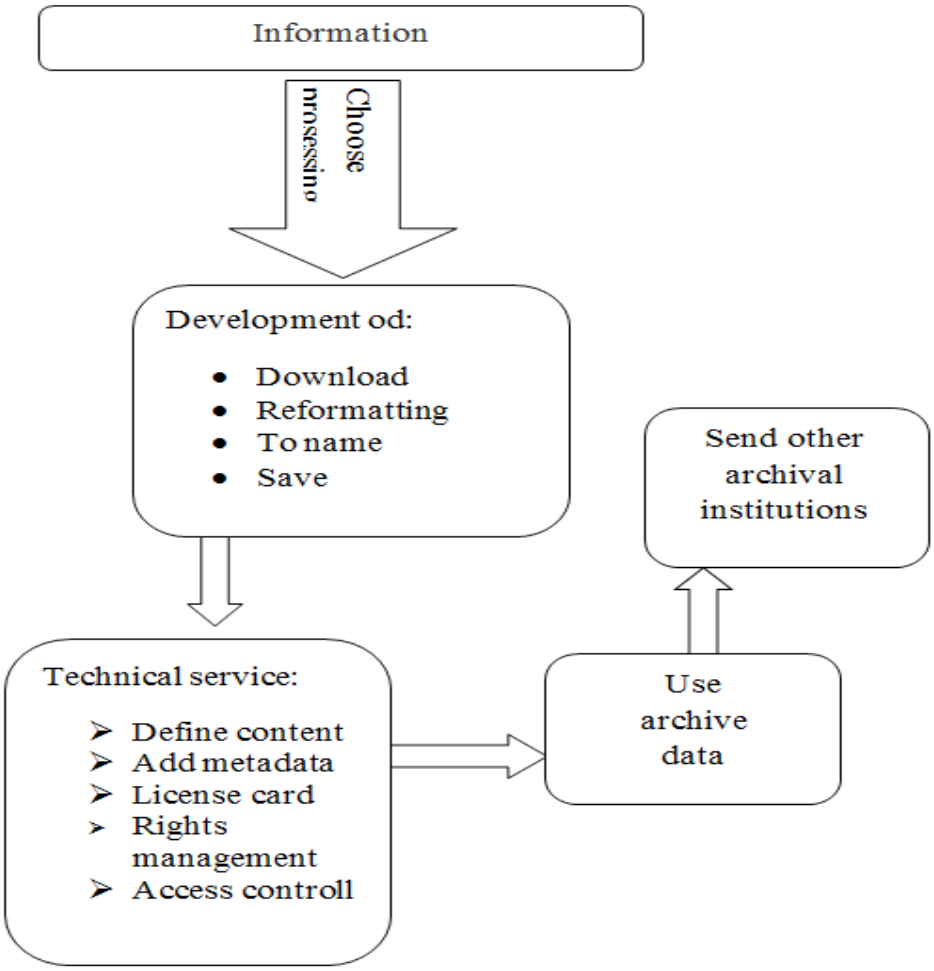
Information model - object model presented in the form of information that describes essential for the consideration of options and variables of the object, the connection between them, the inputs and outputs of the object and allows by applying a model of information about changes of the input variables to simulate the possible states of an object.

Archival documents - material carrier with fixed on it information, which has details that enable him to be identified, and shall be kept because of the importance of these media and information for citizens, society and state.



1- Block-scheme. Information medel of creat electron archive documents in archival institutions.

Information model of exchange, collect and transmission of data in archival institutions



2- Block-scheme. Information medel of exchange, collect and transmission of data in archival institutions.

The concepts of infological and datalogical data models were introduced by Langefors in a series of publications starting in 1963. Infological data models represent information in ways that are supposed to be similar to how people perceive the information (infological realm), without considering their final computer-related representations (data- logical realm). The ideal situation for an information system designer is to have a powerful infological data model that can be easily communicated between humans, and that there is a way to perform a non-loss translation of this infological data model into the datalogical realm.

Infological data model

In the early theoretical work on infological data models, the concepts of object, property, relationship and time were identified as basic. An elementary fact is in this framework represented as a triple (a collection of objects + a property or relationship + time), called an elementary constellation.

Structured textual descriptions (natural language), formal logic (specification in for instance the logic-based programming language Prolog) and other structural tech- niques (with visualisation through diagrams) have been proposed as infological data models.

Structured textual descriptions can express things in a human readable format, but have severe limitations when it comes to data structuring and formalisation for translation into the datalogical realm.

Logic has the advantage of being a formal description, having its roots in mathematics. It is therefore more easily translated into the datalogical realm. A problem is that logic lacks mechanisms for efficient communication of structure.

Diagrams have the advantage that they can show structure (relationships) in a human readable way (usually as two-dimensional maps), and diagrams have therefore become very popular for “semantic” data modelling. A problem with diagrams is that they can be difficult to translate into the datalogical realm, and there is a limit to the amount of information that can be put into a diagram without making it difficult to comprehend.

Semantic data models introduce many useful methods for data structuring and abstraction, and constitute the most interesting branch of infological data models for database modelling. In this chapter, the ER model and an

EER model are described to give a background in high level data modelling.

Infological carry out data analysis and define objects. The purpose infological simulation - providing the most natural for the human ways of collecting and presenting the information that is supposed to be stored in the created database. Therefore infological need to build a data model similar to natural language (the latter can not be used alone because of the complexity of computer word processing, and any ambiguity of natural language). Define the main structural elements Infological model: Essentially, the connection between them and their properties (attributes).

The analysis of documents flow in the organization of the following basic essence of the model have been identified: the document and the employee. Special attention should be paid to the essence of "worker". Since every employee can have different attitudes to the document, it is necessary to distinguish two subentity: the sender and the recipient.

Consider the attributes of certain entities:

1. Document. It is the core essence of the system and has the following attributes:
- author (sender, recipient) of the document;
- the date of creation / sign the document;
- period of execution;
- importance;
- Status of implementation;
- a type;
- document file;
- Document the parent (this attribute is optional, is used to track the responses of the tree).

2. Worker. It is also the core essence.
- Full Name;
- unit;
- status within the division.

REFERENCES

1. Semantic Database Modeling: Survey, Applications, and Research Issues" Richard Hull, Roger King ACM Computing Surveys, vol.19, no.3, Sept. 1987, pp. 201-260

2. Data Models" Dionysios C. Tsichritzis, Frederick H. Lochovsky Prentice Hall, Inc., 1982

ЭКОЛОГИК МАДАНИЯТ ВА АХБОРОТ-КУТУБХОНА МУАССАСАЛАРИ

Маҳмудов Мирали Хайдарович

Мухаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети

“Ахборот-кутубхона тизимлари” кафедраси доценти

педагогика фанлари номзоди

Инсоният ривожининг ҳозирги босқичида жамият ва табиатнинг ўзаро муносабатлари сиёсий партиялар, халкаро ташкилотлар, ҳукуматлар, жаҳон жамоатчилигининг кенг доиралари эътиборини тобора кўпроқ ўзига тортмоқда. Бундай эътиборнинг кучайиши фан ва техника тараққиётининг экологик оқибатларга кенг кўламли ижтимоий ёндашувининг зарурати билан боғликдир. Маълумки, фантехника инқилобининг оқибатлари кўп жиҳатдан барча мамлакатлар учун умумийдир, атроф-мухитни муҳофазалаш, илмий асосланган экология сиёсатини ишлаб чикиш муаммоларини ҳал этиш умуминсоний ёндашувни талаб қилади. Экологик сиёсат дейилганда давлатларнинг «табиат-жамият» тизимидаги ўзаро муносабатларни тартибга солишни энг қулай ва самарали амалга оширишга йўналтирилган фаолиятини тушунмоқ лозим.

Ўзбекистон Республикасининг экологик сиёсати — давлатнинг табиатни муҳофаза қилиш ва табиий ресурслардан оқилона фойдаланиш борасида олиб бораётган ички ва ташқи фаолият ўз аксини кўрсатмоқда. Кейинги йилларда экология ва табиатни муҳофаза этиш борасида ўнлаб қонунлар ҳамда фармойишлар эълон қилинди, уларнинг ижроси бўйича чора-тадбирлар белгиланди.

Маълумки, экологик маданият умуминсоний маданиятнинг бир бўлаги хисобланиб, умуммаданий нормаларга табиат билан мулоқотнинг алохида қоидаларини тарғиб этиш ҳамда инсон ва табиатнинг ўзаро муносабатларида умуммаданий нормаларни тарғиб этишни талаб қилади. Экологик маданият - бу экологик билимлар ва шахс харакатларининг уйғунлигидир. Экологик маданиятни шакллантиришда экологик таълим ва тарбия асосий омил хисобланади. Ушбу ишларни мохияти инсонда ўзини экологик тизимнинг, табиатнинг бир бўлаги деб хисоблаши уни асраш зарурлигини хис этишнинг шакллантиришдир.

Экологик таълим ва тарбиянинг асосий мақсади табиат билан инсоннинг ўзаро муносабатларда маълум бир кўникмаларни, тегишли билим ва малакаларни шакллантиришдир. Шахсни шакллантириш мақсадга йўналтирилган, тизимли жараён тарзида оила, таълим муассасалари шунингдек ахборот-кутубхона муассасалари, оммавий ахборот воситалари, табиатни асраш давлат ва жамоатчилик ташкилотларини биргаликдаги фаолиятида орқали амалга оширилади. Экологик таълим ва тарбияда оила, таълим муассасалари ва оммавий ахборот воситаларининг етакчилик ролини эътироф этиш зарур. Ёш авлодга экологик таълим ва тарбия бериш мураккаб, узок давом этадиган жараёндир. Улар табиат ҳақидаги дастлабки тасаввурларни одатда ўз оиласида оладилар ва ёшлари улғайган сари атроф муҳит ҳақидаги тасаввурлари кенгаяди, табиатга бошқачароқ назар ташлай бошлайдилар.

Илк ёшиданоқ, бола катталарнинг табиатга бўлган муносабатини кўради, эшитади, хис қилади. Катталарнинг бундай таъсири узлуксиз давом этади. Ота- оналарнинг атроф-мухит тўғрисидаги фикрлари, харакат ва холатлари болаларда жонли табиатга бўлган ҳурмат хиссини тарбиялайди.

Шунинг учун ҳам ота-оналар экологик масалалар ҳақида оддий тушунчаларга эга бўлишлари ва бола онгида табиатни севиш туйғусини шакллантиришлари шарт.

Мактаб даврида экологик таълим ва тарбия кенгайиб, бойиб боради. Чунки синфдан ташқари тадбирларда табиатшуносликка доир билимлар бериб борилади. Кейинроқ эса мактаб ўқув жараёнида экологик маълумотларни берувчи назарий фанлар ўқитила бошланади. Ҳозирги пайтда мактабларда табиат мухофазаси бўйича кенгроқ билимлар олишга мўлжалланган экологик таълим амалга оширилмоқда. Бу эса нафақат билим олишга, балки шахснинг маълум хусусиятларини ҳам тарбиялашга хизмат қилади.

Ўзбекистон Республикаси “Халқ таълими вазирлиги” томонидан дарсликлар, ўқув қўлланмалари ва ўқитувчиларга "Экология" фанини ўқитиш бўйича тавсиялар, дастурлар ҳам ишлаб чиқилди. Шунингдек доимий равишда "Гуллар ва қушлар байрами", "Табиат кеча, бугун, эртага", "Томчи сув — хаёт жилваси", "Экология бўйича иқтидорли болалар анжумани" каби кўрик танловлар ва илмий-методик конференциялар ўтказилиб келинмоқда.

Бугунги кунда олий ва урта махсус, касб ҳунар ўқув муассасаларида "Экология" ва "Атроф-мухитни мухофаза қилиш" фанлари ўқитилмоқда.

Табиатни мухофаза қилиш, ёшларга экологик, эстетик, маънавий билимларини бериш бугунги кунниng долзарб масалаларидан хисобланади. Бу масъулиятли вазифани бажаришда ахборот-кутубхона

муассасаларини ҳам ўз ўрни мавжуд. Ахборот-кутубхона муассасалари ўзига хос хусусиятлари, уларда экологияга оид адабиётлар ва маълумот базаларини мавжудлиги, улардан вақт чегараланмаган холда фойдаланиш ҳамда ушбу муассасаларда китобхонлар билан якка, гурухли ва оммавий ишлаш имкониятлари мавжудлиги, уларнинг бошқа муассасалардан фарқидир.

Ахборот-кутубхона муассасалари ўз фаолияти билан экологик таълим ва тарбия тизимини тўлдиради. Ахборот-кутубхона муассасалари ўз фаолиятини ихтиёрийлик ва қизиқишлар асосида ташкил этиб, экологик тарғибот юритишда, оммавий ахборот воситалари, интернет саҳифалари, газета ва журналлар, радио ва телевидение билан ўзаро ҳамкорликда амалга оширадилар.

Ахборот-кутубхона муассасалари китобхонларни, айниқса ёш китобхонларни бадиий, илмий-оммабоп адабиётлар орқали, табиат тўғрисидаги тасаввурлар ва илмий далиллар оламига олиб киришга, унинг бетакрор гўзалликларини кўра билишларига ёрдам беради. Ахборот-кутубхона муассасалари экологик тарбияни амалга ошира бориб, фақат табиат ва уни муҳофаза қилиш ҳақидаги адабиётларни тарғиб қилиш билан чекланиб қолмасдан, балки ёшларга жамият тараққиётининг ҳозирги босқичида экология муаммоси энг долзарб мавзу эканлигини англашга ҳам ёрдам бериши керак.

Ахборот-кутубхона муассасалари ёш китобхонлар ўртасида экологияга оид ишларни амалга ошриш жараёнида уларни ёш ва китобхонлик хусусиятларини эътиборга олишлари мухим аҳамиятга эгадир. Масалан, кичик мактаб ёшдаги ўқувчи (7-9 яшар) табиатнинг нима эканлиги ҳақида аниқ тасаввурга эга эмас, чунки унинг тажрибаси кам, тафаккури мавҳум ва оламни идрок этиши ҳали унча ривожланмаган, бироқ шунга қарамасдан унинг қалбида табиатга муҳаббат уйғотиш, унинг гўзаллигини ҳис қила билишга ўргатиш керак. Бу ёшдаги китобхонлар билн овоз чиқариб ўқишлар ва расмларни томоша қилиш каби иш шаклларидан фойдаланиш муҳим. Уларни ўқилган ва кўрилган китоблар туркум ишлар билан қўшиб олиб бориш керак.

10-11 яшар ўспиринларни жонли жонсиз табиатнинг турли-туман шакли, инсон ва табиатнинг ўзаро боғлиқлиги тўғрисидаги китоблар қизиқтиради. Шунинг учун уларга табиий бойликларнинг хилма-хиллиги ва уларнинг инсон ҳаётидаги ўрин, у ёки бу тарздаги экологик муаммолар ҳақидаги китобларни тавсия қилиш мақсадга мувофиқ бўлади. Болалар инсоннинг маънавий ҳаётида табиатнинг аҳамиятини қанча эрта тушунсалар, унга нисбатан ўйлаб ва эҳтиёткорлик билан муносабатда бўладилар.

12-13 ёш - шахснинг жадал шаклланиш даври хисобланади.Бу ёшдагилар учун экологик тарбия 10-11 ёшлилар учун каби бир хилда бўлади, бироқ улар ёрдамида ҳал қилинадиган материал анча мураккаблаштирилади. Айниқса саёҳатлар, инсон томонидан тариат қонуниятларини ўрганилаётганда илмий-билишга оид, илмий-бадиий китоб муҳим роль ўйнай бошлайди. “Ҳамма нарсани билгим келади”, “Глобус”, “Қуруқликда ва денгизда” альманахлари билан ишлаш катта аҳамият касб этади. Уларни доимо тарғиб эта бориш болаларни илмий билим берувчи китобларни ўқишга ундайди, чунки бу тўпламаларда акс эттирилган муаммоли материаллар, тахминлар шу ёшдаги болаларнинг эҳтиёжларига жавоб беради, уларнинг саргузашт, романтик қизиқишларини қондиради, олдига янгидан-янги саволларни қўяди. Шунингдек болаларни маълумотнома нашрлари билан таништиришни давом эттириш зарур: “Ҳайвонлар олами”, “Болалар қомуси”, “Ёш деҳқон қомуси”, “Ёш кимёгар қомуси” ва бошқалар. Бу ёшдаги болаларга тавсия қилинаётган бадиий асарларда инсониятнинг тинчлик учун, ерда ўсимлик ва ҳайвонот дунёсини сақлаб қолиш учун кураш ҳуқуқи акс эттирилади. Улар болаларни лоқайд бўлмасликка, эзгуликка, инсонийликка ўргатади.

14 ёшлиларнинг ўзига хос хусусияти шахснинг ижтимоий жиҳатдан вояга етишидир. Улар билан ишлаш анча мураккаблашади. Бу ёшдаги болаларга бериладиган экологик тарбиянинг мазмуни табиат ва жамиятнинг ривожланиш тарихи билан боғлиқ бўлган масалаларни ўзига қамраб олиш мумкин .Масалан: табиат қонунларининг бирламчилиги; табиат ва ундаги инсоннинг бир бутунлиги; инсоннинг табиатга таъсир кўрсатишининг моҳияти ва унинг тирикчилигининг табиатга боғлиқлиги; экологик муаммоларни ҳал этишнинг ҳозирги ва инсониятнинг келгуси тараққиёт учун аҳамияти; ва бошқалар.

Ахборот-кутубхона муассасалари китобхонларни экологик маданиятини шакллантиришда хилма-хил иш шаклларидан фойдаланмоқдалар. Улар кўргазмаларидан тортиб кўрик – танловлар ташкил этишдир. Қуйида ахборот-кутубхона муассасаларида экологик йўналиш бўйича тадбирлар ташкил этиш бўйича намунавий иш шакллари ва тахминий мавзулар келтирилган.

Кўргазмалар: Кўргазма-пейзаж “Тирик табиатнинг ранг-баранг мутаносиблиги”

Болалар расмлари ва табиий материаллардан ясалган буюмлар кўргазмаси”.

“Ажойиботларни яратилиши”. Кўргазма – кўрик “Табиат-илхом манбаи”.

Кўргазма-маслахат “Ҳар қандай мевани ювмасдан ема....., Кўргазма-диалог “Ер сайёраси”, Кўргазма-кўрик “Экология. Инсон. Жамият”, Кўргазма-викторина “Дунё катта ва ранг-баранг”, Хонаки ўсимликлар кўргазма-экспозияси “ Гуллар-табиат безаги”, “Дорихона оёғимиз остида”, “Табиат ажойиботлари”, Кўргазма-фикрлаш “Табиат бизнинг умумий дўстимиз”, Кўргазма-саёҳат “Ўзбекистоннинг қўриқхоналари бўйлаб”, “Менинг юртим”, “Дунё биз билан” расмлар кўргазмаси. Кўргазма –стенд “Кичик шаҳарнинг катта муаммолари”. Доимий китоб кўргазмаси “Экологик календарь” . Доимий экспресс-ахборот стенд “Табиат. Инсон. Жамият.

Юқоридаги кўргазмалар китобхонларда ватанпарварлик, фуқоролик мажбуриятини ва табиатимиз-

га бошқача нигох билан қарашни ўргатади.

Мақсадли комплексли дастурлар: “Биз ва табиат”; “Экология.Инсон.Жамият.“Яшна Ер” ; “Планетамиз тозалиги-қалбимиз тозалигидир”; “Сенга ва менга керак бу Замин”.

Қизиқиш клублари: “Эколог”, “Жилға”, Экологик тарбия мактаби”, “Ўлкашунос”.

Қизиқиш клублар ўқувчилар учун қизикарли машғулотлар ташкил қилиб, ихтирочилик, конструкторлик истеъдодларини намоён қилиши, табиатга, ўз ўлкасига муҳаббат уйғотиши мумкин. Қизиқиш клублар фаолиятининг ўзига хослиги шундаки, нафақат уларда истеъдодли болалар, балки барча иштиёқмандлар қатнашишлари мумкин.

Экологик хафталиклар.

Улар бир қанча тадбирлардан ташкил топади. Масалан, “Яшна Ер курраси” китоб кўргазмасидан, “Ерликларга тоза планета” номли экологик маданият дарси, “Биз шу планетада яшаймиз” номли матбуот мақолалари эко-обзори ва хокозо.

Адабиётларни тавсия рўйҳати: “Табиатдан соғлиқ ол”; “Жонажон табиатингни сақла”,

“Ер куррасидаги қўшниларимиз”.

Бюллетень “Эколология ва замон”. Ҳар чоракда чоп этиш мумкин. Унда янги китоблар, матбуотда эълон қилинган мақолалар, адабиётларни тавсия рўйҳатлари, кутубхоначилар ва китобхонлар учун услубий-библиографик ишланмалар бериб борилади. Шунингдек “Экология.Маданият. Жамият” номли газета-журнал мақолалари картотекасини юритиш мақсадга мувофиқдир.Электрон каталогда “Экология” рубрикаси ажратилиб, унда кутубхона фондида ёки бошқа кутубхоналарда мавжуд бўлган хужжатлар ҳақида маълумотлар бериб борилади.

Хулоса қилиб айтганда, ахборот-кутубхона муассасаларининг халқимизни айниқса ёшларни экологик маданиятини шакллантириш бўйича катта имкониятлари мавжуд. Ўйлаймизки, экологик маданиятни шакллантириш бўйича амалга ошириладиган ишлар ахборот-кутубхона муассасалари фаолиятининг асосий йўналишларидан бири бўлиб қолади.

ПРИМЕНЕНИЕ КОНЦЕПЦИИ ARIS В ПРЕПРОЕКТНОМ ИССЛЕДОВАНИИ ОБЪЕКТА НА СОЗДАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Хундибаев Абдурахман Маликович

кандидат технических наук, преподаватель

Ташкентского университета информационных технологий

В данной статье описываются роль и место стадии предпроектного исследования объекта автоматизации на создание информационных систем и применение на этой стадии концепции Архитектуры Интегрированных Информационных Систем (ARIS).

В настоящее время в Узбекистане актуальность разработки и внедрения информационных систем возросла до исторического пика, которая доказывается большим списком планируемых и реализуемых проектов в рамках проекта "Электронное правительство" (www.egovernment.uz). Процесс создания информационных систем урегулируется ГОСТом O`zDst 1986: 2010 "Информационные системы. Этапы создания" [1]. Согласно данному ГОСТу создания любой информационной системы начинается с важного этапа – создания предпроектного документа "Технико-экономическое обоснование (ТЭО)» на создание информационной системы".

Тщательное, основательное создание ТЭО предопределяет качество процессов разработки и внедрения информационной системы, т.е. облегчает процесс разработки и повышает эффективность эксплуатации информационных систем.

Для разработки ТЭО необходимо анализировать существующие бизнес-процессы, документооборот, материальные и информационные потоки на объекте автоматизации. Организуются исследовательские работы на объекте привлечением специалистов-аналитиков. Указания по анализу бизнес-процессов приводятся в нормативных документах (например, в РД 50-34.698-90. Автоматизированные системы. Требования к содержанию документов) [2], но в них не приводятся рекомендации по применению средств и технологий для повышения эффективности работ аналитиков в этом процессе.

Определение организационных, методологических, технико-технологических недостатков в существующих бизнес-процессах и выработка предложений по их устранению является основным пунктом в отчете по результатам проведения исследования для разработки ТЭО. Именно отсутствие данного пункта во многих случаях оставляет под сомнением эффективность проекта в целом.

Для проведения анализа сначала необходимо описать бизнес-процессы и связи между ними, т.е. создается модель деятельности объекта [3]. Использование множества методов для описания реальных ситуаций деятельности объекта требует выработки стандартизированную концепцию (архитектуру) применения в создании информационных систем.

Одной из таких концепций является – Архитектура Интегрированных Информационных Систем – ARIS (Architecture of Integrated Information Systems), разработанная проф. Шеером [4]. Эта концепция имеет два основных преимущества:

- позволяет выбрать методы и интегрировать их, опираясь на основные особенности моделируемого объекта;
- служит базой для управления сложными проектами, поскольку благодаря структурным элементам содержит встроенные модели процедур для разработки интегрированных информационных систем.

Первый шаг при создании архитектуры состоит в разработке модели бизнес-процесса, описывающей все его основные функции. Полученная таким образом чрезвычайно сложная модель разделится на подмодели, или типы моделей, в соответствии с типами представлений. Это позволяет существенно снизить степень ее сложности. Содержимое типов моделей может быть описано методами, предназначенными для конкретного типа представления. Многочисленные взаимосвязи между типами моделей при этом не учитываются.

Вторым подходом, уменьшающим сложность модели бизнес-процесса, является анализ каждого типа моделей на различных уровнях. В соответствии с концепцией модели жизненного цикла различные методы описания информационных систем дифференцируются по степени их близости к информацион-

ным технологиям. Это гарантирует целостность описания на всех этапах, начиная от проблем управления бизнесом до технической реализации информационной системы.

Архитектура ARIS создает основу для разработки и оптимизации интегрированных информационных систем, а также для описания их реализации.

Выбор уровней и типов описаний формирует архитектуру ARIS, которая используется в качестве модели для построения процессов, связанных с управлением бизнесом, их анализа и оценки.

В архитектуре ARIS используется 4 вида модели (модель ресурсов, организационная модель, функциональная модель, информационная модель). На рисунке приведены модели для процесса выполнения заказа в библиотеках.

Взаимосвязи процессов представляются в компактном виде с помощью диаграмм (PCDs), которые также позволяют описывать информационные системы. Диаграмма типа ***PCDs (Process Chain Diagram)*** – это диаграмма цепочки процесса, или просто диаграмма процесса. В диаграмме этого типа цепочка (последовательность шагов/функций) процесса отображается в виде замкнутого цикла. Отдельные типы моделей бизнес-процессов (организационная модель, модель данных, функциональная модель и модель ресурсов) и их взаимосвязи выражаются более отчетливо.

В приведенном примере (рис.1) событиями вступают: *«получен заказ», «введен заказ», «заказ обработан», «заказ выполнен», а в качестве функциями: «вести заказ», «обработать заказ», «доставить заказ»*.

Функция «вести заказ» инициируется событием «заказ получен». В результате выполнения этой функции происходит событие «заказ введен», которое в свою очередь инициирует следующую функцию «обработать заказ». Это отношение между событиями и функциями составляет процедурную последовательность функций как логическую цепочку событий. Логическая взаимозависимость возможных точек ветвления и циклов потока управления может быть выражена посредством логических операций (and, or, not), связывающих функции и события.

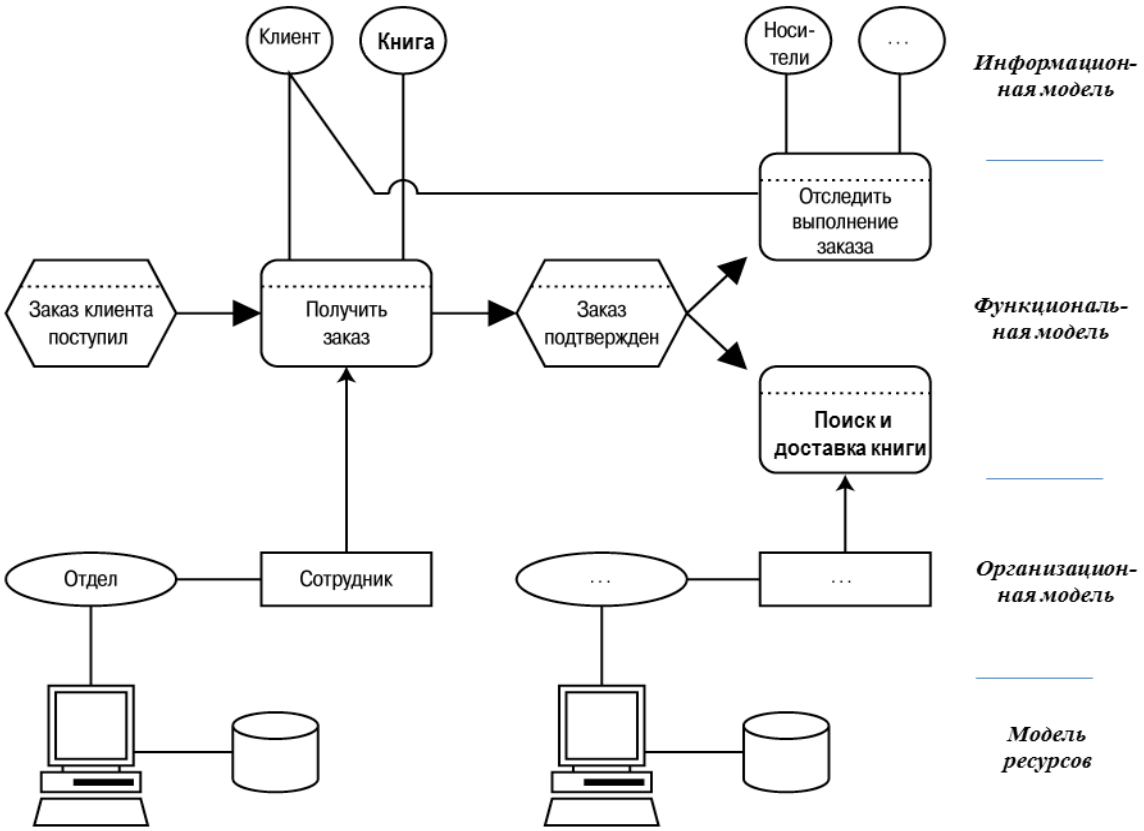


Рис.1. Модели в процессе выполнения заказа в библиотеках.

Входные и выходные данные для функций, можно показать в виде кластеров данных. Входные данные для функции «обработать заказ» - это «данные заказа»; генерируемые выходные данные – «заказ клиента».

При описании начальной ситуации диаграммы процессов создаются с относительно высоким уровнем обобщения (без детализации). Поскольку эти диаграммы используются главным образом для отображения взаимосвязей всех компонентов ARIS (моделей различных типов), они служат основой для создания управляющей модели ARIS. При создании управляющей модели используются не только диаграммы процесса, но и диаграммы цепочки процесса, управляемого событиями (***EPCs – Event-driven Process Chain***). С точки зрения моделирования событийные диаграммы процессов также полезны, как и

простые диаграммы процессов.

Декомпозиция бизнес-процесса на отдельные типы моделей уменьшает степень его сложности за счет исключения из рассмотрения взаимосвязей между компонентами процесса, относящихся к другому типу моделей.

Для каждого бизнес-процесса определяются бизнес-роль и владелец процесса. Бизнес-роль - ответственность персонала за исполнение функции, операции или ответственность подразделения за исполнение процесса. Владелец процесса - лицо или группа лиц, отвечающие за исполнение процесса и имеющие полномочия на изменение его с целью усовершенствования.

Описание бизнес-процесса до 4-уровня (т.е. декомпозиция до нижнего уровня) определяет атрибуты показателей объекта. Обычно это описание достаточно для определения структуры базы данных об объекте.

Более детальное описание бизнес-процесса позволяет:

- Определение схожих или дублированных процессов (например, в двух отделах выполняется одинаковая операция);
- Определение узловых процессов, автоматизация которых приносит наибольший эффект;
- Приоритетность автоматизируемых процессов (на основе анализа процессов вырабатывается рекомендация об очередности автоматизации);
- Построение алгоритмов автоматизации процесса;
- Определение структуры базы данных объекта.

Практика показывает для описания бизнес–процессов библиотеки необходимо до тысячи PCDs.

Разработанные PCDs бизнес-процессов объекта автоматизации, полезно не только для специалистов, занимающихся автоматизацией, но и управленческого персонала объекта. На основе анализа этой модели бизнес-процессов руководство организации могут узнать об «узких местах» своего объекта, приняв соответствующие меры, могут получать эффект, даже без внедрения информационных систем.

Литература

1. O`zDst 1986: 2010 “Информационные системы. Этапы создания”.
2. РД 50-34.698-90. “Автоматизированные системы. Требования к содержанию документов”.
3. Попов, А.И. Свободные инструменты проектирования информационных систем: учеб.-метод, пособие / А.И. Попов; Сев. (Арктич.) федер. ун-т им. М.В. Ломоносова. - Архангельск: ИПЦ САФУ, 2012. - 78 с
4. Инструментарий ARIS: Методы ARIS. Версия 4.1., Весть-МетаТехнология, 2000.

АТРИБУТЫ ПОТОКА

Шокиров Шодмон Шойимович
Ассистент, ТУИТ

Атрибуты процесса содержат информацию, которая описывает процесс для операционной системы. Операционная система использует эту информацию для управления процессами, а также для того, чтобы отличать один процесс от другого. Процесс совместно использует со своими потоками практически все, включая ресурсы и переменные среды. Разделы данных, раздел программного кода и все ресурсы связаны с процессом, а не с потоками. Все, что нужно для функционирования потока, определяется и предоставляется процессом. Потоки же отличаются один от другого идентификационным номером (id), набором регистров, определяющих состояние потока, его приоритетом и стеком. Именно эти атрибуты формируют уникальность каждого потока. Как и при использовании процессов, информация о потоках хранится в структурах данных и возвращается функциями, поддерживаемыми операционной системой. Например, часть информации о потоке содержится в структуре, именуемой информационным блоком потока, который создается вместе с потоком.

Идентификационный номер (id) потока — это уникальное значение, которое идентифицирует каждый поток во время его существования в процессе. Приоритет потока определяет, каким потокам предоставлен привилегированный доступ к процессору в выделенное время. Под состоянием потока понимаются условия, в которых он пребывает в любой момент времени. Набор регистров для потока включает программный счетчик и указатель стека. Программный счетчик содержит адрес инструкции, которую поток должен выполнить, а указатель стека ссылается на вершину стека потока.

Библиотека потоков POSIX определяет объект атрибутов потока, инкапсулирующий свойства потока, к которым его создатель может получить доступ и модифицировать их. Объект атрибутов потока определяет следующие компоненты:

- область видимости;
- размер стека;
- адрес стека;
- приоритет;
- состояние;
- стратегия планирования и параметры.

Объект атрибутов потока может быть связан с одним или несколькими потоками. При использовании этого объекта поведение потока или группы потоков определяется профилем. Все потоки, которые используют объект атрибутов, приобретают все свойства, определенные этим объектом. На рис. 4.3 показаны атрибуты, связанные с каждым потоком. Как видите, оба потока (A и B) разделяют объект атрибутов, но они поддерживают свои отдельные идентификационные номера и наборы регистров. После того как объект атрибутов создан и инициализирован, его можно использовать в любых обращениях к функциям создания потоков. Следовательно, можно создать группу потоков, которые будут иметь «малый стек и низкий приоритет» или «большой стек, высокий приоритет и состояние откреления». Откреленный (detached) поток — это поток, который не синхронизирован с другими потоками в процессе. Иначе говоря, не существует потоков, которые бы ожидали до тех пор, пока завершит выполнение откреленный поток. Следовательно, если уж такой поток существует, то его ресурсы (а именно id потока) немедленно принимаются на повторное использование. [8] Для установки и считывания значений этих атрибутов предусмотрены специальные методы. После создания потока его атрибуты нельзя изменить до тех пор, пока он существует.

Атрибут области видимости описывает, с какими потоками конкретный поток конкурирует за обладание системными ресурсами. Потоки соперничают за ресурсы в рамках двух областей видимости: процесса (потоки одного процесса) и системы (все потоки в системе). Конкуренция потоков в пределах одного и того же процесса происходит за дескрипторы файлов, а конкуренция потоков в масштабе всей системы — за ресурсы, которые выделяются системой (например, реальная память). Потоки соперничают с потоками, которые имеют область видимости процесса, и потоками из других процессов за использование процессора в зависимости от состязательного режима и областей выделения ресурсов (набора процессоров). Поток, обладающий системной областью видимости, будет обслуживаться с учетом его приоритета и стратегии планирования, которая действует для всех потоков в масштабе всей системы.

КАК НА С++ ВЫПОЛНИТЬ ПАРАЛЛЕЛЬНЫЕ МАТЕМАТИЧЕСКИЕ ВЫЧИСЛЕНИЯ?

Шокиров Шодмон Шойимович
Ассистент, ТУИТ

Параллельные вычисления — способ организации компьютерных вычислений, при котором программы разрабатываются как набор взаимодействующих вычислительных процессов, работающих параллельно (одновременно). Термин охватывает совокупность вопросов параллелизма в программировании, а также создание эффективно действующих аппаратных реализаций. Существуют различные способы реализации параллельных вычислений. Например, каждый вычислительный процесс может быть реализован в виде процесса операционной системы, либо же вычислительные процессы могут представлять собой набор потоков выполнения внутри одного процесса ОС. Параллельные программы могут физически исполняться либо последовательно на единственном процессоре — перемежая по очереди шаги выполнения каждого вычислительного процесса, либо параллельно — выделяя каждому вычислительному процессу один или несколько процессоров.

Основная сложность при проектировании параллельных программ — обеспечить правильную последовательность взаимодействий между различными вычислительными процессами, а также координацию ресурсов, разделяемых между процессами.

У меня есть числа от 1 до 18446744073709551615. И для каждого числа вычисляется остаток от деления. Но вычисления получаются бесконечными, мне сказали, что нужно делать в несколько потоков и тогда будет все параллельно, но я не понимаю как это.

Получение простого числа 100%. Первые 500 простых чисел по таблице прогонял, ответ тоже 100%. Исходя из готовых алгоритмов (так как вероятностные использовать нельзя).

```
#include <iostream>
#include <biginteger.cpp>
using namespace std;
int main(int argc, char *argv[]) {
  char *text = "274876858367";
  BigInteger n(text), k, q;
  if (n % 2 == 0 || n == 1) {
    cout << "число не является простым" << endl;
    return 0;
  }
  q = n.sqrt() + 1;
  BigInteger m;
  bool prm = true;
  // простые делители
  // начинаются с тройки
  for(k = 3; k <= q; ) {
    // все четные делители и все делители,
    // кратные простым числам, могут быть опущены
    if ((k % 2 == 0) || (k % 3 == 0)) { k++; continue; }

    //m = n%k;
    //cout << "n = " << n << " k = " << k << ", n % k = " << m <<endl;
    if (n % k == 0) {
      prm = false;
      break;
    }
    k++;   }
  if (prm) cout << "число является простым" << endl;
  else cout << "число не является простым" << endl;
  return 0; }
```

ОПРЕДЕЛЕНИЕ ПОТОКА И КОНТЕКСТНЫЕ ТРЕБОВАНИЯ ПОТОКА

Шокиров Шодмон Шойимович
Ассистент, ТУИТ

Работу любой последовательной программы можно разделить между несколькими подпрограммами. Каждой подпрограмме назначается конкретная задача, и все эти задачи выполняются одна за другой. Вторая задача не может начаться до тех пор, пока не завершится первая, а третья — пока не закончится вторая и т.д. Описанная схема прекрасно работает до тех пор, пока не будут достигнуты границы производительности и сложности. В одних случаях единственное решение проблемы производительности — найти возможность выполнять одновременно более одной задачи. В других ситуациях работа подпрограмм в программе настолько сложна, что имеет смысл представить эти подпрограммы в виде мини-программ, которые выполняются параллельно внутри основной программы. В главе 3 были представлены методы разбиения одной программы на несколько процессов, каждый из которых выполняет отдельную задачу. Такие методы позволяют приложению в каждый момент времени выполнять сразу несколько действий. Однако в этом случае каждый процесс имеет собственные адресное пространство и ресурсы. Поскольку каждый процесс занимает отдельное адресное пространство, то взаимодействие между процессами превращается в настоящую проблему. Для обеспечения связи между раздельно выполняемыми частями общей программы нужно реализовать такие средства межпроцессного взаимодействия, как каналы, FIFO-очереди (с дисциплиной обслуживания по принципу «первым пришел — первым обслужен») и переменные среды. Иногда нужно иметь одну программу (которая выполняет несколько задач одновременно), не разбивая ее на множество мини-программ. В таких обстоятельствах можно использовать потоки. Потоки позволяют одной программе состоять из параллельно выполняемых частей, причем все части имеют доступ к одним и тем же переменным, константам и адресному пространству в целом. Потоки можно рассматривать как мини-программы в основной программе. Если программа разделена на несколько процессов, как было показано в главе 3 , то с выполнением каждого отдельного процесса связаны определенные затраты системных ресурсов. Для потоков требуется меньший объем затрат системных ресурсов. Поэтому потоки можно рассматривать как облегченные процессы, т.е. они позволяют воспользоваться многими преимуществами процессов без больших затрат на организацию взаимодействия между ними. Потоки обеспечивают средства разделения основного «русла» программы на несколько параллельно выполняемых «ручейков».

Под потоком подразумевается часть выполняемого кода в UNIX- или Linux-процессе, которая может быть регламентирована определенным образом. Затраты вычислительных ресурсов, связанные с созданием потока, его поддержкой и управлением, у операционной системы значительно ниже по сравнению с аналогичными затратами для процессов, поскольку объем информации отдельного потока гораздо меньше, чем у процесса. Каждый процесс имеет основной, или первичный, поток. Под основным потоком процесса понимается программный поток управления или поток выполнения. Процесс может иметь несколько потоков выполнения и, соответственно, столько же потоков управления. Каждый поток, имея собственную последовательность инструкций, выполняется независимо от других, а все они — параллельно друг другу. Процесс с несколькими потоками, называется многопоточным.

Все потоки одного процесса существуют в одном и том же адресном пространстве. Все ресурсы, принадлежащие процессу, разделяются между потоками. Потоки не владеют никакими ресурсами. Ресурсы, которыми владеет процесс, совместно используются всеми потоками этого процесса. Потоки разделяют дескрипторы файлов и файловые указатели, но каждый поток имеет собственные программный указатель, набор регистров, состояние и стек. Все стеки потоков находятся в стековом разделе своего процесса. Раздел данных процесса совместно используется потоками процесса. Поток может считывать (и записывать) информацию из области памяти своего процесса. Когда основной поток записывает данные в память, то любые сыновние потоки могут получить к ним доступ. Потоки могут создавать другие потоки в пределах того же процесса. Все потоки в одном процессе считаются равноправными. Потоки также могут приостановить, возобновить или завершить другие потоки в своем процессе.

Потоки — это выполняемые части программы, которые соревнуются за использование процессора с потоками того же самого или других процессов. В многопроцессорной системе потоки одного процесса могут выполняться одновременно на различных процессорах. Однако потоки конкретного процесса выполняются только на процессоре, который назначен этому процессу. Если, например, процессоры 1, 2 и 3 назначены процессу А, а процесс А имеет три потока, то любой из них может быть назначен любому

процессору. В среде с одним процессором потоки конкурируют за его использование. Параллельность же достигается за счет переключения контекста. Контекст переключается, если операционная система поддерживает многозадачность при наличии единственного процессора. Многозадачность позволяет на одном процессоре одновременно выполнять несколько задач. Каждая задача выполняется в течение выделенного интервала времени. По истечении заданного интервала или после наступления некоторого события текущая задача снимается с процессора, а ему назначается другая задача. Когда потоки выполняются параллельно в одном процессе, то о таком процессе говорят, что он — многопоточный. Каждый поток выполняет свою подзадачу таким образом, что подзадачи процесса могут выполняться независимо от основного потока управления процесса. При многозадачности потоки могут конкурировать за использование одного процессора или назначаться другим процессорам. Но в любом случае переключение контекста между потоками одного и того же процесса требует меньше ресурсов, чем переключение контекста между потоками различных процессов. Процесс использует много системных ресурсов для отслеживания соответствующей информации, а на управление этой информацией при переключении контекста между процессами требуется значительное время. Большая часть информации, содержащейся в контексте процесса, описывает адресное пространство процесса и ресурсы, которыми он владеет. Переключаясь между потоками, определенными в различных адресных пространствах, контекст переключается и между процессами. Поскольку потоки в рамках одного процесса не имеют собственного адресного пространства (или ресурсов), то операционной системе приходится отслеживать меньший объем информации. Контекст потока состоит только из идентификационного номера (id), стека, набора регистров и приоритета. В регистрах содержится программный указатель и указатель стека. Текст (программный код) потока содержится в текстовом разделе соответствующего процесса. Поэтому переключение контекста между потоками одного процесса займет меньше времени и потребует меньшего объема системных ресурсов.

СОЗДАНИЕ ПОТОКОВ

Шокиров Шодмон Шойимович
Ассистент, ТУИТ

Библиотека Pthreads используется для создания, поддержки и управления потоками многопоточных программ и приложений. При создании многопоточной программы потоки могут создаваться на любом этапе выполнения процесса, поскольку это — динамические образования. Функция pthread_create() создает новый поток в адресном пространстве процесса. Параметр thread указывает на дескриптор, или идентификатор (id), создаваемого потока. Новый поток будет иметь атрибуты, заданные объектом attr. Созданный поток немедленно приступит к выполнению инструкций, заданных параметром start_routine с использованием аргументов, заданных параметром arg. При успешном создании потока функция возвращает его идентификатор (id), значение которого сохраняется в параметре thread.

```
#include <pthread.h>
int pthread_create(pthread_t *restrict thread,
const pthread_attr_t *restrict attr,
void *(*start_routine)(void*),
void *restrict arg) ;
```

Если параметр attr содержит значение NULL, новый поток будет использовать атрибуты, действующие по умолчанию. В противном случае новый поток использует атрибуты, заданные параметром attr при его создании. Если же значение параметра attr изменится после того, как поток был создан, это никак не отразится на его атрибутах. При завершении параметра-функции start_routine завершается и поток, причем так, как будто была вызвана функция pthread_exit() с использованием в качестве статуса завершения значения, возвращаемого функцией start_routine.

При успешном завершении функция возвращает число 0 . В противном случае по-не создается, и функция возвращает код ошибки. Если в системе отсутствуют ресурсы для создания потока, или в процессе достигнут предел по количеству возможных потоков, выполнение функции считается неудачным. Неудачным оно также будет в случае, если атрибут потока задан некорректно или если инициатор вызова потока не имеет разрешения на установку необходимых атрибутов потока.

Приведем примеры создания двух потоков с заданными по умолчанию атрибутами:

```
pthread_create(&threadA,NULL, taskl,NULL) ;
pthread_create(&threadB,NULL, task2, NULL) ;
```

Это — два вызова функции pthread_create () из листинга 1. Оба потока создаются с атрибутами, действующими по умолчанию.

В программе 1 отображен основной поток, который передает аргумент из командной строки в функции, выполняемые потоками.

```
// Программа 1
#include <iostream>
#include <pthread.h>
#include <stdlib.h>
int main(int argc, char *argv[]) {
pthread_t ThreadA,ThreadB;
int N;
if(argc != 2) {
cout << «error» << endl;
exit (1); }
N = atoi(argv[l]);
pthread_create(&ThreadA,NULL, taskl,&N);
pthread_create(&ThreadB,NULL, task2, &N);
cout « «Ожидание присоединения потоков.» « endl;
pthread_join(ThreadA,NULL) ;
pthread_join(ThreadB,NULL);
return (0) ; };
```

В программе 1 показано, как основной поток может передать аргументы из командной строки в каждую из потоковых функций. Число в командной строке имеет строковый тип. Поэтому в основном потоке аргумент сначала преобразуется в целочисленное значение, и только после этого результат преобразо-

вания передается при каждом вызове функции pthread_create () посредством ее последнего аргумента.

В программе 2 представлена каждая из потоковых функций.

```
// Программа 2
void *task1(void *X) {
int *Temp;
Temp = static_cast<int *>(X);
for(int Count = 1;Count < *Temp;Count++){
cout << «work from thread A: " << Count << " * 2 = "
<< Count * 2 << endl; }
cout << «Thread A complete» << endl; }
void *task2(void *X) {
int *Temp;
Temp = static_cast<int *>(X);
for(int Count = 1;Count < *Temp;Count++){
cout << «work from thread B: " << Count << " + 2 = "
<< Count + 2 << endl; }
cout << «Thread B complete» << endl; }
```

В программе 2 функции taskl и task2 выполняют цикл, количество итераций которого равно числу, переданному каждой функции в качестве параметра. Одна функция увеличивает переменную цикла на два, вторая — умножает ее на два, а затем каждая из них отправляет результат в стандартный поток вывода данных. По выходу из цикла каждая функция выводит сообщение о завершении выполнения потока. Инструкции по компиляции и выполнению программ 1 и 2 содержатся в профиле программы 1.

Профиль программы 1

Имя программы •program-12.cc

* Описание Принимает целочисленное значение из командной строки и передает функциям: потоков. Каждая функция выполняет цикл, в котором переменная цикла увеличивается (в одной функции на два, а в другой в два раза), а затем результат отсылается в стандартный поток вывода данных. Код основного потока выполнения приведен в программе 1, а код функций — в программе 2.

THE ROLE OF INCREASING ICT AND E-GOVERNMENT

Kudratov S.G.

Extensive and widespread use of information and communication technologies (hereinafter - ICT) is a global trend of world development. The level of development of ICT is now one of the most important indicators of economic and social well-being of the state. Development and implementation of ICT is crucial to improve the efficiency of public administration and local self-government, increase the competitiveness of the national economy in the world.

Impressive is an example of such countries as the Republic of Korea, Singapore which made bets on the development of ICT and were able to bring their economies at the forefront of the world market.

However, information and communication technologies require specific qualifications, in this connection, the education and training of ICT specialists play an important role in shaping the economy based on knowledge.

Realizing the importance of this industry leading foreign countries are investing heavily in the development of ICT. So, if we look at the table, which lists the world's leading countries for spending on IT in 2014 (Appendix №1, table №1), we see that US spending on IT in 2014 totaled 654.55 billion. USD, China 182.74 billion Dollars. In addition, the growth rate of IT spending in countries such as India (growth in IT spending in the year - 19.7%, growth of GDP per year - 5.0%), Brazil (up IT spending in the year - 15.8%, growth of GDP per year - 2.5%), Japan (increase IT spending year - 3.4% GDP growth per year - 1.5%) is significantly higher than the annual rate of GDP growth, indicating that the priority use of information technology to improve the competitiveness of these countries in the world.

Specific assessment of the state, success and prospects of development of ICT in a country can be obtained using various international ratings which take into account a number of specific indicators or indices.

Thus, the United Nations, through its specialized unit, which determines international standards in the field of ICT - International Telecommunication Union (International Telecommunication Union, ITU) monitors the development of ICT in the various countries of the world. The purpose of research is to make an objective evaluation of the effectiveness of the international based on quantitative indicators and benchmarks, which will serve as an important contribution to the discussion of ICT policy in the States - Members of the ITU. The studies determined by ICT development index (ICT Development Index, IDI). The organization publishes the index on a regular basis, which allows countries to monitor changes across time.

The index was developed in 2007 on the basis of 11 indicators, which relate to:

a) The accessibility of ICT (IDI access sub-index) - 5 indicators:

1. Fixed telephone lines per 100 inhabitants (nominal value - 60);
2. The contracts for mobile cellular telephone subscriptions per 100 inhabitants (nominal value - 120);
3. The bandwidth of the international Internet traffic (bit / s) per Internet user (nominal value - 787 260);
4. The proportion of households with a computer (nominal value - 100%);
5. The proportion of households with Internet access (nominal value - 100%);

b) Use of ICT (IDI use sub-index) - 3 indicators:

6. The proportion of people using the Internet (nominal value - 100%);
7. Contracts for fixed (wired) broadband subscriptions per 100 inhabitants (nominal value - 60);
8. Contracts for wireless broadband subscriptions per 100 inhabitants (nominal value - 100%);

c) The skills of the population to ICT (IDI skills sub-index) - 3 indicators:

9. The literacy rate among the adult population (nominal value - 100%);
10. Coverage of secondary education (nominal value - 100%);
11. Coverage of higher education (nominal value - 100%).

A report issued in 2014, the study presents data on the ICT Development Index of 166 countries for 2013 in comparison with 2012 (Appendix №2, table №2). According to the report Denmark is the rating leader. It is followed by the Republic of Korea, Sweden, Iceland and the United Kingdom. Uzbekistan ranks 115 (out of 166 countries) in the ranking with an index of 3.40, ahead of a country like India, which is on the 129 place. In 2012, our country occupies 116th place in the ranking.

As shown in the report, ICT indicators is higher in those countries in which the higher the proportion of the population living in urban areas, where there are more favorable conditions for the development of ICT infrastructure, ICT use and ICT skills. In countries with the highest levels of the index of the government to promote the information economy have identified a number of major objectives in the field of ICT, including the provision of high-speed access to the Internet for the most part (and sometimes entire) population, the promotion

of wireless broadband (including LTE) and implementation ICT in homes. In particular, in the European Union (EU) recognizes the importance of access of households to high-speed and super-fast broadband connection and become the largest target to connect 50% of households to superfast broadband connections (at least 100 Mbit / s) and achieve coverage of all households with broadband connections with the rate of at least 30 Mbits / s 2020.

Also, this study was compiled ranking countries in terms of development of the Internet. This index is calculated by the method of the International Telecommunication Union as the number of Internet users per 100 people in the country.

Published in 2014 (as of 2013) study presents data on 211 countries of the world. This ranking Uzbekistan takes 114th place (out of 211 countries) with an index of 36.52 users per 100 inhabitants. Our country is ahead of countries such as Ukraine (118th), Iran (132), Kyrgyzstan (139), Tajikistan (155), India (161), and Turkmenistan (176).

The ranking is the Falkland Islands (1st place, the rate of -96.92, Iceland (2nd place, figure - 96.21), Norway (3 place measure - 94.65). The Republic of Korea took 19th place with 84.07.

Ranking of countries by level of development of e-government is built on the basis of e-Government Development Index (E-Government Development Index, EGDI), is a composite indicator that measures the willingness and ability of governments to use information and communication technologies to provide services to the population. The research ranking conducted by the UN Department of Economic and Social Affairs, which assesses the level of development of e-government in 193 countries, was held at the United Nations. EGDI is published every two years, and methodologically is calculated as a simple average of three basic indicators evaluating the most important aspects of e-government:

1) Latitude and quality of on-line service (Online Service Index, OSI). It is calculated based on the analysis of questionnaires, which fills a group of experts in the field of public administration, the testing sites of state institutions of each country (national portal, e-services, web-sites of the ministries of education, labor, social protection, finance and the environment, etc.) on a number of key topics related to e-government and online services;

2) The level of development of telecommunications infrastructure (Telecommunication Infrastructure Index, TII). Includes 5 indicators with equal weights: subscribers of cellular mobile communication (100 people); Internet users (% of population); fixed telephone subscribers (per 100 people); wireless broadband subscribers (per 100 people); fixed broadband subscribers (per 100 people);

3) The volume of human capital (Human Capital Index, HCI). Includes 4 indicators: literacy (literacy rate of the population aged 15 years and older); Gross school attendance rate (the ratio of total enrollment in educational institutions 1-3 steps regardless of their age, to the number of population in the age of learning in educational institutions 1-3 stages); estimated duration of schooling (years); the number of years spent in education the average adult (average of years of education of the population aged 25 years and above).

The top three rankings included (respectively): South Korea, Australia and Singapore. Uzbekistan in this ranking, published in 2014, won 100 out of 193 countries included in the study. Our country is ahead of countries such as Kyrgyzstan (101 seats), Iran (105th place), India (118th) and Turkmenistan (128 place), Tajikistan (129 place).

Index of e-government in Uzbekistan amounted to 0.4695 points. The indicator "Online services" amounted to - 0.4488, indicators of "telecommunications infrastructure" - 0.2333 and indicators of "human capital" - 0.7264 points.

In addition, in the above study, the UN Department of Economic and Social Affairs also participate in the index is computed electronic government (E-Government Participant Index, EGPI), which shows how citizens can participate in the discussion and decision-making with the help of online resources. This index complements the development of e-government index. That is, in the UN study measured not only as a State affects the lives of citizens by means of Internet technologies, but also as citizens may affect the operation of the state.

Among the leaders of the rankings in 2014: the Netherlands, South Korea, Uruguay, United Kingdom, France and Japan.

In the ranking Uzbekistan is on 71 place. For comparison, Kazakhstan - 22 place, Germany - 24, Russia - 30, China - 33, Ukraine and Azerbaijan - 77, Kyrgyzstan - 81, Switzerland - 91, Belarus - 92, Tajikistan and Turkmenistan - 158th place.

In general, the citizens of our country are willing and able to use e-government services that have been created for them.

Thus, the international rankings can be a useful tool for monitoring and assessing the level of development of ICT and e-government in the country.

Sources:

1. The index of information and communication technologies: http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2014.aspx

2. The index of e-government:
http://unpan3.un.org/egovkb/Reports/UN-E-Government-Survey-2014

3. The International Telecommunication Union www.itu.int

PRINCIPLES OF EXCHANGE DOCUMENTS

Ishniyazov Odil Olimovich

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

assistant, Basic of Informatics

To fully understand the operation of the electronic exchange documents management system, we introduce a summary of the main components.

The document - is fixed on a material bearer with requisites allowing to identify it.

An electronic document (ED) - the information recorded in electronic form, certified electronic digital signature and having other details of the electronic document, allowing him to be identified.

Exchange document - the movement of documents in the organization since its creation or receipt to complete the execution or administration.

Exchange Electronic Document Management (EEDM) - Electronic document is a collection of sending and receiving electronic documents through the information system.

Automation System workflow, exchange electronic document management system (EEDMS) - an automated multi-user system that accompanies the work of the management of hierarchical organization to ensure compliance with the organization of its functions. It is assumed that the control process is based on the human-readable documents containing instructions for employees required to perform.

Consider two of the electronic document management system, which was introduced earlier in the archival institutions in some of the CIS (Commonwealth of Independent States) countries:

The free application "BOSS-Referent 4J» - exchange electronic document and interaction management system, aimed at improving the efficiency of work across the organization in different areas of their joint activities.

Advantages:

- Manage the organizational structure
- Manage external recipients
- Processing of incoming and outgoing correspondence

Disadvantages:

- The lack of easy access to all the documents on the subject: categorization and search of documents
- Can not support the full route management processing document
- Enough complex installation, configuration and restart the program
- Low performance and scalability

The software for a fee, the MOTIVE system - the first system of management of the company in real time. Control of execution of orders, a collective work on the project, coordination of documents, electronic archive and much more.

Advantages:

- Save time and reduce the routine work;
- risk control (the ability to keep control of the most important tasks, not forgetting the less important);
- Reducing the time to search for the information you need;

Disadvantages:

- Lack of remote access and efficient interaction with branches;

accumulation of intellectual experience of the company.

- The main disadvantage is the limited system of work with a lot of information - each user of the system may not be thousands of tasks, but only two or three.

After reviewing the above exchange electronic document management system, the management of archival institutions, it was decided to create a "Program complex exchange electronic document archival institutions", which will include materials and documents relating to the archival institutions.

When designing the system already in the initial stages, it is necessary to lay the basic principles of rational construction of the structure, which will significantly affect the course of the design, development and implementation of the system, ensure the correct course of action leaders and experts in solving various issues. These principles specify that you must first be provided, and then perform to achieve this goal the most effective way.

Collection of information and research activities of the program complex exchange electronic document archival institutions should be carried out in several stages:

• study of functional areas in order to determine the required input and output information;

• building the organizational and functional charts and analysis of information flows, reflecting the specifics of the structure and activities;

• definition of information objects and details of appropriate composition.

In order to achieve the efficiency of the automated system is required complete information. In addition to access to current information, it is desirable to have access to the archive data in accordance with the principles of the document, which set mandatory storage of archival documents. Thus, the system should have the function of information storage.

Tradition and workflow rules were formulated in 1811 by M.M.Speransky, it was then for the first time feature the requirements for working with documents in public institutions. There was a records management - the science that studies the laws of records and exchange document management and how these patterns affect the management of organizations and enterprises in the framework of documentary maintenance of management of the enterprises.

Fundamentals and challenges facing Documentation, since then has not changed significantly. Many of the requirements and rules fixed in O`zDST 1157-2008 and a number of other regulations.

It is known that the exchange document is part of a records management. Documentary management software - A branch of activity, providing documentation and organization of the official documents, which has its own technology. Technology document management - a document the organization, storage and use of documents in the current activities of the institution.

PROBLEMS IN THE IMPLEMENTATION OF ELECTRONIC DOCUMENT ARCHIVAL INSTITUTIONS

Ishniyazov Odil Olimovich

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

assistant, Basic of Informatics

In general, enterprise management can be divided into two components: the actual management and its information support. The first group includes the activities involved in the "decision-making system", and the second - the processes that ensure the accumulation, processing, analysis of the information needed to guide the company. Any large organization, such as archival institutions, operates the huge flow of information.

It should be noted that there are specialized software for implementing document management process, in principle, take into account all that is necessary. However, in this case, we have to deal with some range of issues.

First of all, note that when you buy the software, third-party manufacturers in our region there is practically no support, and not only technical. No support for staff working with the software. Let us try to explain the problem.

Electronic document management systems have a certain feature: a system should be implemented in all workplaces, related to the creation, editing and storage of information (documents), or the efficiency of its use will be minimal. This approach immediately identifies one of the key implementation problems: conservatism of personnel, due to the reluctance of trained and retrained, and possibly, low education in the field of computer technology. This problem can to stall the whole process of implementation. This is especially true of organizations in which the personnel policy is conservative, and nobody, not even the head is not free to move or upgrade training.

Another problem for any organization under the current electronic document are permanent structural changes. This is required even if small, but all the restructuring of the system structure. In the absence of a part of the staff of specialists in the field of information technology, this process can take a lot of time at all, which in turn will lead to a simple production process and as a result, financial losses.

The third problem may lie in the complete absence of exchange document (even paper). In such a situation has its advantages. First and foremost is the lack of need someone to retrain. In addition, there are objective prerequisites for to convince the management to implement exchange document management system. If the leadership given a choice: to introduce archival paper or modern electronic, most likely that the latter will be chosen.

A serious problem is that if a large organization does not do any formal document, then it is constantly confronted with many challenges, and management does not always understand the reason for the lack of a formalized scheme of doing things. As a result, managers are constantly falls heap of problems, and they do not have time to understand the issues of document management systems. In this case it is necessary to carry out a gradual introduction of the system, to run, so to speak, a pilot project, the work of which will be invisible to the authorities, but the effectiveness of it still appears. This process can take several months before you see results. Support for the pilot project, as well as continued full implementation of the enterprise can result in a considerable amount.

Consider the main features and workflow issues in an organization or enterprise:

• The document management documents must be legally significant

• The documents can be divided into original and copy. Quite often, only to original documents received consideration. What would a copy of the document was the legal value it is necessary to assure a notary.

• Documents are the primary (cash receipt, invoice, certificate, report, etc.) and secondary. The primary document is the first evidence of the facts occurred and confirms validity of produced economic operation. It sets individual performers responsible for the performance of their business operations.

• If your organization has a large document (large volume of documents), then sooner or later the question arises about the correct storage of documents and the organization of the archive documents (document repository).

• When moving offices, or other difficult situations some of the documents may be lost or corrupted. When the competent organization of workflow, these risks can be minimized.

• If the wrong workflow or storage of documents is often difficult and time consuming to find the right document in a document repository or to make a thematic selection from the archive documents.

If you go to exchange electronic document, it is possible to minimize the risk of loss or damage of documents to facilitate the signing and transmission of documents, significantly reduce document storage costs.

These problems apply to all businesses regardless of their specificity. We now consider the specific archival institutions. These problems apply equally to them, that does not speak in favor of third parties. The archival institutions are quite extensive parks of computer technology, which have the potential to significantly improve the quality and efficiency of work with data. Nevertheless, the formation of a local area network, as well as the creation of a local network, only slightly impact on increasing the performance efficiency of the archival institution units.

In addition there are now many units of archival institutions use to exchange information rather inefficient methods described previously. There are no common standards on the size of incoming and outgoing data streams: one used drives, flash drives and other shared resources - which ultimately leads to disruption of the single information space of archival institutions and, in general, to the inability to find the necessary document. In many cases, departments keep up not only their own documents but also included, resulting from the work of other departments. The consequence of such an approach to the process workflow is a redundancy and low efficiency display the changes.

It follows from the foregoing that the archival institutions need to focus efforts not only on the development of the hardware platform, but also for the development of software that would allow the most efficient use possible of personal computers. As already mentioned the purchase of third-party software does not meet the archival institutions, not only in terms of financial costs, but also in terms of support staff and the introduction into the structure. In addition, the software market there are also systems developed by various organizations for their needs. The price of such programs are much lower, but they are designed for specific universities, and their use in archival institutions require serious revision.

The best solution for archival institutions is the creation of the necessary software on their own. The benefit of this solution is the fact that currently the archival institutions have sufficient intellectual capacity to create an electronic workflow system.

Description of the subject area

In general, the subject area covers all processes, actions and interactions that take place within the system, as well as between the system and the environment. Thus, this section is devoted to the description of the archival institution's structure, namely, the agency "Uzarhiv" its individual units and links between them.

USABILITY OF VISUAL EVOKED POTENTIALS AS BEHAVIORAL CHARACTERISTICS FOR BIOMETRIC AUTHENTICATION

Ubaydullayevna Iqbol Xolimtayeva

Tashkent, Uzbekistan

Abstract. *Biometric authentication methods are one of three approaches currently used. They offer a lot of benefits as well as they have few disadvantages. One of these disadvantages is low level of flexibility. It's not possible to change your biometric characteristic or even to increase number of your characteristics. This could be problem if we consider many systems with different level of security. Corruption of system with low level of security could help attacker to gain access to system with higher level of security. Solution of this problem could lie in use of behavioral biometric. The article introduces challenge-response approach in this area. We discuss possibilities of challenge-response biometric authentication and show new behavioral biometric suitable for this approach – visual evoked potentials. We give description of physiological features of this characteristic, discuss this properties and usability. We try to answer the question if it's suitable only for liveness testing or it's possible to use it for full authentication. Further we present design of prototype challenge-response biometric authentication system which takes advantage of visual evoked potentials.*

Keywords*: VEP; biometrics; authentication*

INTRODUCTION

In recent years, there is a great progress in area of biometric authentication and commonly used techniques are well designed and processed. Specifications of used devices are on high level as well as its effectiveness. In our opinion, there is one huge problem which remains - detection of fraud, when active attacker tries to impersonate to system as authorized user. Thus topic of protection against miscellaneous attacks comes to the forefront of the interests.

The main problem of biometric devices is a possibility of copying samples, which are used for biometric authentication. These samples are stable – what is, from criminalist point of view, one of the biggest advantages. On the other hand, there are techniques which allows attacker to obtain some biometrics samples, and start to experiment with them. "Gummy" fingers can serve us as an example. Obtained fingerprints can be used to create fake "gummy" finger, further usable for fingerprint reader confusion. Another example can be using printed pictures on iris recognition.

There are few solutions of this problem. The biggest success brings using sensors able do detect liveness of samples. Another solution is finding biometric characteristics, which are hard to steal without knowledge of relevant person. We should also try to gain and process real biometric response of person in dependency of concrete perceptions.

This article discusses new method which should potentially manage with problems mentioned above. The main idea is to process the reflexive behavior of human. We try to answer question of suitability of this method for user recognition and liveness testing.

As is well known, humans are not able to control behavior of their bodies if we deal with unconditional reflexes. Time response of reflexive behavior is much shorter then responses of conditional reflexes or non-reflexive reactions. In case we are able to gain samples which are unique on basis of stimulation, we should gain high-quality biometrics authentication which is hard to reproduce.

We are narrowly focused to searching for new utilizable eye feature suitable for biometrics authentication. In cooperation with medical professionals, we discover few new features applicable in following research. There are plenty of measurable characteristics of eyes known only to medical experts and despite that the majority of them are useless from biometric authentication point of view, there is one feature which seems to be very perspective. Specifically the ability of eye to generate electric charge on measurable level based on light stimulation. Thus we open here the idea of using visual evoked potentials (VEP) for biometric authentication. We give description of physiological features of this characteristic, discuss this properties and usability. We try to answer the question if it's suitable only for liveness testing or it's possible to use it for full-fledged authentication. Additionally, we present design of prototype challenge-response biometric authentication system which takes advantage of VEP.

PROBLEMS OF BIOMETRIC AUTHENTICATION

As well as other security measures, also biometric authentication is exposed to various types of attacks. There is a great number of biometric characteristic used for authentication [1, 4]. From that reason, there is also great variability in attacks applicable to them. These attacks are narrowly focused on concrete type of biometric and usually, they are not applicable to different type. Regardless, we can see to some extend analogy in these attacks.

Using of artificially "gummy" fingers on fingerprint systems can serves us as a good example [3]. Artificial copy of fingerprint from appropriate material is created on the basis of original finger print. This "gummy" finger exactly copies papillary lines of the original. Subsequently is used for gaining access to the target system. There are many useful applications of this method in practice. On the other hand, there are few methods (and development of new continues), how to protect fingerprint systems against this type of attack. There are usually based on modification of sensors acquiring biometric data. Let's mention for example use of electronic nose for gummy finger smell detection [2]. This method gets advantage of specific smell of latex or silicon, which are materials usually used for gummy finger creation. Electronic nose is able to detect this smells. Other protective methods are for example: determination of finger temperature, detection of blood pulse in finger, movement of sweat glands, deformation of papillary lines during enrollment etc. Here we can clearly see, that this specific attack has also specific countermeasures which are completely irrelevant in case of different biometric such a voice recognition.

One of the promoted approaches of fake detection in biometric authentication systems is so called liveness testing [7]. It is a test which confirm, that biometric sample comes from living person. Normal routine for authentication can safely take place after that. Liveness testing can be for example provided by human standing near sensor. Here we lose advantages of biometric authentication such a self-service. For all that is this approach usable in some cases. More often is liveness testing implemented directly into device as an automatic service.

In general, automatic liveness testing is based on three major areas. First is control of real properties of living human body such a conductibility, weight, color or shape. Second is control of signals generated by living human body – pulse, temperature, smell. Third area uses reaction of body such a pupil contraction as reaction on light. Also reactions on heat or cold are usable – sensor change its temperature and user hast to guess if it's colder or warmer. This is variation on challenge – response systems.

It is necessary to solve problem of fake detection, because fakes significantly affect security of biometric authentication systems.

Another problem which contemporary practice shows is also shortage of appropriate biometric. We can give a question why we need high number of biometric, why not to use only few widespread and most accurate systems. The answer is simple. There is expansion of system based on biometric authentication, which brings using of the same biometric samples over and over again. These cannot be changed and their number is limited (human has usually at most 10 fingers).

Unlike password, you cannot change your fingerprint. Here, you can see low flexibility of biometrics in case of compromising authentication mechanism. This can lies in acquiring of templates stored in database. Hereby attacker gains access to high quality images usable for example for fake creation.

In our opinion, it's not wise to use same biometric for all systems. Requirements for security of individual systems can be diametrically different. Corruption of authentication mechanism in weakly secured system could lead to direct danger of high secured system. Therefore, it's necessary to continue in research of biometric which doesn't suffer from these problems. Authentication based on visual evoked potentials could be a good candidate.

CHALLENGE-RESPONSE BIOMETRIC AUTHENTICATION

Idea of use challenge-response approach comes with searching for mechanism, which would increase security of biometrics. Use of behavioral biometric, which will be able to react on different stimulus, should solve some problems mentioned above, including liveness testing.

Challenger-response biometric authentication has special requirements and it is unclear which characteristic is suitable. The problem is that people are able to some degree learn, how to control their behavior and then attack systems based on behavior. Signature dynamics can serve as an example. It is possible to learn signature dynamics of other people as well as style of writing on keyboard.

Different situation arises if we attempt to use unconditional reflexes. Unconditional reflexes are reactions of your body to outer impulses, where people are not able to control these reactions. Knee-jerk reflex, intestine contractions or pupil dilatations are good examples of unconditional reflexes. As mentioned above, people are not able to control them, thus they are unable to wittingly misuse them.

Some medicals can be used to affect unconditional reflexes, but they do not provide enough granularity. We will discuss this problematic later.

Use of unconditional reflexes open possibility to think about biometric system based on challenge-response approach. System will generate stimulation, which will server as a challenge, and user will react in relation. We could gain high robustness while using biometric based on some appropriate unconditional reflex. First huge benefit of this method is impossibility of reaction control. This makes harder to misuse this biometric, particularly from two reasons: unawareness of challenge and problematic theft of reactions on this stimulus. Unawareness of challenge, which should vary, is not insurmountable problem. Attacker can try to authenticate and despite rejection, he can record and subsequently reproduce challenge. Bigger problem is theft of reactions on this

stimulus from targeted subject. While it's quite easy to acquire fingerprint from glass, measuring of unconditional reactions without knowledge of target will be nontrivial. In this phase, we could not imagine any technique how to gain this characteristic without restrictions of freedom.

Approach taking advantage of unconditional reflexes can be proper way to solving lack of biometric with high number of systems.

Challenge changes leads to altering conditions for authentication and allows us scale authentication for bigger number of different systems. One of following idea which is not in our focus is possibility of challenge changing during one single authentication process. This should help us refine selection of candidates etc. Here we move to deep speculations.

This article deals with one, from our point of view, suitable reflex - visual evoked potentials (VEP). The VEP as [6] specifies, is an evoked electrophysiological potential, that can be extracted, using signal averaging, from the electroencephalographic activity recorded at the scalp. This is, in essence, measurable reaction of brain in reaction on some kind of light stimulus. In presence, this reflexes are used in medicine (ophthalmology), where it servers to revelation of some diseases such a multiple sclerosis. There are standardized methods for measuring these signals for medical purposes. We want to use these techniques and verify appropriateness of VEP as biometric characteristic. Security oriented properties of resultant signal are yet unclear. Most generalized sample of VEP is used for comparison with real sample in medical examination, while for biometric authentication, we wants to take advantage of great variety of small differences in real data. We will discus detailed structure and properties of VEP later. Here we describe standardized medical examination which brought us to base idea - use results of this examination aka VEPs, possible little changed, for biometric authentication. Description of whole process is given to get the base idea.

DISCUSSION

As we mentioned above, the final product of measuring is curve with questionable level of uniqueness. From available data, we are not able to determine if the output is really unique for humans, because there is no medical study dealing with this question. But flash stimulus looks very promisingly and if our assumptions will prove true, the new possibilities in biometric authentication will open to us. What are requirements to take advantage of this biometrics in real life? First, it must provide sufficient differentiate ability and accuracy, to be able to differentiate individual persons. As well as fingerprints have got unique structure for each individual, it seems that curves which characterize reaction of individuals to light stimulations should have the same property. Another substantial requirement on biometrics is its stability. Repeated measuring must show sufficient similarity, in ideal case identity, namely in longer period of time. We can deal with more requirements, for example controllability by person, but they are not relevant at the moment. First it's necessary to prove the basic properties mentioned above. During discussion about properties of this biometrics, it is necessary to mention that there are few diseases which affect reactions of eye, but they come through in longer time interval. Moreover, there are drugs which should affect output signal. In our opinion this is only problem of service unavailability. Affecting of unconditional reflexes by drugs or disease only prevent access to the system, which could be restored after update of characteristic changed by disease or age.

The design of prototype of biometric authentication system

Although there is no prove about properties of measured feature, we should start to think about potential applications of this method. In dependence on variability of samples, we should get fully adequate and autonomous system which relies on this biometric (Figure 1). The authentication should be based on challenge – response principle, where challenge will be light sequence, respectively altering of chessboards or flash stimulus, and response will be according reaction. By contrast to medical application, we don't have to respect ordered properties of stimulus. This opens possibility for combination of biometric together with modifiable challenge. We should select values independently and thereby distinguish individual systems, because reactions will differ. Another possibility is in reactive authentication, where input will change in dependency on outputs. We can see that this method can be easily used for liveness testing. It is because of ability to react on alteration of frequency and resolution.

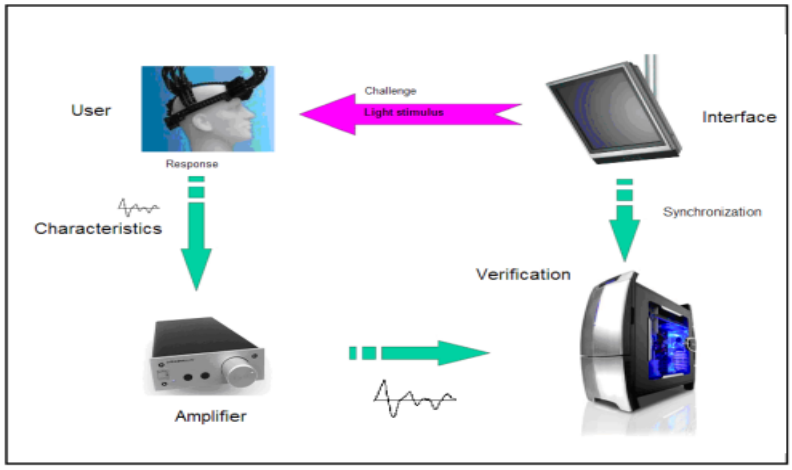


Figure 1. Structure of prototype biometric authentication system.

Here we can see potential of this biometric. Even it will not fulfill requirements for full biometric authentication, e.g. uniqueness and stability; it is still suitable candidate for additional controls (for ex. liveness testing) in combination with other type of biometric based on eye features.

Current Results

We are in the first phase of experiment which have goal primary to verify properties of VEP and secondary to create the methodology for measuring and further processing of VEP as biometric. After creating the testing database of samples, we can prove our assumptions which allow further research. At the present time, we are looking for device capable of capturing and measuring structure of charge.

First experiments were done with standard oscilloscope Fluke Scopemeter 123. It allows storing result in electronic form for further processing. Regrettably, after many measuring, we find out that this device don't provide sufficient accuracy. Moreover, result included lot of noise from surrounding environment, which we were unable to filter.

Thus we took advantage of having high-level oscilloscope with satisfactory capability to provide detailed results, for our needs. It should provide sufficient samples of charge. We have got few test samples and reaction for developing technique of filtering noise. Unfortunately, current results shows, that we still face the big imprecision of measuring and the result are unsatisfactory.

CONCLUSION AND FURTHER WORK

In this work, we present our idea of using unconditional reflexes for biometric authentication. This approach should enable to use challenge-response concept. We introduced suitable candidate – visual evoked potentials. VEP are adopted in medical applications, thus we introduce properties and methods which are used. We choose a proper candidate from different stimulus – flash stimulus, as ideal candidate for unconditional behavioral biometric characteristic. We presented design of prototype system for user authentication based on this biometric.

Our main goal is to prove appropriateness of our approach and creation of function prototype, which would demonstrate this biometric authentication method. Way to this prototype is complicated and further research is required. Techniques of measuring VEP must be checked on real EEG devices. Next step is creation of sufficient database of samples. This data will be used for finding suitable characteristic structure. Further methods of characteristic extraction and manners of its storing in database, must be designed. Here we can be inspired be already existing systems. Then algorithms for finding this characteristic and matching of samples must be implemented. In this phase, all resources for design and implementation of prototype system will be prepared.

Finally, we will get automatic tools for proving our challenge-response concept, which should bring easier scalability and personalization of biometric authentication systems.

REFERENCES

[1] Ashbourn, J.: "Practical Biometrics From Aspiration to Implementation", Springer, 2003, ISBN 1852337745

[2] Baldisserra, D., Franco, A., Maio, D., Maltoni, D.: "Fake Fingerprint Detection by Odor Analysis", Lecture Notes In Computer Science, Volume 2013, pp. 369 - 376, Springer-Verlag, 2001

[3] Cappelli, R., Maio, D., Maltoni, D.: "Modelling Plastic Distortion in Fingerprint Images", Proceedings of the Second International Conference on Advances in Pattern Recognition, pp. 369 - 376, Springer-Verlag, 2001

[4] Ratha, N.K.: "Guide to Biometrics", Springer, 2003, ISBN 0387400893

[5] Thorpe, J., van Oorschot, P.C., Somayaji, A.: "Pass-thoughts: Authenticating With Our Minds", In Proceedings of New Security Paradigns Workshop. Lake Arrowhead, 2005, pp. 45-56, ACM Press

[6] Odom JV, Bach M, Barber C, Brigell M, Marmor MF, Tormene AP, Holder GE, Vaegan Visual Evoked Potentials Standard (2004). Doc Ophthalmol 2004;108:115–123

[7] Woodward, J.D., Orlans N.M., Higgins P.T.: "Biometrics", McGraw-Hill/OsborneMedia, 2002, ISBN 0072222271

DAVLAT STANDARTLARI ASOSIDA AVTOMATLASHTIRILGAN O'LCHOV VOSITALARINI DASTURIY HIMOYALASH

Salimov Sardor Baxtiyor o'g'li
To'rayev Murod Baraka o'g'li
Yo'ldoshov Murod Xolmo'minovich
Botirov Fayzullajon Baxtiyorovich
Tashkent University of Information Technologies
named after Muhammad Al-Khorazmi,
Tashkent, Uzbekistan

Anotatsiya: Ushbu maqolada AES shifrlash algoritmining o'zgartirilgan ko'rinishi taklif etilgan. Taklif etilgan algoritm yordamida o'lchov vositalaridan olingan qiymatlarni har bir foydalanuvchi o'z shifrlash kaliti yordamida bazaning ayrim jadvallarini shifrlab saqlashi mumkin. Foydalanuvchilar turini o'lchash uchun olib kelingan qurilmalar asosida farqlashimiz mumkin. Yaratilgan dasturiy ta'minot autentifikatsiya, yangi foydalanuvchini ro'yhatga olish va ma'lumotlar bazasini shifrlash qismlaridan iboratdir. Ishning oxirida o'lchov vositalarida axborotlarni himoyalash bo'yicha tavsiya takliflar ishlab chiqilgan.

Kalit so'zlar: AES, shifrlash, kalit uzunligi, o'lchov vositalari.

AES-FIPS 197 standart simmetrik blokli shifrlash algoritmi. AES shifrlash algoritmi DES (Data Enctyption Standart) algoritmining ayrim kamchiliklarini bartaraf etish uchun ishlab chiqilgan, ya'ni:

kalit uzunligining kichigligi (56 bit);

S-blok akslantirishlarining differensial kriptotahlil usuliga bardoshsizligi boshqa sabablarga ko'ra eskirgan deb sanaladi. Ayniqsa 1999 yilda DES shifrlash algoritmi yordamida shifrlangan ma'lumotning Internet tarmog'iga ulangan 300 ta parallel kompyuter tomonidan yigirma to'rt soat davomida ochilishi haqidagi ma'lumotning tasdiqlanishi bundan keyin mazkur standart algoritmi yordamida ma'lumotlarni kriptografik muhofaza qilish masalasini qaytadan ko'rib chiqish va yangi standart qabul qilish zaruratini keltirib chiqardi.

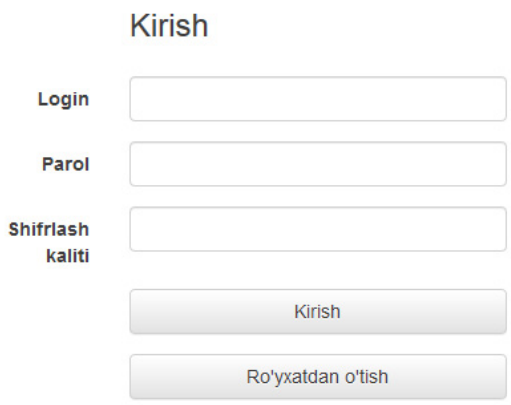
Amerika Qo'shma Shtatlarining "Standartlar va Texnologiyalar Milliy Instituti (NIST)" 1997 yilda XXI asrning ma'lumotlarni kriptografik muhofazalovchi yangi shifrlash algoritmi standartini qabul qilish maqsadida tanlov e'lon qildi. 2000 yilda standart shifrlash algoritmi qilib, RIJNDAEL shifrlash algoritmi asos qilib olingan AES (Advanced Encryption Standard) (FIPS 197) qabul qilindi. Algoritmning yaratuvchilari belgiyalik mutaxassislar Yon Demen (Joan Daemen) va Vinsent Ryumen (Vincent Rijmen) larning familiyalaridan RIJNDAEL nomi olingan.

AES FIPS 197 blokli shifrlash algoritmida 8 va 32-bitli (1-baytli va 4-baytli) vektorlar ustida amallar bajariladi. AES FIPS 197 shifrlash algoritmi XXI asrning eng barqaror shifrlash algoritmi deb hisoblanadi. Bu algoritm boshqa mavjud standart simmetrik shifrlash algoritmlaridan farqli o'laroq, Feystel tarmog'iga asoslanmagan blokli shifrlash algoritmlari qatoriga kiradi.

DES shifrlash algoritmida keltirilgan kamchiliklar AES shifrlash algoritmida oldi olingan bo'lishiga qaramasdan unda ham ayrim kamchiliklar aniqlangan. Ushbu ishda blokli shifrlash algiritmlari uchun qo'llaniladigan almashtirish jadvali S bloklarni samarali usul yordamida yaratish asos qilib olingan.

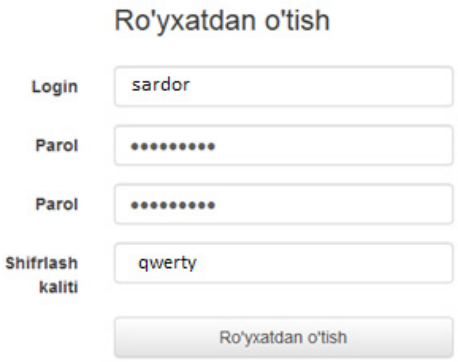
Avtomatlashtirilgan o'lchov vositalarining parametrlarini bazada himoyalash dasturiy vositasi

Yuqorida keltirilgan shifrlash algoritmi yordamida o'lchov vositalaridan olingan natijalarni bazada saqlash dasturiy ta'minoti ishlab chiqilgan. Ushbu dasturiy vosita foydalanuvchilarni ro'yhatga olish, autentifikatsiya, bazani shifrlash va deshifrlashni o'z ichiga oladi. Dasturning asosiy oynasi 1-rasmda berilgan. Unga ko'ra login va parolni kiritib tizimga kirish yoki Registratsiya qismi orqali yangi foydalanuvchi qo'shish mumkin.



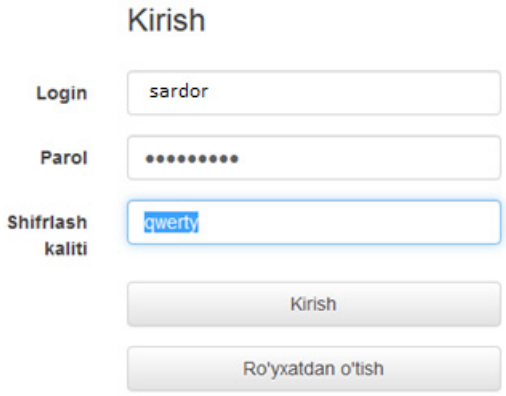
1-rasm. Dasturning kirish oynasi

Registratsiya oynasida foydalanuvchi familiyasi, ismi, logini va paroli kiritiladi, shundan so'ng ro'yhatga olish jarayoni yakunlanadi (2-rasm).



2-rasm. Yangi foydalanuvchi yaratish

Ro'yhatdan o'tgan foydalanuvchi login va parolini kiritib, o'ziga biriktirilgan ma'lumotlar bazasi jadvalini shifrlashi mumkin.



3-rasm. Tizimga kirish

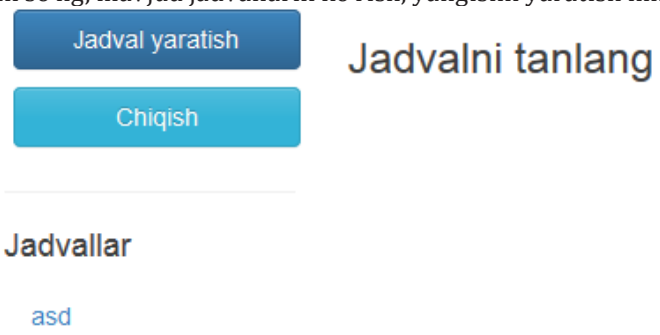
Ro'yhatdan o'tgan foydalanuvchining login va parollari bazada shifrlangan ko'rinishda saqlanadi.

secure_db_users.db_users: 5 всего строк (приблизительно)

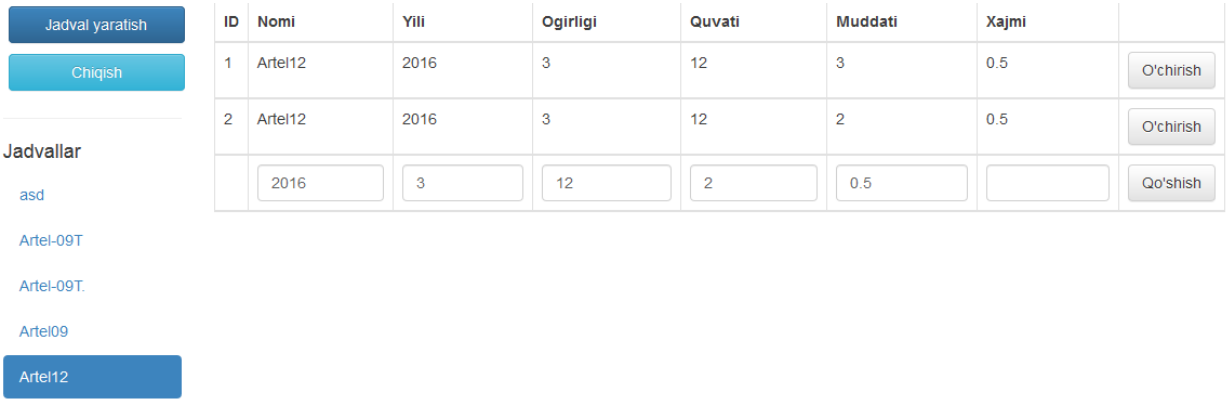
id	login	pass	aes
1	as	df211ccdd94a63e0bcb9e6ae427a249484...	a94a8fe5ccb19ba61c4c0873d391e98798...
2	najmiddin	6506c773978f99efb7a15d5da0be153657...	b1b3773a05c0ed0176787a4f1574ff0075f...
3	najmiddin	6506c773978f99efb7a15d5da0be153657...	f7c3bc1d808e04732adf679965ccc34ca7a...
4	Admin	d033e22ae348aeb5660fc2140aec35850c...	f7c3bc1d808e04732adf679965ccc34ca7a...
5	user	12dea96fec20593566ab75692c99495968...	7c4a8d09ca3762af61e59520943dc26494f...

4-rasm. Parol va kalitning bazadagi ko'rinishi

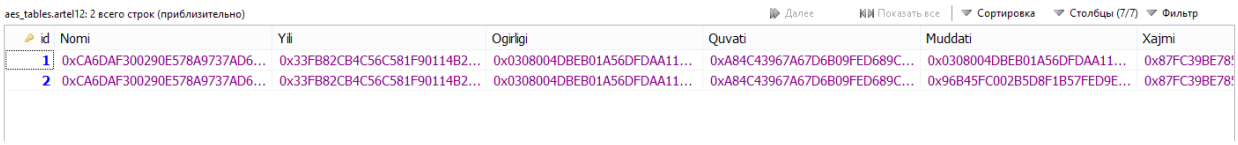
Tizimga tashrif buyurgandan so'ng, mavjud jadvallarni ko'rish, yangisini yaratish imkoniyati paydo bo'ladi.



5-rasm. Mavjud jadvallar



6-rasm. Jadval maydonlarini to'ldirish



7-rasm. Bazada shifrlab saqlash

Ushbu dastur yordamida standardga tekshiruvchi bir hodim o'ziga tegishli mahsulotning xususiyatlarini bazada saqlash imkoniyatiga ega bo'ladi. Boshqa hodim o'zidan boshqaning ma'lumotlarini o'qiy olmaydi.

8-rasm. Boshqa foydalanuvchida o'zidan boshqaning ma'lumotlari "null" bo'lib ko'rinadi

Xulosa

Taklif etilgan algoritm yordamida yaratilgan dasturiy ta'minot orqali metrologik o'lchashni amalga oshiruvchi hodim o'lchash parametrlarini bazada shifrlab saqlash imkoniniga ega bo'ladi. Buning natijasida, ma'lumotlar bazasidagi o'lchash natijalarini qalbakilashtirish, o'zgartirish va qayta foydalanish xujumlaridan himoyalash mumkin. Bundan tashqari o'lchov vositalaridan olingan qiymatlarni bazada saqlab, hosil bo'lgan bazani har bir foydalanuvchi o'zi uchun shifrlab qo'yishi mumkin. Foydalanuvchilar turini o'lchash uchun olib kelingan qurilmalar asosida farqlashimiz mumkin. Yaratilgan dasturiy ta'minot autentifikatsiya, yangi foydalanuvchini ro'yhatga olish va ma'lumotlar bazasini shifrlash qismlaridan iboratdir. Ishning oxirida o'lchov vositalarida axborotlarni himoyalash bo'yicha tavsiya va takliflar ishlab chiqilgan.

Foydalanilgan adabiyotlar

1. Ismatullayev P.R., Maqsudov A.N., Abdullayev A.X., Ahmedov B.M., A'zamov A.A.Metrologiya, standartlashtirish va sertifikatlashtirish. — T.: «O'zbekiston» 2010.
2. Абдувалиев А.А. и др.Стандартизация, метрология, сертификация, качество. — Т.: НИИСМС, 2012.
3. Ким К.К., Анисимов Т.Н., Барборович В.Ю., Литвинов Б.Я.Метрология, стандартизация, сертификация и электроизмерительная техника. — СПб.: «Питер», 2011.
4. Nurmuhamedov N.K., Karimov A., Salimov S.B. "Metrologik o'lchash vositalariga asosiy tahdidlar". XXVI Международной научной конференции «Актуальные научные исследования в современном мире». 26-27 июня 2017г. Украина.
5. Nurmuhamedov N.K., Salimov S.B. "Metrologik o'lchash vositalarini himoyalash usullari". XXVI Международной научной конференции «Актуальные научные исследования в современном мире». 26-27 июня 2017г. Украина.

СТЕГАНОГРАФИЯ ИЗОБРАЖЕНИЙ И СТЕГОАНАЛИЗ

Имамалиев Айбек Тураббаевич
Халимтаева Икбол Убайдуллаевна
Салимов Сардор Бахтиёр угли
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий,
г. Ташкент, Республика Узбекистан

Аннотация: *Стеганография скрывает информацию в нескольких обложках, например текст, изображение, аудио, видео или протоколы. Существует несколько методов стеганографии для скрытия секретных данных в цифровых изображениях, некоторые из них более сложные, чем другие. Однако все они имеют свои преимущества и недостатки. Этот документ намеревается дать понимание и эволюцию различных существующих типов и анализов стеганографии цифрового изображения. Он объединяет исследовательскую работу по стеганографии и стеганализу. Битва между стеганографией и стеганализом бесконечна. В этой статье представлен отчет о стеганографии и стеганализе.*
Ключевые слова: *стеганография, стегоанализ, LSB, стего-изображения.*

IMAGE STEGANOGRAPHY AND STEGOANALYSIS

Abstract: *Steganography hides information in several covers, for example text, image, audio, video or protocols. There are several methods of steganography for hiding secret data in digital images, some of them more complex than others. However, they all have advantages and disadvantages. This document intends to give understanding and evolution of various existing types and analyzes of digital image steganography. He combines research on steganography and steganalysis. The battle between steganography and steganalysis is endless. This article presents a report on steganography and steganalysis.*
Key words: *steganography, stegoanalysis, LSB, stego-image.*

Введение

В интернет-связи одним из важнейших факторов информационной технологии и коммуникации является безопасность информации. Ежедневные тонны данных передаются через Интернет по электронной почте, сайтам обмена файлами, сайтам социальных сетей. По мере роста числа пользователей Интернета понятие «безопасность в Интернете» также приобретает очень большое значение. Цель стеганографии заключается в том, чтобы скрыть само присутствие коммуникации, вставив сообщения в безобидные объекты обложки. В сегодняшнем цифровом мире невидимые чернила и бумага были заменены гораздо более универсальными и практичными обложками для скрытия таких сообщений, как цифровые документы, изображения, видео и аудиофайлы. До тех пор, пока электронный документ содержит информацию, не имеющую отношения к делу или избыточную информацию, ее можно использовать в качестве обложки для скрытия секретных сообщений. Каждая система стеганографической связи состоит из алгоритма внедрения и алгоритма извлечения. Чтобы разместить секретное сообщение, исходное изображение, также называемое обложкой, модифицируется алгоритмом внедрения. В результате вложения получается стего-образ.

Процесс скрытия данных в стеганографии начинается с идентификации избыточных битов обложки. Резервные биты - это биты, которые могут быть изменены без разрушения его целостности. Затем процесс внедрения создает стего-образ, заменяя эти избыточные биты битами сообщения, которое должно быть скрыто. В стеганографии цифрового изображения секретное сообщение встроено в цифровое изображение, называемое обложкой. “Coverimage”, несущий встроенные секретные данные, называется “stegoimage”.

Стеганография изображений

Изображения - самые популярные обложки, используемые для стеганографии. В области цифровых изображений существует множество различных форматов файлов изображений, большинство из кото-

рых предназначено для конкретных приложений. Для этих разных форматов файлов изображений существуют различные стеганографические алгоритмы [3].

Стеганография изображений определяется как скрытое вложение данных в цифровые изображения. Хотя стеганография скрывает информацию в любом из цифровых медиа, цифровые изображения являются самыми популярными в качестве носителя из-за их частотного использования в Интернете. Поскольку размер файла изображения большой, он может скрыть большой объем информации. HVS (Human Visual System) не может отличить нормальное изображение и изображение со скрытыми данными. В дополнение к тому, что цифровые изображения включают большое количество избыточных бит, изображения стали наиболее популярными обложками для стеганографии. Следовательно, это исследование использует изображение в качестве файла обложки. В качестве обложек можно использовать различные форматы изображений, такие как файлы JPEG, BMP, TIFF, PNG или GIF. Формат растрового изображения или BMP - это простой формат файла изображения. Данные легко манипулировать, поскольку он несжатый. Но несжатые данные приводят к большему размеру файла, чем сжатое изображение. JPEG (Joint Photographic Expert Group) - наиболее часто используемый формат файла изображений. Он использует метод сжатия с потерями; Качество изображения отличное. Размер файла также меньше. Формат TIFF использует сжатие без потерь. Файл разработан без ущерба для качества изображения [2].

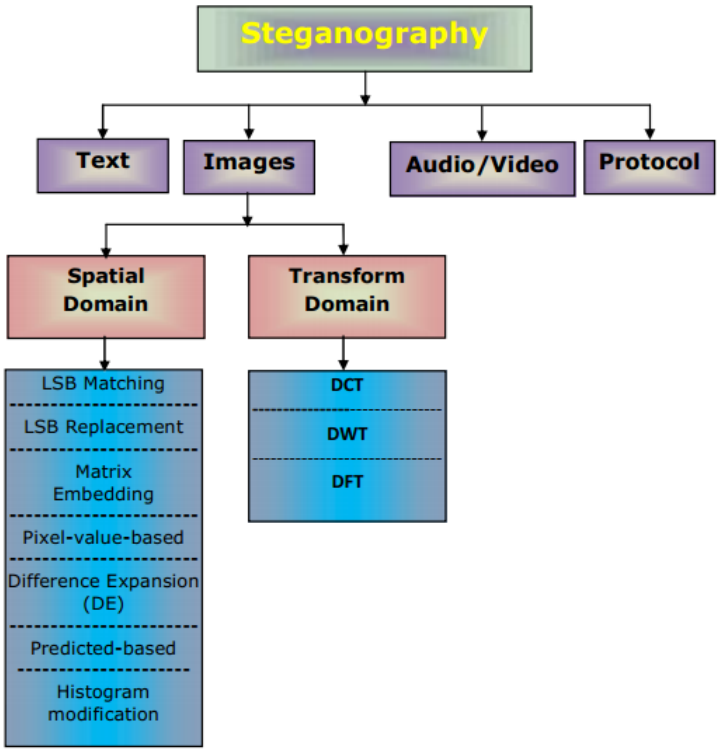


Рис. 1. Классификация стеганографии изображений

Пространственная и трансформированная доменная стеганография. Основываясь на способе внедрения данных в изображение, методы стеганографии изображений можно разделить на следующие группы:

1. Пространственный домен или область изображения.
2. Преобразовать домен или частотный домен.

Пространственный домен. Этот метод напрямую встраивает сообщения в интенсивность пикселей. Некоторые из методов пространственной области:

1. Совпадение наименее значимого бита (LSB).
2. Замена наименее значимого бита (LSB).
3. Матричное вложение.
4. Спряжение изображения на основе пикселя.
5. Различия Расширение (DE).
6. Изменение гистограммы.
7. Прогнозируемое скрытие изображения.

Преобразовать домен. В преобразованном пространстве, изображения сначала преобразовали, а затем сообщение встраивается в нее. Это надежные методы для сокрытия данных. Это более сложный способ, чтобы скрыть секретное сообщение в изображение. Он выполняет данные скрываются путем манипулирования математических функций и преобразований изображения. Трансформация чехла изо-

бражения осуществляется путем небольшой коррекции коэффициентов и инвертирует трансформации.

Метод LSB

Техника наименьшей значимости встраивания - самая популярная техника стеганографии. В зависимости от двоичного кодирования секретного сообщения оно скрывает сообщение в двоичном кодированном изображении. На приведенном ниже рисунке изображены значения пикселей и секретные сообщения. LSB вносит изменения в изображение, которое очень легко распознается, и стего-изображения легко атаковать.

Шаги для скрытия сообщения с использованием метода LSB:

1. Выберите правильное изображение для обложки.
2. Сканируйте изображение по строке и закодируйте его в двоичную форму.
3. Кодируйте секретное сообщение в двоичную нотацию.
4. Вычислите размеры изображения и секретного сообщения.
5. Рассмотрим один пиксель изображения.
6. Разделите изображение на три части (красная, зеленая и синяя части).
7. Спрячьте два-два бита секретного сообщения в каждой позиции пикселя на последних двух значимых позициях.
8. Задайте изображение с новыми считанными значениями.
9. Установите изображение и сохраните его.

Метод LSB скрывает секретный текст как минимум за два значащих бита пикселей изображения. Следовательно, изменение значения пикселей изображения влияет на разрешение изображения, что в конечном итоге приводит к снижению качества изображения и делает изображение легким для атаки. Этот метод LSB уже атакован и сломан. Поэтому в продвинутом LSB мы скрываем секретное сообщение, основанное на поиске идентичных значений между пикселями изображения и секретными сообщениями. Изображение, показанное ниже, дает четкое представление о расположении бит в пикселе изображения. Алгоритм расширенного метода LSB. Шаги для скрытия сообщения с использованием метода LSB. Стеганография сегментации с плоской плоскостью была введена Кавагути и др. Основная идея заключается в том, что более высокие битовые плоскости могут также использоваться для встраивания информации. Здесь каждый блок разбивается на бит-плоскость. Плоскость LSB изображения будет бинарным изображением, состоящим из LSB каждого пикселя в изображении и так далее. В каждой сегментированной битовой плоскости анализируется ее сложность. И на основе порогового значения блок делится на информационную область и шумоподобную область, а секретные данные скрыты в зонах шума без ухудшения качества изображения. Этот метод обеспечивает высокую вместимость и наименьшее ухудшение изображения обложки по сравнению с традиционными методами манипуляции LSB.

Обнаружение LSB скрывает.

Предыдущий метод используемый для того чтобы обнаружить скрывающихся LSB является 2 (хи-квадрат) метод успешно используется для stegdetect для обнаружения LSB прячется в коэффициентах в формате JPEG. Еще одна схема обнаружения LSB был предложен использованием бинарной меры сходства между 7-й бит самолет и 8-й (наименее значимый) бит самолет. Предполагается, что существует естественная корреляция между битовых плоскостей, что нарушается LSB скрывает. Эта схема не автоматическая калибровка на основе изображения, и вместо калибрует на обучающем наборе крышки и стеганографические изображений. Схема работает лучше, чем универсальный схема стегоанализа, но не так хорошо, как государство-оф-арт- LSB стегоанализа. Еще одна схема для обнаружения LSB был предложен используя бинарные меры сходства между 7-й бит самолет и 8-й (наименее значимый) бит самолет. Предполагается, что существует естественная корреляция между битовых плоскостей, что нарушается LSB скрывает. Эта схема не автоматическая калибровка на основе изображения, и вместо калибрует на обучающем наборе крышки и стеганографические изображений. Образец пара анализ является более тщательного анализа, из-за основе метода RS, объясняя, когда и почему это работает. Развратник использует оценки совместной вероятность массового функция (BMP) для повышения частоты выявления пар образцов анализа RS. Фридрих использует локальные оценки, основанные на кварталы пикселей, чтобы немного улучшить обнаружение LSB за RS.

Заключение

В этой статье представлен обзор различных типов стеганографии и методов изображения. Обсуждаются некоторые из инструментов стеганографии.

В этом документе были представлены исследовательские работы в области стеганографии, развернутые в областях пространственного, преобразования и сжатия цифровых изображений. Методы преобразований домена изменяют частотные коэффициенты, а не напрямую манипулируют пикселями изображения. Следовательно, искажение минимально и, следовательно, предпочтительнее, чем методы пространственной области. Но для хорошей встраивающей способности методы пространственной области дают лучшие результаты. Существует компромисс между качеством изображения и способностью встраивания.

В этой статье представлен, проанализирован и внедрен новый метод стеганографии. Предлагаемый метод скрывает секретное сообщение на основе сравнения и поиска наименее значимых бит изображения RGB в порядке (3 бита к R-компоненту, 3 бита к компоненту G, 2 бита к B-компоненту), с помощью которых мы можем скрыть Один символ в одном пиксельном изображении, так что для скрытия секретного сообщения требуется только соответствующее количество пиксельных изображений. Хотя мы выбираем изображение в пикселях случайным образом, изображение не будет затронуто в вопросах разрешения и ясности. Предлагаемый метод сравнивали с LSB и продвинутыми методами LSB, которые скрывали данные в наименее значимых битах и одинаковых битах. Предлагаемые и методы LSB использовались для реализации stego-изображения для секретного сообщения по количеству разных изображений. Результаты предложенных и методов скрытия LSB анализировались на основе среднего исходного изображения и изображения. В этом документе делается вывод, что предложенный метод стегонографии является высокоэффективным, точным и точным, чем предлагаемые методы LSB, он начинает сравнивать и искать идентичные биты в пиксельном изображении и скрывает данные в нем, так что разрешение и качество Изображения никогда не будут затронуты и обеспечат безопасность сообщения. Экспериментальные результаты также показывают, что коэффициент эффективности предлагаемого метода относительно высок по сравнению с существующими методами.

Список использованных источников:

1. Dr.M.Umamaheswari, Prof.S.Sivasubramanian, S.Pandiarajan, “Analysis of Different Steganographic Algorithms for Secured Data Hiding”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.
2. Asha Pathak, Vrushali Bhuyar, “Image Steganography and Steganalysis : A Survey”, International Journal of scientific research and management (IJSRM), Volume 2, Issue 12, Pages 1753-1757, 2014.
3. T. Morkel, J.H.P. Eloff, M.S. Olivier, “An overview of image steganography”.

VARIETY AND CLASSIFICATION OF MATHEMATICAL MODELS OF SECURITY OF COMPUTER SYSTEMS

Irgasheva Durdona Yakubdjanovna, Salimov Sardor Baxtiyor ugli

Tashkent University of Information Technologies

named after Muhammad Al-Khorazmi,

Tashkent, Uzbekistan

***Abstract**: The paper reviews and analyzes security models for the reliability of the information security system in the user's access to information resources requiring the performance of protective functions.*

***Keywords**: computer systems, security models, subject, object, discretionary access control model, mandatory access model, role model with access demarcation.*

Currently, it pays more attention to information security. And this is obvious. The large normative and theoretical base, formal mathematical methods that justified most of the concepts were created. Earlier the concepts formed only by verbal descriptions. The developers of security systems that implement the various techniques and methods to counter threats to information6 try as much as possible to facilitate the work safety administration. To do this, in the majority of the information systems used standard approaches that are the result of the experience of the developers of such protection systems. Development of information protection system must realize a security policy and with this full and accurate verification of its conditions must also be realized. Security policy - a set of rules defining the set of feasible actions in the system. There are special security models in which systems operate on a strictly defined set of rules and implement any security policy.

All the mathematical models of security of computer systems are classified into five main types:

- Models of discretionary access control systems;
- Models of mandatory access control systems;
- Models of security of information flows;
- Models of role-based access;
- Subject-oriented model sandbox.

Nowadays, the most effective and used mathematical models of computer systems considered as a model of discretionary systems, mandate and role-based access control.

Classification scheme and the relationship of the provisions under consideration of mathematical models of computer systems security fully shown in Fig. 1.

Model discretionary access control systems.

This model is characterized by the differentiation of access between the named subjects and objects. A subject with a certain access rights may transfer this right to any other entity. For each pair (subject - object) must be given a clear and explicit enumeration of permissible types of access (read, write, etc.), which are authorized for a given subject (individual or group of individuals) to this resource (object). There are at least two approaches to building Discretionary Access Control:

- each system object has attached to it a subject called the owner. It is the owner establishes the right of access to the object;
- the system has selected one subject - the root, which has the right to establish ownership for all other entities of the system.

There are variants of mixed and when simultaneously present in the system as the owners of establishing rights of access to its facilities, as well as the superuser, has the ability to change the rights for any object and / or change its owner. It is this mixed version implemented in the majority (UNIX or Windows family NT) operating systems.

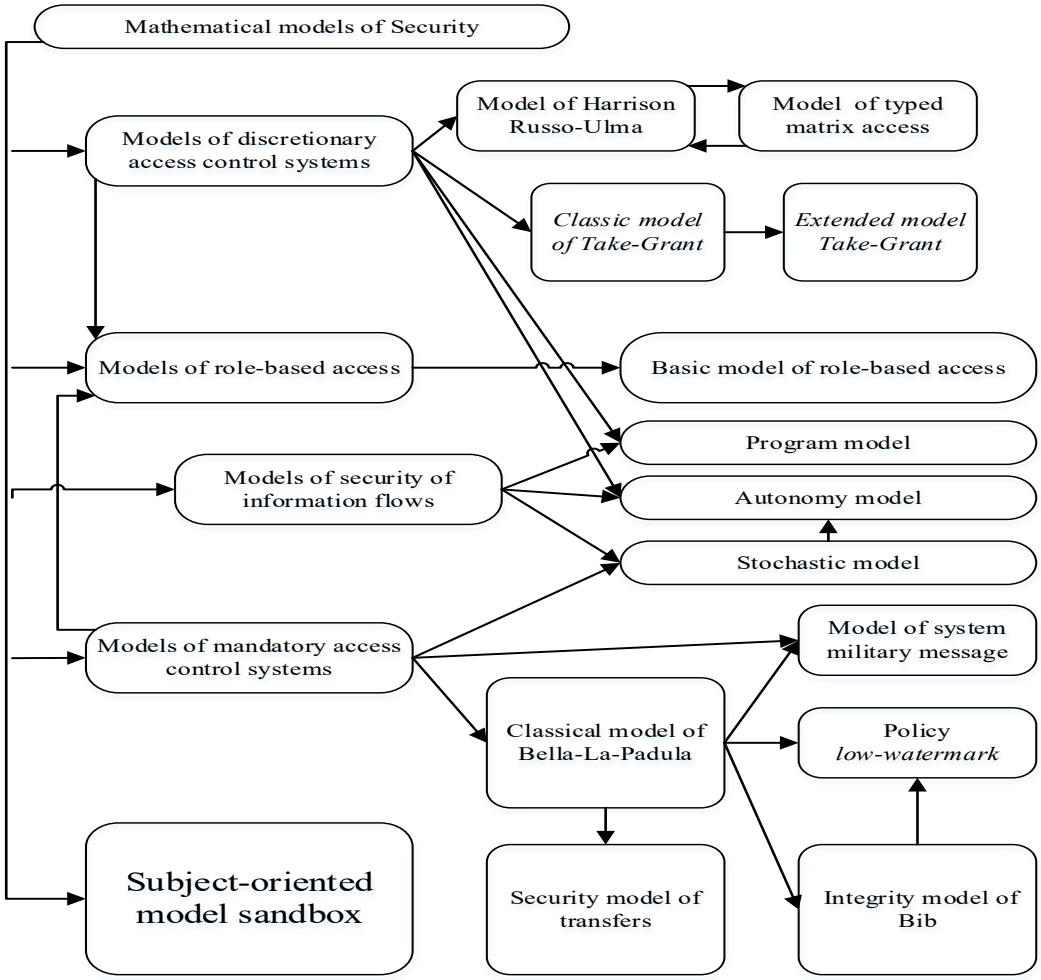


Fig. 1. Diagram of the classification and the relationship of the provisions of mathematical models of computer systems security

Discretionary access control is the basic implementation of a differentiating policy of access to resources in the processing of confidential information in accordance with the requirements for information security.

Models of mandatory access control systems.

To implement this principle, each subject and object should be compared classification labels that reflect the place of the subject (object) in the corresponding hierarchy. Through these tags to subjects and objects must be assigned classification levels (levels of vulnerability, privacy category, etc.), is a combination of hierarchical and non-hierarchical categories. These tags should be the basis of the principle of mandatory access control. SGC when you enter new data into the system must request and receive from the authorized user classification labels of the data. When an authorized user entering in the list of the new entity should be a comparison of his classification labels. External classification label (subjects, objects) should correspond exactly to the inner label (inside LTV).

Models of role-based access.

The main role-based access control idea is the idea of linking the access permissions with the roles allocated to each user. This idea came simultaneously with the advent of multi-user systems. However, until recently, researchers paid little attention to this principle.

Role-based access control is a development of the discretionary access control policies, with the right to access the system of subjects to objects are grouped in accordance with their specificity of their application, forming part.

This access control is a component of many modern computer systems. Usually, this approach is applied in the database protection system, and the individual elements are implemented in the network operating systems.

Role Assignment allows you to define a clear and understandable for users of the computer system of access control rules. At the same time, this approach is often used in systems for users that clearly defined the scope of their official duties and responsibilities.

The role is a set of access rights to the objects of the computer system, but the role-based distinction is not a special case of a discretionary distinction, as its rules determine the procedure for granting access rights to subjects of a computer system according to the session of his work and of existing (or absent) in his roles each moment of time, which is typical for mandatory access control systems. On the other hand, the rules of role-based access control are more flexible than the Credentials approach to differentiation.

Subject-based model sandbox.

In this model, it is believed that subjects generated other subjects (active entities) of the object (a passive entity). The concept of object and associated subject. To talk about it if the object state affects state the subject the next time (it is believed that the system discrete time). An entity shall display the associated object at the time / on the set associated object at time / + I. This may select a subset of objects (transmitter), a change that involves a change in the subject of other objects (receivers). As a result, we get the information thread between two objects. This flow has the property of transitivity. Access subject to the object is called the product of the flow of information between a certain object and the object access. Among the streams there are legal and unauthorized. The security policy describes the decomposition of flows on these two sets. Terms of access control has formally description legal flows.

To split all the threads on the set of legal and unsectioned allocated a special entity that activate in any stream and is able to classify limits - reference monitor. It turns out the concept monitor security objects (IBA) - a reference monitor, allowing only legal flows (transactions on the object). However, when you change the objects associated with the IBO can change himself IBO, therefore introduced the concept of the correctness of the subjects, or they do not affect each other. Two subjects to names mutually correct, if at any time there is no flow between two objects associated with these subjects. We absolutely correct subjects' sets associated objects do not intersect at all.

The introduction of the concept of absolute correctness allows forming sufficient conditions for the implementation of only legal access. For all subjects in this system, including the SBC must be totally correct with respect to each other. This is a rather hard and fast rule, and at first glance it is not clear how to solve the problem of the correctness of the subject generated and the IBO. Help comes the introduction of the concept of subjects of the security monitor (MBS) - a subject that allows the generation only a subset of pairs of subjects and objects of activating sources.

The computer system, in which there is MBS, called closed. If the generated entities are absolutely correct concerning each other and MBS, the system is called a closed isolated. Below is shown and proved a theorem describing a sufficient condition for guaranteed execution policy no-danger in the computer system: "If in an isolated environment, there program IBO and generated by actors absolute correct with the IBO, MBS and others, as well as MBS absolutely correct from SBC, the SBC in a software environment allows only the legitimate offspring of flows".

In order for a software environment was always isolated (and hence guaranteed to be secure), you must request that the product of the subjects accompanied control immutability of their parent objects.

To summarize, then each of these contact systems have their advantages, but the key is that none of these models is not standing still and develops dynamically. Proponents have each of them, but objectively looking at things, it is difficult to give preference to any one system. They are just different and serve different purposes.

REFERENCES

1. Devyanin P.N. Models of security of computer systems: Textbook for High Schools.-M .: Publishing Center: Academy, 2005. - p. 144.

2. Ganiev S.K., Karimov M.M., Irgasheva D.Y. On the way of delimiting access to information resources in telecommunication systems // International Scientific and Practical Conference/Innovation - 2009: Collection of scientific articles. - Tashkent, 2009.- p. 287-289.

3. M.M. Karimov, D.Ya.Irgasheva, K.A.Tashev, R.I. Rakhimov. Effective Model Of System Of Detection Of Intrusion For Computer Networks. ICEIC: International Conference on Electronics, Informations and Communications. 2008.

METADATA STANDARD FOR DIGITAL ARCHIVES MANAGEMENT SYSTEM OF ARCHIVAL INSTITUTIONS OF UZBEKISTAN

Mukhammadjonov Sherzod

Department of Information and Library Systems
Tashkent University of Information Technologies named after al-Khwarizmi, Uzbekistan

Abstract*. This paper explores several metadata standards, which used in archives management systems (AMS). It introduces the digital preservation problems and notes the importance of metadata for the archival institutions of Uzbekistan. The experience of using archival metadata standards is analyzed in this research. It studies different metadata formats for archives. And suggests ISAD(G) as a main standard in creation of digital archives.*

Keywords*: metadata, metadata standard, archival information system, digital archives, records management, recordkeeping, ISAD(G).*

Introduction

At present time for archival institutions of Uzbekistan, there is the problem of steady increase of various documents, both paper and digital forms. Besides, accounting and storage of huge volume of different types of information resources, especially, multimedia and their granting to users without special software and hardware complicates work of archives. It is important to create digital archives and archival networks for long-term preservation of information, as well as the exchange of records between archives. Digital archives are necessary for the effective operation of modern archival institutions. The main issue is to develop AMS based on metadata standard. Electronic metadata makes the digital archives go round. The digital world also works better when there are standards. Standards encourage best practice. They help the end user by encouraging the adoption of common platforms and interfaces in different systems environments.

Today only in the Central State Archives (CSA) of Uzbekistan there is a software called Archive Documents Management System (ADMS), which is being used over 9 years. This system was designed for automation of the main archival processes. It has all the basic functions, such as attaching and classifying documents, archival description, searching and browsing, etc. But ADMS has its own metadata schema that is not well constructed. With the growing number of records in the database, it becomes difficult to search and browse documents.

Other institutions use their own archival systems, which differ from the ADMS and are quite simple, some archives still use Microsoft Access or Excel sheets to store records. That's why we need to create metadata standard to use in development of archival systems. Electronic metadata makes the digital world go round (Cunningham, 2001). The digital world also works better when there are standards. Standards encourage best practice. They help the end user by encouraging the adoption of common platforms and interfaces in different systems environments.

Research goals and objectives

The objective is to choose international metadata standard for adapting or creating new national standard on its basis. Metadata format for using in development of digital archives in archival institutions should be defined. What metadata standards exist? What is the purpose of different standards? What is the difference between them? What we need to pay attention to the use of metadata standards? To answer these questions the local and foreign experience on this field is analyzed, using metadata standard in foreign archives is studied. This paper attempts to review some recent initiatives that relate to preservation metadata for digital archives.

Metadata standards for Recordkeeping

Here is a definition of the standard given by The British Standards Institution, the oldest organization for standardization (1901): "In essence, a standard is an agreed way of doing something. It could be about making a product, managing a process, delivering a service or supplying materials – standards can cover a huge range of activities undertaken by organizations and used by their customers. It is a published document that contains a technical specification or other precise criteria to be used systematically as rules, guidelines or definitions. Standards help to make life easier and increase the reliability and efficiency of products and services that we use"[1].

In the table 1 the list of the main international standards on records and archives management are given.

1 The British Standards Institution (BSI) http://www.bsigroup.com/en-GB/standards/Information-about-standards/what-is-a-standard/

Table 1. Main international standards on records and archives management

International Organization for Standardization (ISO)	
ISO 15489 (2001, 2016)	Records management (Part 1 & 2)
ISO 18492 (2005)	Document Management Applications, Long-term preservation of electronic document-based information
ISO 22310 (2006)	Guidelines for standards drafters for stating records management requirements in standards
ISO 23081 (2006; 2009 and 2011)	Records management processes, Metadata for records (Part 1–3)
ISO 26122 (2008)	Work process analysis for records
ISO/TR 13028 (2010)	Implementation guidelines for digitization of records
ISO 16175 (2010 and 2011)	Principles and functional requirements for records in electronic office environments (Part 1 to 3)
ISO 30300 and ISO 30301 (2011)	Information and documentation, Management systems for records
ISO 13008 (2012)	Digital records conversion and migration process
ISO 14721 (2012)	Space data and information transfer systems - Open Archival Information System (OAIS) - Reference model
ISO 16363 (2012)	Space data and information transfer systems - Audit and certification of trustworthy digital repositories
ISO 17068 (2012)	Trusted third party repository for digital records
ISO/IEC 17826 (2012)	2012 Information Technology/Cloud Data Management Interface (CDMI)
ISO 14641-1 (2012)	Electronic archiving – Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation
International Council on Archives (ICA)	
ISAD(G)	General International Standard Archival Description
ISDIAH	International Standard for Describing Institutions with Archival Holdings
ISDF	International Standard for Describing Functions
ISAAR(CPF)	International Standard Archival Authority Record for Corporate Bodies, Persons and Families, Second edition
ICA	Principles of Access to Archives
ICA	Guidelines for developing a retention schedule for records management and archival professional associations, including a model retention schedule
ICA	Code of Ethics for Archivists
Other standards and formats	
DOD 5051.2	Electronic records (US National Archives)
MoReq2 (European Union)	Requirements for the Management of Electronic Records
DUBLIN CORE	The Dublin Core Element Set Version 1.1
MARC	MAchine-Readable Cataloguing MARC 21 Concise Format for Bibliographic Data
EAD	Encoded Archival Description
MODS	Metadata Object Description Schema

These standards are used in different archival institutions in the world.

In 2001 International Standard Organization (ISO) has developed ISO 15489-1:2001 Information and documentation – Records management – Part 1: Concepts and principles (ISO 15489). A year ago the International Organization for Standardization (ISO) began selling a "technically revised" edition of the same name with the designation of ISO 15489- 1:2016, which cancels and replaces its predecessor (Barnes, 2016). One of the main part this standard is devoted to archives/records management, focusing management systems for records and metadata.

The Library of Congress archival collections and finding aids are created using the Encoded Archival Description (EAD), an international standard maintained by the Library of Congress in partnership with the Society of American Archivists[2].

The International Council on Archives (ICA) has developed a general standard for archival description called International Standard for Archival Description (General) (ISAD(G))[3]. According to ISAD(G), archival description proceeds from general to specific as a consequence of the provenance principle and has to show, for every unit of description, its relationships and links with other units and to the general fonds. Therefore, archival descriptions

2 EAD Best Practices at the Library of Congress - https://www.loc.gov/rr/ead/lcp/

3 International Council on Archives. ISAD(G): General International Standard Archival Description, 2nd edn. International Council on Archives, Ottawa (2000)

produced according to the ISAD(G) standard take the form of a tree which represents the relationships among more general and more specific archive units going from the root to the leaves of the tree.

In order to respect ISAD(G) principles, archival description metadata should meet the following three main requisites (Ferro, N., Silvello, G., 2008):

1. Context: archival description metadata have to retain information about the context of a given record, such as the relations between records and with the production environment, as stated by the respect des fonds principle discussed above.

2. Hierarchy: archival description metadata have to reflect the archive organization which is described in a multi-leveled fashion, as defined by ISAD(G).

3. Variable granularity: archival description metadata have to facilitate access to the requested items, which may belong to different hierarchical levels, with the desired degree of detail and without requiring access to the whole hierarchy.

But ISAD(G) basically was developed for the institutions of Western countries. There some complications in its adaptation. However there are examples of using ISAD(G) in Asian archives. For instance, archival institutions of Korea have adopted it in their systems (Youn, 2015).

EAD is an archival description metadata standard that reflects and emphasizes the hierarchical nature of ISAD(G) (Pitti, 1999). EAD fully enables the expression of multiple description levels central to most archive descriptions and reflects hierarchy levels present in the resources being described. EAD cannot be considered a one-to-one ISAD(G) implementation, although it does respect ISAD(G) principles and is useful for representing archival hierarchical structure.

An Australian research project (the Recordkeeping Metadata Project) based in the School of Information Management and Systems at Monash University has developed a general framework known as the Australian Recordkeeping Metadata Schema (RKMS) (Day, 2001). It has also been concerned with supporting interoperability with more generic metadata standards like the Dublin Core and relevant information locator schemes like the Australian Government Locator Service (AGLS) scheme. The RKMS defines a highly structured set of metadata elements that conforms to a data model based on that developed for the Resource Description Framework (RDF). The schema is designed to be extensible and can inherit metadata elements from other schemas.

Ruhl has conducted an on-line survey which was executed 2010 in german archives of all branches (Ruhl, 2012). The survey focused on metadata and used metadata standards for the annotation of audiovisual media like pictures, audio and video files (analog and digital). The survey found that the issue of metadata for audiovisual objects, metadata standards and their exchange plays a minor role for most of the german archives. This can only be attributed to a lack of knowledge of the subject and its benefits to the archival landscape or to an extreme lack of personnel, temporal and financial resources in the archives. The same situation in archival institutions of Uzbekistan. Many archivists don't know about metadata and many of them don't have any experience on working with digital archives. In this case we're working on developing the unique archival network and it's union catalog. Every institution will be connected to this network and they will work in unique system. Then it will be easy to train archivists on working in this system.

Methodology

Today there are 102 state archives (including 4 CSA), 107 archives of staff documents, 15 non-state archives, more than 10000 archival departments of the state organizations in Uzbekistan. Total amount of archives is more than 13 million storage units. The national archival fond of the Republic of Uzbekistan includes more than 6 million documents. In particular, more than 38 000 scientific and technical documents, 16 000 film documents, 402 000 photo documents, 14 000 sound documents are very important. 2 million documents in archive departments in public organizations, 1 million documents in non-state archives. Some archives have experiences on using library description standard – MARC21[4] based software as their repository system. This software called ARMAT was initially designed for libraries and now it is widely being used in corporate network of libraries (Rakhmatullayev, 2014). There are other experiences on implementing MARC21 as a main format of digital archives in different countries. But this format has one principal minus: it can not cover hierarchy of archives. Therefore it is used in conjunction with archival standard, for instance, with EAD. But this complicates the work.

In our research we use experimental design as a research method to implement archival system in 3 CSA of Uzbekistan and create archival network. These pilot archives are: Central State Archive of the Republic of Uzbekistan, Central State Archive of Scientific-technical and medical documents of the Republic of Uzbekistan, Central State Archive of Films, Photographs and Sound Recordings of the Republic of Uzbekistan. In this research we are expecting to get results on metadata using for various types of documents and relations between records. This system's metadata format will be in ISAD(G).

Findings

ISAD(G) gives several opportunities. It can cover all levels of records, such as fond, series, file and item. It easily can be related with other standards that can be used in digital archives: ISAAR(CPF) for Authority Files and ISDIAH for Archival Institutions when working on corporate network. In Fig.1 there is a semantic model of digital

4 MARC 21 Format for Bibliographic Data, https://www.loc.gov/marc/bibliographic/

archives system based on above mentioned standards.

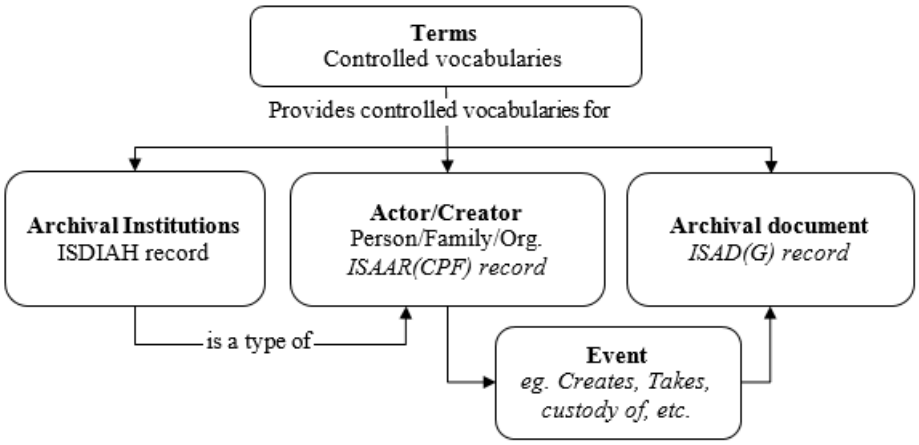


Figure 1. Recordkeeping model and relationship between records.

Implications

With development of digital archives based on metadata standard, archival institutions will get a significant effect in the following areas:

- Long-term preservation of documents;
- Operative, more complete providing population with various and necessary information;
- Fast search and browse archives;
- Reduction of documents duplication;
- One training system;
- Interoperability with digital systems of other institutions, such as libraries and museums.
- Rich information space based on modern technology solutions;
- Unification of documents and forms of their description and representation;
- Social benefits (information openness of the state, development of scientific, cultural, educational ties, etc.).

References

1. Barnes, N. D. (2016). ISO 15489 – Revised and Redesigned for 2016. Information Management Journal, 50(5), 30-33.
2. Cunningham, A. (2001). Six Degrees of Separation: Australian Metadata Initiatives and Their Relationships with International Standards. ArchivalScience, 271-283.
3. Day, M. (2001). Metadata for Digital Preservation: A Review of Recent Developments. Constantopoulos PSølvberg I.T. (eds) Research and Advanced Technology for Digital Libraries. ECDL 2001. Lecture Notes in Computer Science, vol 2163, 161-172.
4. Duff, W. (2001). Evaluating metadata on a metalevel. Archival Science, 1(3), 285-294. doi:10.1007/BF02437692
5. Evans, J., McKemmish, S. & Bhoday, K. (2005). Create Once, Use Many Times: The Clever Use of Recordkeeping Metadata for Multiple Archival Purposes. Archival Science, 5(1), 17-42. doi:10.1007/s10502-005-4625-x
6. Ferro, N., Silvello, G. (2008). A Methodology for Sharing Archival Descriptive Metadata in a Distributed Environment. Christensen-Dalsgaard B., Castelli D., Ammitzbøll Jurik B., Lippincott J. (eds) Research and Advanced Technology for Digital Libraries. ECDL 2008. Lecture Notes in Computer Science, vol 5173.
7. Mauthner, N. S., & Gárdos, J. (2015). Archival Practices and the Making of "Memories". New Review Of Information Networking, 20(1/2), 155-169. doi:10.1080/13614576.2015.1114825
8. Pitti, D. (1999). Encoded Archival Description. An Introduction and Overview. D-Lib Magazine, 5(11).
9. Rakhmatullayev, M. (2014). Informatcionnoe obespechenie universitetov v korporativnoy bibliotechnoy seti. "Society, Integration, Education". PROCEEDING of the International Scientific Conference, (pp. 333-342). Rezekne, Latvia.
10. Ruhl, M. (2012). Do we need metadata? - An on-line survey in German archives. Proceedings of the 2nd International Workshop on Semantic Digital Archives, 30-36.
11. Steiner, E., & Koch, C. (2015). A Digital Archive of Cultural Heritage Objects: Standardized Metadata and Annotation Categories. New Review Of Information Networking, 20(1/2), 255-260. doi:10.1080/13614576.2015.1112171
12. Wallace, D. (2001). Archiving metadata forum: Report from the Recordkeeping Metadata Working Meeting, June 2000. Archival Science, 1, 253-269.
13. Youn, E. (2015). Adoption of ISAD(G) in practice: a close look at the standardization process of ISAD(G) in a manuscript archives of Korea. Archives & Records, 36(2), 128-145. doi:10.1080/23257962.2015.1029892

THE ANALYSIS OF TEXT STEGANOGRAPHY METHODS

Salimov Sardor Baxtiyor ugli,
Botirov Fayzullajon Baxtiyorovich
Sattorov Abduqodir Abduqahhorovich

Abstract*: Today, in any sphere of our life, any type of data (text, image, audio, video etc.) can be stored and transmitted at high speed. However, they are easy to access illegally, tamper with, and copy. For this reason, the issue of information security has become more important with the development of computer. One of the grounds discussed in information security is the exchange of information through the cover media using steganography methods. In this paper, we analyze some basic approaches of text steganography and compare it according their performance based on the advantages and disadvantages.*

Keywords*: steganography, cryptography, encrypt, hash, stegotext, cover object, attackers, cipher text.*

Introduction

Steganography is a branch of information hiding and its main goal is to communicate or transmit the data securely in a completely undetectable manner. Literally meaning writing in a cover is the practice of hiding messages within other messages in order to conceal the existence of the original [1]. The inventor of the word *steganography* is Trithemius, the author of the early publications on cryptography: Polygraphia and Steganographia. Besides invisible ink, an oft-cited example of steganography is an ancient story from Herodotus, who tells of a slave sent by his master, Histiaeus, to the Ionian city of Miletus with a secret message tattooed on his scalp. He then journeyed to Miletus and, upon arriving, shaved his head to reveal the message to the city's regent, Aristagoras. The message encouraged Aristagoras to start a revolt against the Persian king. In this scenario, the message is of primary value to Histiaeus and the slave is simply the carrier of the message [2].

We can classify the steganography methods based on cover media as follows:

Text, Image, Audio, Video, Protocol.

Text steganography

The text steganography is a method of using written natural language to conceal a secret message. In text documents, we can hide information by introducing changes in the structure of the document without making a notable change in the concerned output. Storing text file require less memory and its faster as well as easier communication makes it preferable to other types of steganographic methods. Text steganography can be broadly classified into three types: Format based, Random and Statistical generation, Linguistic methods.

Format based methods

This method uses the physical formatting of text as a space in which to hide information. Insertion of spaces or non-displayed characters, careful errors tinny throughout the text and resizing of fonts are some of the many format-based methods used in text steganography. Some of these methods, such as deliberate misspellings and space insertion, might fool human readers who ignore occasional misspellings, but can often be easily detected by a computer [3].

Random and statistical methods

In order to overcome the problem of comparison with a known plaintext, steganographers often choose to generate their own cover texts. The methods used are - concealing information in random looking sequence of characters, the statistical properties of word length and letter frequencies are used in order to create words which will appear to have same statistical properties as actual words in the given language [3].

Table 1. Advantages and disadvantages of Text steganography methods

Text Steganography methods	Advantage	Disadvantage
Line Shift	This method is suitable only for printed text.	When attackers use OCR (character recognition program), the hidden information easily would get destroyed.
Word Shift	Word shifting method identify less because of change of distance between words to fill line is quite common.	If someone knows the algorithm of distances, using the difference in the distances one can obtain the hidden text by comparing the stego text with the algorithm. Also, retyping or using OCR programs destroys the hidden information.
White Steg	Due to the fact that in practically all text editors, extra white space at the end of lines is skipped over, it won't be noticed by the casual viewer.	Inconsistent use of white space is not transparent.
Semantic method	Attacker cannot detect by retyping or using OCR programs.	Smart reader who has huge knowledge of words can discover their synonyms or antonyms.
Syntactic method	The amount of information to hidden the method is trivial.	It requires identification of correct places to insert punctuation marks.
CSS	Using RSA public key cryptosystem and cipher text makes more secure.	Text Correlation Program or any function corrected text is easily detect it.
Mixed-case font	The hiding capacity will be very high compared to other text steganography methods.	Attackers can easily detect with the special program. Retyping and using OCR programs destroys the hiding information.
SMS-Texting	Attacker cannot detect by retyping or using OCR programs.	It takes a long time to make a wordlist and the capacity of the text must be large to hide the secret message.
Feature Coding	A large volume of information can be hidden in the text without making the reader aware of the existence of such information in the text.	By placing characters in a fixed shape, the information is lost. Retyping the text or using OCR program destroys the hidden information.
SSCE (Secret Steganographic Code for Embedding)	Using SSCE table and a certain mapping technique by inserting articles (a, an) with the nouns increases the security of the data.	Inserting articles would attract smart reader, especially, when non-specific nouns are used a lot.
Hiding data in wordlist	It is based on the special calculated algorithm. Secret message is hidden to the text without any changes and cover is dynamically generated.	If attackers would be aware of the algorithm of this method, it is easy to detect it.
Hiding data in paragraphs	The approach works by hiding a message using start and end letter of the words of a cover file. A word having same start and end letter is skipped. Since no change is made to cover, the cover file and its corresponding stego file are the same.	The volume of data hiding in the paragraph would be very less. The capacity of hiding the large volume of data leads to the challenge.

CONCLUSION

There are some methods of text steganography that are analyzed and provided with advantages and disadvantages of each method (Table 1). Each method has its special algorithm, respective capability to hide data in text and using sphere which allows it increases its security. By using line shifting method, we can hide huge amount of data, but line shifting method only capable for printed text because in this method, other than printed text character reorganization program(OCR) is used and hidden information get destroyed. In Syntactic method, (.) and (,) is used to send very important information and hide very small amount of data. However, smart reader can easily detect or destroy secret message. Semantic method is efficient and its security is higher than previous method. In my view, Hiding Data in Paragraphs being the most efficient can be used to transmit confidential data securely over the Internet.

To sum up, some methods are easily detected by attackers or destroyed by retyping and using special programs (OCR), on the other hand, some of them is based on word structure and their meaning.

References

1. I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker *"Digital watermarking and steganography"*, Morgan Kaufman Publishers, Second edition, 2000.
2. J. Cummins, P. Diskin, S. Lau, R. Parlett *"Steganography and Digital watermarking"*, School of computer science, The University of Birmingham, 2004.
3. K.A. Kumar, S. Pabboju, N.M. Shyam *"Advance text steganography algorithms: an overview"*, IJRA, Vol. 1, No. 1(1), pp. 31-35, 2014.
4. L.Y. POR and B. Delina, *"Information Hiding: A New Approach in Text Steganography"*.
5. V. Saraswathi and S. Kingslin, *"Different approach to text steganography: a comparison"*, IJERMT, Vol. 3, No. 11, pp. 124-127, 2014.
6. L.Y. Por, T.F. Ang, and B. Delina, *"WhiteSteg - a new scheme in information hiding using text steganography"*, WSEAS Transactions on Computers, Vol.7, No.6, pp. 735-745, 2008.

ОКАЗАНИЕ УСЛУГ ПОЧТОВОЙ СВЯЗИ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Ишдавлетова Эмине Талгатовна
старший преподаватель кафедры «Технология почтовой связи»
Ташкентский университет информационных технологий
имени Мухаммада Ал-Хоразмий

В данной статье приведены автоматизированные информационные системы почтовой связи на основе информационно-коммуникационных технологий.

Инфокоммуникационные технологии (ИКТ) играют важнейшую роль в развитии почтового сектора и вносят значительный вклад в интеграцию почтовых сетей. Почтовые операторы региона предоставляют широкий ассортимент электронных услуг, включая гибридную почту, а также интерактивные сетевые почтовые услуги через Интернет, которые пользуются большим успехом.

В странах региона с благоприятными условиями наблюдается интенсивное развитие электронных почтовых и электронных государственных услуг. Почтовые службы многих стран имеют все возможности, чтобы проводить работу по преобразованию в онлайн форму административных процедур, отвечая таким образом на растущий интерес руководителей относительно использования таких онлайновых услуг, чтобы сократить расходы на их предоставление для служащих.

Многие страны данного региона стали обращать особое внимание на новые почтовые услуги, такие, как развитие интернет - магазинов. Более того, различные почтовые службы изучают услуги директ - маркетинга с целью оказания помощи в развитии бизнеса путем проведения целевых рекламных кампаний.

Система «Автоматизированной системы электронных денежных переводов» (АС ЭДП) функционирует с декабря 2005 года. В настоящее время к АС ЭДП подключено 186 узлов почтовой связи, производственных участков и 1539 отделений почтовой связи всего 1725 объектов почтовой связи (ОПС). Осуществляется обмен международными почтовыми переводами со всеми странами СНГ, причем с Украиной, Российской Федерацией, Республикой Беларусь, Республикой Казахстан, Молдовой, Азербайджаном и Арменией через международную финансовую систему ВПС. В целях совершенствования системы международных электронных переводов в феврале 2011 года осуществлен переход с системы IFS - Light на систему IFS. В августе 2011 года был разработан интерфейс между системами IFS и ККС. Принятые меры позволили значительно сократить время прохождения международных переводов внутри республики. На базе АС ЭДП внедрена с 1 марта 2012 года система «Гибридные денежные переводы», позволяющая оказывать услуги по приему и оплате почтовых переводов, как из автоматизированных, так и неавтоматизированных отделений почтовой связи.

В целях автоматизации процессов учета и контроля приема платежей от населения в 2008-2009 годах был разработан и внедрен пилотный проект «Автоматизированной системы приема платежей» (АСПП). В настоящее время к данной системе подключены 184 узлов почтовой связи, производственных участков и 1546 отделений почтовой связи всего 1730 ОПС. Данная система состыкована с биллинговой системой АО «Узбекэнерго» и позволяет обмениваться информацией в режиме «Online». В целях автоматизации процессов учета и контроля приема платежей от населения за газ в 2015 году были проведены работы по разработке модуля «Автоматизированной системы приема платежей за газ» АСПП «Газ».

В целях автоматизации процессов учета и контроля выплаты пенсий и пособий в 2008-2009 годах был разработан и внедрен пилотный проект «Автоматизированной системы учета выплаты пенсий и пособий» (АСУВП). В 2013 году осуществлена модернизация и сдача в эксплуатацию программы АСУВП. На сегодняшний день к АСУВП подключены 1730 ОПС. Между автоматизированной системой учета выплаты пенсий, пособий и АС «Пенсия» внебюджетного Пенсионного фонда при Министерстве финансов Республики Узбекистан, а также автоматизированной системой приема платежей и биллинговой системой ГАК «Узбекэнерго» организована «Online» связь по обмену данными. «Автоматизированная систе-

ма мониторинга прохождения регистрируемых почтовых отправлений» (АСМПРО) внедрена в сентябре 2011 года. Система работает с применением технологии штрихкодов и позволяет оперативно получать и обмениваться информацией о прохождении почтовых отправлений с операторами почтовой связи других государств, а также позволяет отображать данную информацию на сайте Общества. К системе подключены АРМ 609 объектов почтовой связи. В августе месяце 2015 года была разработана программа АС «Интернет подписка» и внедрена услуга «Интернет подписка» для осуществления подписки через Интернет. Система позволяет оформлять подписку через сеть Интернет в пределах г.Ташкента с предоставлением возможности оплаты за подписку со счетов банковских пластиковых карточек клиентов через Интернет.

В настоящее время через сайт (www.pochta.uz) Общества оказываются интерактивные услуги: поиск регистрируемых почтовых отправлений; поиск индексов объектов почтовой связи; прием заявок на вызов курьера. На сайте размещена информация для пользователей услуг: тарифы на услуги почтовой связи; рекламная и другая информация для пользователей. Через «Единый портал государственных интерактивных услуг» оказываются следующие виды услуг: размещение имеющихся вакансий и рассмотрение поступающих по ним предложений заявителей в Общество; размещение адресов, контактов, дней приема граждан, «Online» запись на прием к руководителю Общества; прием и обработка жалоб, заявлений и предложений физических и юридических лиц»; прием заявок на курьерские услуги филиала «Тошкент почтамти»; автоматизированный поиск регистрируемых почтовых отправлений.

СТРАТЕГИЯ РАЗВИТИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В ПОЧТОВОЙ СВЯЗИ РЕСПУБЛИКИ УЗБЕКИСТАН

Ишдавлетова Эмине Талгатовна
старший преподаватель кафедры «Технология почтовой связи»
Ташкентский университет информационных технологий
имени Мухаммада Ал-Хоразмий

В данной статье приведена выработка стратегии развития услуг почтовой связи в современных условияхв АО «Узбекистон почтаси» на основе Стратегии деятельности ВПС на период 2017-2020 гг и Программы модернизации сети почтовой связи, внедрения и развития новых видов услуг на базе информационно-коммуникационных технологий 2017-2020 годах.

Основным направлением развития почтовой связи Республики Узбекистан является оказание услуг с уровнем организации производства, отвечающим современным требованиям, удовлетворяющим возросшие потребности клиентуры и обеспечивающим качество обработки почтовых отправлений по стандартам Всемирного почтового союза. Основные направления - это поэтапное создание корпоративной сети передачи данных и оснащение компьютерной техникой и информационной технологией объектов почтовой связи Общества и внедрение современных услуг.

Основным направлением развития услуг почтовой связи в 2017 году определено оказание услуг с уровнем организации производства, отвечающим современным требованиям, удовлетворяющим возросшие потребности пользователей и обеспечивающим качество обработки почтовых отправлений по стандартам ВПС.

Для чего Общество планирует провести модернизацию основных фондов и существующих автоматизированных систем для предоставления более широкого круга услуг на базе информационно-коммуникационных технологий: увеличить инвестиции в развитие почтовой инфраструктуры и технологий на базе ИКТ для обеспечения устойчивого развития финансовых (почтово-банковских, банковских и страховых) услуг, а также развития электронной коммерции и услуг логистики по продвижению товаров и грузов; обеспечить доступ органам государственного управления, государственным предприятиям, коммерческим структурам и широким слоям населения к информационным ресурсам для предоставления государственных услуг через сеть объектов почтовой связи Общества.

Во исполнении Постановление Президента Республики Узбекистан от 16 мая 2016 года № ПП-2530 «О мерах по дальнейшему расширению торгово-экономического, инвестиционного и финансового сотрудничества с Республикой Корея» Общем собранием Общества от 30 июня 2016 года утверждена «Программа модернизации сети почтовой связи, внедрения и развития новых видов услуг на базе информационно-коммуникационных технологий 2017-2020 годах». В рамках этой программы в 2017 году предусмотрено: развитие автоматизированной информационной системы «Прием платежей», с дальнейшей интеграцией ее с информационными (платежными) системами поставщиков услуг; создание межведомственной платформы по электронному обмену данными с таможенной службой; подготовка помещений и установка 1750 шт. инфокиосков и терминалов для доступа к системе «Электронное правительство» в почтовых отделениях, в том числе в сельской местности; внедрение и развитие дилерских услуг операторов мобильной связи; разработка интеграционного модуля с КАИС «Административная практика» ГУБДД МВД РУз по доставке постановлений о наложении штрафов по нарушениям ПДД; дальнейшее развитие автоматизированной информационной системы учета и контроля движения автотранспорта и оснащение автомобильного транспорта GPS-трекерами; внедрение и развитие автоматизированной информационной системы «Страховые услуги».

В целях расширения профиля деятельности назначенных операторов на рынке платежных электронных почтовых услуг ВПС ввел в действие совместный бренд под названием PosTransfer.

Совершенно новое название бренда явилось результатом совместных усилий по унификации разрозненной практики различных стран. Целью данной работы было также добиться доверия клиентов, включая многочисленных работников-мигрантов, нуждающихся в доступных платежных услугах

для поддержки своих семей, оставшихся дома.

Уже более 25 назначенных операторов выразили свое намерение присоединиться к группе "PosTransfer", созданной в рамках ВПС, которая будет рассматривать вопросы, связанные с совместным брендом. В данную группу входит и Россия, осуществляющая через Международную финансовую систему (IFS) самое большое количество транзакций. Другим крупным игроком, предусматривающим использование бренда "PosTransfer", является Почтовый банк Франции, направляющий в 33 страны денежные средства посредством своей системы "Международные экспресс-переводы". Группа "PosTransfer" надеется, что к 2020 г. число ее членов увеличится до 100.

Мировой бренд оказывает давление на владельцев в деле создания такого совместного опыта. Почтовые работники, действительно предоставляющие услугу "PosTransfer", будут тем самым играть решающую роль в качестве представителя бренда, уделяя клиентуре внимание и оказывая ей доверие, что, по ее мнению, и должно происходить при предоставлении основных услуг в операционном окне.

Если удастся быстро достичь того, что клиенты будут преданы новому бренду, это может быть многообещающим. Такие услуги, как перевод денежных средств, создают тесные связи с клиентурой, так как они многое ставят на карту, включая элемент доверия. Этот продукт требует большого участия, поскольку клиент должен совершенно доверять тому кому отдает деньги в надежде, что они дойдут до получателя. Она также отмечает, что преобразование бренда не проходит без риска, так как сегодняшние клиенты могут чувствовать себя спокойнее с таким оператором, как Western Union, нежели с новым брендом.

Процесс требует проведения рекламных кампаний в отношении нового бренда, во время которых клиентам предоставляется надежная информация о функциональных аспектах услуги (цена, сроки и т. д.). Рекламная кампания должна также затрагивать эмоциональный аспект среди клиентуры, упоминая при этом, например, ее значение.

Не в первый раз международные почтовые службы объединяются под совместным брендом. PosTransfer напоминает создание кооператива EMS в рамках ВПС. С момента своего создания в 1998 г. этот кооператив предоставляет под брендом EMS высококачественные услуги. Сегодня экспресс - услуги предоставляются примерно в 200 странах. Операторы объединились под брендом EMS, и сегодня услуга известна во всем мире, ее оценили клиенты, отправляющие экспресс - почту.

Группа "PosTransfer" хотела бы содействовать предоставлению услуг путем рационализации сложных процессов и способствовать управлению мировой почтовой сетью электронных платежей ВПС (RPMPE). В конце 2014 г. этой сетью пользовались 69 назначенных операторов, 68 из которых применяли Международную финансовую систему ВПС (IFS).

Вышеуказанная финансовая система должна была упростить сложные отношения, требуемые мировым рынком денежных переводов. Таким образом, если новый пользователь присоединяется к сети ВПС, то о каждом "коридоре" необходимо договариваться, и он должен быть открыт на двусторонней основе между почтовыми партнерами. Согласно новой системе, назначенные операторы должны будут иметь возможность быстрее создавать новые "коридоры" с операторами, подписавшими многостороннее соглашение об услугах, управляемое группой "PosTransfer".

Система "PosTransfer" должна также упростить сложные связи между почтовыми службами и непочтовыми финансовыми системами.

СТУПЕНЧАТЫЙ ПРОФИЛЬ РАСПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЯ ПРЕЛОМЛЕНИЯ

Алишер Абдуллаев Илхамович

ассистент кафедры «Аппаратное и программное обеспечение систем управления в телекоммуникации»

Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Свет направлялся в стекле сердцевины волоконного световода со *ступенчатым профилем показателя преломления* благодаря полному внутреннему отражению, необходимо иметь показатель преломления n_1 стекла сердцевины немного больше показателя преломления n_2 стекла оболочки на границе раздела двух стеклянных сред. Если показатель преломления n_1 одинаков по всему поперечному сечению сердцевины, то тогда говорят, что показатель преломления имеет ступенчатый профиль, так как при переходе от стекла оболочки к стеклу сердцевины показатель преломления возрастает ступенеобразно и остается там неизменным. На рис. 1.1 приведены ступенчатый профиль показателя преломления волоконного световода, а также распространение луча света с соответствующими углами.

Такой волоконный волновод называется *световодом со ступенчатым профилем показателя преломления* или *ступенчатым световодом.* Этот тип волоконного световода легко изготовить. Однако в настоящее время он применяется довольно редко. Для того чтобы лучше проиллюстрировать распространение света в таком световоде, выбран нижеследующий пример (рис. 1.1).

Типичные размеры многомодового световода со ступенчатым профилем показателя преломления

Диаметр сердцевины	$2a$	100 мкм
Диаметр оболочки	D	140 мкм
Показатель преломления сердцевины	n_1	1.48
Показатель преломления оболочки	n_2	1.46

В этом случае для критического угла a_0 полного внутреннего отражения, т.с. наименьшего угла к нормали падения, при котором луч света направляется в стекле сердцевины и не преломляется в стекло оболочки, справедливы

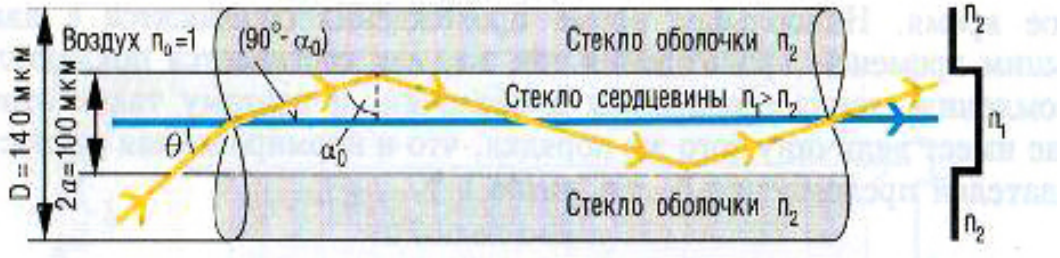


Рис. 1.1 Свеювод со ступенчатым профилем показателя преломления

$$\sin\alpha = \frac{\eta 1}{\eta 2} = \frac{1.46}{1.48} \approx 0.9865; \qquad \alpha 0 = 80.6°$$

Все лучи света, которые образуют угол с осью волоконного световода ≤ (90° - $\boldsymbol{a_0}$) = 9.4°, распространяются в стекле сердцевины.

Когда свет вводится в стекло сердцевины снаружи (воздух $\boldsymbol{n_0}$ = 1), то следует учитывать закон преломления, так как свет может войти в оптическое волокно только в пределах определенного апертурного угла ∴. В таком случае справедливы

$$\sin \ominus = \sqrt{\eta \frac{2}{1} - \eta \frac{2}{2}} = \sqrt{1.48^2 - 1.46^2} \approx 0.242; \quad \ominus \approx 14.0^\circ$$

Так как синус входной угловой апертуры определяется как “числовая апертура", то

NA=sin $\ominus$ $\approx_{0.242.}$

Нормированная разность показателей преломления Д для такого оптического волокна со ступенчатым профилем показателя преломления равна

$$\Delta = \frac{NA^2}{2 \times n\frac{2}{1}} \approx \frac{0.242^2}{2 \times 1.48^2} \approx 0.0134 = 1.34\%$$

Структурный параметр (нормированная частота) ***V,*** подсчитанный для ступенчатого оптического волновода с диаметром сердцевины 2***a*** = 100 мкм при длине волны = 850 нм, равен

$$V = \pi \frac{2a}{\lambda} NA = \pi \frac{100 \text{ мкм}}{0.85 \text{ мкм}} \times 0ю242 \approx 89.4.$$

Тогда число мод для такого волоконного световода примерно равно

$$N \approx \frac{V^2}{2} = \frac{89.4^2}{2} \approx 4000.$$

Такой волоконный световод является многомодовым. Импульс света, распространяющийся в нем, состоит из многих составляющих, направляемых в отдельных модах световода. Каждая из этих мод возбуждается на входе волновода под своим определенным углом ввода и направляется по нему в пределах стекла сердцевины соответственно по различным траекториям движения луча. Каждая мода проходит разнос расстояние оптического пути и поэтому приходит на выход световода в разное время. Наибольшее время прохождения соотносится с наименьшим временем прохождения так же, как соотносятся показатели преломления стекла сердцевины и оболочки, и поэтому такое отношение имеет величину того же порядка, что и нормированная разность показателей преломления Л, т.е. выше 1 %.

Пример:

Свет проходит через ступенчатый волоконный световод длиной 1 км примерно за 5 мкс. Тогда время задержки (разность времени прохождения) примерно равно

Δt ≈ 5мкс×1%=50нс

Искажения, обусловленные дисперсией времени задержки отдельных мод, называются ***модовой дисперсией***. Она обусловливает тот факт, что короткий световой импульс уширяется (во времени) по мере прохождения по ступенчатому световоду. Это является недостатком для оптических систем передачи информации, так как уменьшает скорость передачи (скорость передачи битов) и полосу пропускания передачи. Это влияние смягчается благодаря тому, что отдельные моды при прохождении по световоду воздействуют друг на друга и обмениваются энергией. Такое ***смешение мод***, или ***связь мод***, проявляется особенно интенсивно в местах неоднородностей стекла сердцевины, например на микроизгибах или на стыках волоконных световодов.

При прохождении мод вдоль оси волоконного световода моды низшего порядка с малым углом по отношению к оси световода за счет обмена энергией преобразуются в моды высшего порядка с более крутым углом по отношению к оси световода и наоборот. Вследствие этого различие схоро- стей мод выравнивается, а величина уширения Δt введенного светового импульса становится пропорциональной не длине световода, т.е. Δt~L, а скорее, в идеальном случае, корню квадратному из длины, т.е. Δt~L.

Эта модовая дисперсия может быть полностью исключена, если структурные параметры ступенчатого световода подобрать таким образом, что в нем будет направляться только одна мода, а именно — фундаментальная (основная) мода LP_{01}.

Однако основная мода также уширяется во времени по мере ее прохождения по такому световоду. Это явление называется ***хроматической дисперсией*** (раздел 5.4). Поскольку она является свойством материала, она, как правило, имеет место в любом оптическом световоде. По сравнению с дисперсией мод хроматическая дисперсия в диапазоне длин волн от 1200 до 1600 нм относительно мала или отсутствует.

Чтобы описать размер (радиальную амплитуду поля) фундаментальной моды, был введен термин диаметр поля моды 2и»$_0$ (раздел 5.6).

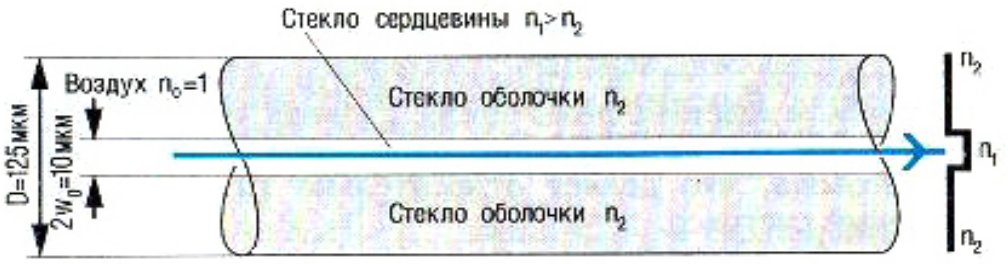


Рис. 1.2 Одномодовый волоконный световод

Для изготовления ступенчатого волоконного световода с малым затуханием, который направляет только фундаментальную моду в диапазоне длин волн более 1200 нм, диаметр поля моды $2w_0$ должен быть.

КОММУТАЦИЯ И МАРШРУТИЗАЦИЯ

Элов Жамшид Бекмуродович
Старший преподаватель,
Ташкентский университет информационных технологий
Ташкент, Узбекистан

Одной из основных характеристик узла сети передачи данных является коммутация и маршрутизация информации. Сущность ее заключается в выборе Узлом Связи последовательности каналов, по которым следует передать пакеты (блоки, на которые делится массив информации перед передачей). Программному обеспечению узла необходимо решить, в каком порядке и по каким каналам направить пакеты информации абонентам. Об этом процессе говорят, что в узле происходит коммутация информации.

Существует два способа коммутации информации: коммутация каналов и коммутация пакетов. При коммутации каналов предварительно путем посылки определенного сигнала устанавливается связь абонента А с абонентом В, который с помощью сигнала обратной связи сообщает о готовности принять сообщение. После этого абонент А начинает передавать данные. Время передачи данных зависит от длины передаваемого сообщения, пропускной способности канала и времени распространения сигнала по каналу.

Метод коммутации каналов прост, но имеет ряд существенных недостатков:

время организации линии для передачи информации достаточно велико;

нерациональное использование каналов связи (во время сеанса между двумя абонентами могут быть большие паузы, однако каналы связи между этими абонентами в период пауз не могут быть заняты другими);

низкая достоверность передачи информации (это связано с тем, что данные, передаваемые по последовательности каналов, нигде не проверяются).

Стремление устранить эти недостатки привело к созданию метода коммутации пакетов. Сущность его заключается в том, что здесь каждый пакет имеет адрес назначения и самостоятельно передается через подсеть. При использовании этого метода в узле проверяется адрес пакета и по каждому из них принимается решение по какому очередному каналу его передавать. Здесь ни одна пара абонентов во время сеанса взаимодействия не занимает монопольно ни одного канала.

Метод коммутации пакетов имеет ряд существенных преимуществ:

эффективное использование каналов связи за счет разделения времени работы каналов между различными парами абонентов (мультиплексирование потоков данных);

высокая достоверность передаваемой информации (достигается за счет выполнения проверки каждого пакета всеми узлами сети);

почти мгновенное предоставление возможности передачи информации (не нужно ожидать пока освободятся каналы, образующие путь от отправителя к получателю).

Метод коммутации каналов при всех своих недостатках имеет одно преимущество перед коммутацией пакетов. Оно заключается в том, что при монопольном владении каналами все пакеты проходят путь за одно и то же время. При коммутации пакетов из-за пиковых нагрузок в узлах могут возникать некоторые задержки.

TCP— Transmission Control Protocol

Обмен данными, ориентированный на соединения, может использовать надежную связь, для обеспечения которой протокол уровня 4 посылает подтверждения о получении данных и запрашивает повторную передачу, если данные не получены или искажены. Протокол TCP использует именно такую надежную связь. TCP используется в таких прикладных протоколах, как HTTP, FTP, SMTP и Telnet.

Протокол TCP требует, чтобы перед отправкой сообщения было открыто соединение. Серверное приложение должно выполнить так называемое пассивное открытие (passiveopen), чтобы создать соединение с известным номером порта, и, вместо того чтобы отправлять вызов в сеть, сервер переходит в ожидание поступления входящих запросов. Клиентское приложение должно выполнить активное открытие (activeopen), отправив серверному приложению синхронизирующий порядковый номер (SYN), идентифицирующий соединение. Клиентское приложение может использовать динамический номер порта в качестве локального порта.

TCP — это сложный, требующий больших затрат времени протокол, что объясняется его механизмом установления соединения, но он берет на себя заботу о гарантированной доставке пакетов, избавляя нас от необходимости включать эту функциональную возможность в прикладной протокол.

Протокол TCP имеет встроенную возможность надежной доставки. Если сообщение не отправлено корректно, мы получим сообщение об ошибке. Протокол TCP определен в RFC 793.

UDP — User Datagram Protocol

В отличие от TCP UDP — очень быстрый протокол, поскольку в нем определен самый минимальный механизм, необходимый для передачи данных. Конечно, он имеет некоторые недостатки. Сообщения поступают в любом порядке, и то, которое отправлено первым, может быть получено последним. Доставка сообщений UDP вовсе не гарантируется, сообщение может потеряться, и могут быть получены две копии одного и того же сообщения. Последний случай возникает, если для отправки сообщений в один адрес использовать два разных маршрута.

UDP не требует открывать соединение, и данные могут быть отправлены сразу же, как только они подготовлены. UDP не отправляет подтверждающие сообщения, поэтому данные могут быть получены или потеряны. Если при использовании UDP требуется надежная передача данных, ее следует реализовать в протоколе более высокого уровня.

Так в чем же преимущества UDP, зачем может понадобиться такой ненадежный протокол? Чтобы понять причину использования UDP, нужно различать однонаправленную передачу, широковещательную передачу и групповую рассылку.

Однонаправленное (unicast) сообщение отправляется из одного узла только в один другой узел. Это также называется связью "точка-точка". Протокол TCP поддерживает лишь однонаправленную связь. Если серверу нужно с помощью TCP взаимодействовать с несколькими клиентами, каждый клиент должен установить соединение, поскольку сообщения могут отправляться только одиночным узлам.

Широковещательная передача (broadcast) означает, что сообщение отправляется всем узлам сети. Групповая рассылка (multicast)- это промежуточный механизм: сообщения отправляются выбранным группам узлов.

UDP может использоваться для однонаправленной связи, если требуется быстрая передача, например для доставки мультимедийных данных, но главные преимущества UDP касаются широковещательной передачи и групповой рассылки.

Обычно, когда мы отправляем широковещательные или групповые сообщения, не нужно получать подтверждения из каждого узла, поскольку тогда сервер будет наводнен подтверждениями, а загрузка сети возрастет слишком сильно. Примером широковещательной передачи является служба времени. Сервер времени отправляет широковещательное сообщение, содержащее текущее время, и любой хост, если пожелает, может синхронизировать свое время с временем из широковещательного сообщения. UDP **— это быстрый протокол, не гарантирующий доставки. Если требуется поддержание порядка сообщений и надежная доставка, нужно использовать TCP. UDP главным образом предназначен для широковещательной и групповой передачи.**

АРХИТЕКТУРНОЕ ПРОЕКТИРОВАНИЕ, ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ ПРОЕКТИРОВАНИЕ

Элов Жамшид Бекмуродович
Старший преподаватель,
Ташкентский университет информационных технологий
Ташкент, Узбекистан

Архитектурным проектированием называют первый этап процесса проектирования, на котором определяются подсистемы, а также структура управления и взаимодействия подсистем.

Целью архитектурного проектирования является описание архитектуры программного обеспечения. Модель системной архитектуры часто является отправной точкой для создания спецификации различных частей системы. В процессе архитектурного проектирования разрабатывается базовая структура системы, т.е. определяются основные компоненты системы и взаимодействия между ними.

Этапы, общие для всех процессов архитектурного проектирования:

1. Структурирование системы. Программная система структурируется в виде совокупности относительно независимых подсистем. Также определяются взаимодействия между подсистемами.
2. Моделирование управления. Разрабатывается базовая модель управления взаимоотношениями между частями системы.
3. Модульная декомпозиция. Каждая определенная на первом этапе подсистема разбивается на отдельные модули. Здесь определяются типы модулей и типы их взаимосвязей.

Результатом процесса архитектурного проектирования является документ, отображающий архитектуру системы. Он состоит из набора графических схем представлений моделей системы с соответствующим описанием. В описании должно быть указано, из каких подсистем состоит система и из каких модулей слагается каждая подсистема. Графические схемы моделей системы позволяют взглянуть на архитектуру с разных сторон.

Как правило, разрабатывается четыре архитектурные модели:

1. Статическая структурная модель, в которой представлены подсистемы или компоненты, разрабатываемые в дальнейшем независимо.
2. Динамическая модель процессов, в которой представлена организация процессов во время работы системы.
3. Интерфейсная модель, которая определяет сервисы, предоставляемые каждой подсистемой через общий интерфейс.
4. Модели отношений, в которых показаны взаимоотношения между частями системы, например поток данных между подсистемами.

Объектно-ориентированное проектирование (ООП) — это часть объектно-ориентированной методологии, которая предоставляет возможность программистам оперировать понятием «объект», нежели понятием «процедура» при разработке своего кода. Объекты содержат инкапсулированные данные и процедуры, сгруппированные вместе, отображая т.о. сущность объекта. «Интерфейс объекта», описывает взаимодействие с объектом, то, как он определён. Программа, полученная при реализации объектно-ориентированного исходного кода, описывает взаимодействие этих объектов.

Объектно-ориентированный подход использует объектную декомпозицию. При этом статическая структура системы описывается в терминах объектов и связей между ними, а поведение системы описывается в терминах обмена сообщениями между объектами. Каждый объект системы обладает своим собственным поведением, моделирующим поведение объекта реального мира.

Понятие объект впервые было использовано около 30 лет назад в технических средствах при попытках отойти от традиционной архитектуры фон Неймана и преодолеть барьер между высоким уровнем программных абстракций и низким уровнем абстрагирования на уровне компьютеров. С объектно-ориентированной архитектурой также тесно связаны объектно-ориентированные операционные системы. Однако наиболее значительный вклад в объектный подход был внесен объектными и объектно-ориентированными языками программирования: Simula, Smalltalk, C++, ObjectPascal. На объектный подход оказали влияние также развивавшиеся достаточно независимо методы моделирования баз данных, в особенности подход сущность – связь.

Концептуальной основой объектно-ориентированного подхода является объектная модель.

Основными ее элементами являются:

- абстрагирование;
- инкапсуляция;
- модульность;
- иерархия.

Кроме основных, имеются еще три дополнительных элемента, не являющихся в отличие от основных строго обязательными:

- типизация;
- параллелизм;
- устойчивость.

Абстрагирование – это выделение существенных характеристик некоторого объекта, которые отличают его от всех других видов объектов и, таким образом, четко определяют его концептуальные границы относительно дальнейшего рассмотрения и анализа. Абстрагирование концентрирует внимание на внешних особенностях объекта и позволяет отделить самые существенные особенности его поведения от деталей их реализации. Выбор правильного набора абстракций для заданной предметной области представляет собой главную задачу объектно-ориентированного проектирования.

Инкапсуляция – это процесс отделения друг от друга отдельных элементов объекта, определяющих его устройство и поведение. Инкапсуляция служит для того, чтобы изолировать интерфейс объекта, отражающий его внешнее поведение, от внутренней реализации объекта. Объектный подход предполагает, что собственные ресурсы, которыми могут манипулировать только методы самого класса, скрыты от внешней среды. Абстрагирование и инкапсуляция являются взаимодополняющими операциями: абстрагирование фокусирует внимание на внешних особенностях объекта, а инкапсуляция (или, иначе, ограничение доступа) не позволяет объектам пользователям различать внутреннее устройство объекта.

Модульность – это свойство системы, связанное с возможностью ее декомпозиции на ряд внутренне связных, но слабо связанных между собой модулей. Инкапсуляция и модульность создают барьеры между абстракциями.

Иерархия – это ранжированная или упорядоченная система абстракций, расположение их по уровням. Основными видами иерархических структур применительно к сложным системам являются структура классов (иерархия по номенклатуре) и структура объектов (иерархия по составу). Примерами иерархии классов являются простое и множественное наследование (один класс использует структурную или функциональную часть соответственно одного или нескольких других классов), а иерархии объектов – агрегация.

Типизация – это ограничение, накладываемое на класс объектов и препятствующее взаимозаменяемости различных классов (или сильно сужающее ее возможность). Типизация позволяет защититься от использования объектов одного класса вместо другого или по крайней мере управлять таким использованием.

Устойчивость – свойство объекта существовать во времени (вне зависимости от процесса, породившего данный объект) и/или в пространстве (при перемещении объекта из адресного пространства, в котором он был создан).

ВНЕДРЕНИЕ СТАНДАРТА DVB–T2 НА ТЕРРИТОРИИ РЕСПУБЛИКИ УЗБЕКИСТАН

Акмурадов Бахтиёр Уралович
Ассистент,
Ташкентский университет информационных технологий
имени Мухаммада ал-Хоразмий

Аннотация*. Статья посвящена актуальной задаче исследованию внедрение стандарта DVB–T2 на территории Республики Узбекистана. А также исследуется дискуссионный вопрос о поэтапному переходу на цифровое вещание в Узбекистане.*

Ключевые слова: *DVB-T2, тюнеры, цифровое телевидение, , ТВ приёмник..*

Внедрение стандарта DVB–T2 позволит вывести эфирное цифровое телевизионное вещание на качественно новый уровень. Стандарт нового поколения открывает значительные перспективы по увеличению количества вещаемых программ стандартной четкости и созданию мультиплекса с программами высокой четкости.

Наряду со многими странами Европы и СНГ, в 2006 году в рамках проведения Региональной конференции радиосвязи по наземному цифровому вещанию в Женеве, Узбекистан подписал договор о постепенном переходе к цифровому телерадиовещанию. Внедрение цифрового телевидения в Республике Узбекистан началось в 2008 году.

Переход на цифровое телевизионное вещание осуществляется в соответствии с госпрограммой, утвержденной Постановлением Президента Республики Узбекистан от 17.04.2012 г. № ПП-1741 «О государственной программе по техническому и технологическому переходу на цифровое телевещание в Республике Узбекистан».

Сегодня в Узбекистане установлены 22 передатчика цифрового телевидения стандарта DVB-T, благодаря которым сигналами цифрового ТВ охвачены более 54 % населения.

Этожители города Ташкента и большинства районов Ташкентской, Сурхандарьинской, Самаркандской, Хорезмской, Бухарской, Андижанской, Наманганской, Ферганской, Навоийской, Кашкадарьинской и Сурхандарьинской областей, а также Республики Каракалпакстан.

В соответствии с постановлением Кабинета Министров Республике Узбекистан от 15.05.2015 г. № 123 инвестиционный проект «Развитие сети наземного цифрового вещания Республики Узбекистан» будет реализован с участием Японского банка международного сотрудничества в консорциуме с другими коммерческими банками этой страны. По итогам конкурсного отбора наилучших предложений поставщиков среди ведущих японских производителей цифровых телепередатчиков заключен контракт между ООО «Узимпэксалока» и компанией «Ogawa SeikiCo. Ltd» (Япония) на поставку оборудования цифрового телевещания для Государственного унитарного предприятия «Центр радиосвязи, радиовещания и телевидения» (ГУП «ЦРРТ») на общую сумму 8 751 343 200 японских иен (в эквиваленте 73,63 млн. долларов США).

В первом этапе (2015-2016 гг.) планируется установка 90 мощных цифровых телепередатчиков в областных центрах и густонаселённых пунктах. По окончании первого этапа будет обеспечен охват население цифровым телевещанием порядка 98 %.

Во втором этапе (2016-2017 гг. включительно) планируется установить 404 маломощных передатчиков в удалённых и труднодоступных населённых пунктах. В данном этапе для транспортировки цифрового потока от студии до передатчика будут использоваться спутниковые системы связи. В результате завершения второго этапа цифровым вещанием будет охвачено 100 % населения.

Внедрение цифрового телевидения не предусматривает отказ от кабельного ТВ. Эти два вида телевизионного вещания дополняют друг друга. Просто кабельная студия теперь будет поставлять не аналоговый сигнал в телевизоры своих абонентов, а цифровой.

Распространение пакета социально значимых телепрограмм осуществляется в Узбекистане на бесплатной основе. Сегодня в этот пакет включено12 цифровых телеканалов НТРК Узбекистана.

Вместе с тем, коммерческими операторами распространяются и пакеты программ на коммерческой основе в рамках договора с оператором телевидения. Тарифы на платные пакеты телепрограмм, также

как и на услуги кабельного телевидения, устанавливаются самими операторами (студиями) на рыночной основе.

Для приема сигналов цифрового телевидения абонентам необходимо или обновить телевизоры, заменив их на модели последнего поколения или приобрести приставки «Set-top-Box» (тюнеры) для имеющихся телевизоров. Рыночная ситуация в Узбекистане сегодня благоприятствует внедрению услуг цифрового телевидения. Есть несколько крупных предприятий по производству современных телевизоров, и с каждым годом для населения становятся доступны телеприемники с широким спектром возможностей: большая диагональ экрана, высокая яркость и контрастность, стереозвук, высокое разрешение изображения, а также встроенный тюнер цифрового телевидения.

Население Узбекистана в целом готово к поэтапному переходу на цифровое вещание. Подтверждением тому является большая популярность и огромный спрос на телевизоры (LCD, LED) с цифровыми тюнерами, наблюдаемый за последние 3-4 года.

Согласно Государственной программе, по мере повсеместного внедрения сети цифрового телевидения предусмотрено отключение существующей системы аналогового телевидения. Таким образом, переход на цифровой стандарт является обязательным для всех. Помимо телевизоров, как уже было сказано в СИЭЗ «Навои» компания СП «Telecom Innovations» освоила выпуск тюнеров для имеющихся телевизоров, что является недорогой альтернативой способом получения цифрового сигнала на старые модели телевизоров.

Методы построения сети DVB–T2 в регионах Республики Узбекистана. Существенным положением первого этапа создания сети цифрового телерадиовещания в Республики Узбекистана в условиях дефицита частотных каналов для строящихся радиотелевизионных передающих станций (РТПС) является использование одночастотных сетей, в которых все смежные цифровые РТПС конкретной локальной зоны работают на одном ТВ канале.

В регионах в соответствии с разработанным частотно–территориальным планом (ЧТП) для сети трансляции в Узбекистана первого мультиплекса организуется несколько локальных зон с разными частотными каналами.

В Ферганской области осуществлен переход к цифровому телевещанию. В настоящее время сигналы цифрового телевидения передаются по всем районам Ферганской области от цифровых передатчиков расположенных в Фергане, Коканде и Сохском районе Ферганской области.

Чтобы более эффективно использовать радиочастотный спектр с мая месяца 2015 года в городе Фергана был запущен для наземного телевещания стандарт DVB-T2, который имеет возможность вещать 16 SD телевизионных каналов.

По данным Центра электромагнитной совместимости, DVB-T2 принципиально отличается как архитектурой системного уровня, так и особенностями физического уровня, вследствие чего приёмники DVB-T несовместимы с DVB-T2. Причины несовместимости можно определить из таблицы указанной здесь.

Для приема цифрового сигнала DVB-T2 необходим специальный тюнер, поддерживающий данный стандарт. Данный вид тюнеров выпускаются в ООО СП "TELECOM INNOVATIONS" в Навоийской области и можно приобрести в офисах продаж «Единое окно» АК "Узбектелеком" Ферганской области.

В настоящее время жители Ферганской области могут смотреть с улучшенным качеством каналы цифрового телевидения: "O‘zbekiston", "Yoshlar", "Sport", "Navo", "Kinoteatr", "Bolajon", "Dunyo Bo‘ylab", "Madaniyat va Ma’rifat", "Diyor", "Oilaviy", "Mahalla", "Farg‘ona" и "UzHD"

ТЕКУЩЕЕ СОСТОЯНИЕ РАЗВИТИЯ ЦИФРОВОГО ТЕЛЕВИДЕНИЯ В УЗБЕКИСТАНЕ

Абдалимов Маъруф Норкулович
Ассистент,
Ташкентский университет информационных технологий
имени Мухаммада ал-Хоразмий

Аннотация*. Статья посвящена актуальной задаче исследованию метода расчета и определения зон покрытия ТВ передатчиков распространение радиоволн диапазона телевизионного вещания в Республики Узбекистан. А также исследуется дискуссионный вопрос о требование перехода к цифровому телевещанию в горных массивах Узбекистан.*
Ключевые слова: *цифровое телевидение, DVB-T2, HD, внедрения, ТВ передатчик.*

Сегодня в Узбекистане широко внедряется цифровое телевидение стандарта DVB-T2. Старые аналоговые стандарты телевещания уходят в прошлое, поэтому пользователям, планирующим приобретение нового телевизора необходимо обязательно обратить внимание на наличие в нем поддержки стандарта цифрового вещания стандарта DVB-T2. Мы попытаемся рассказать: как и зачем это нужно сделать во время.

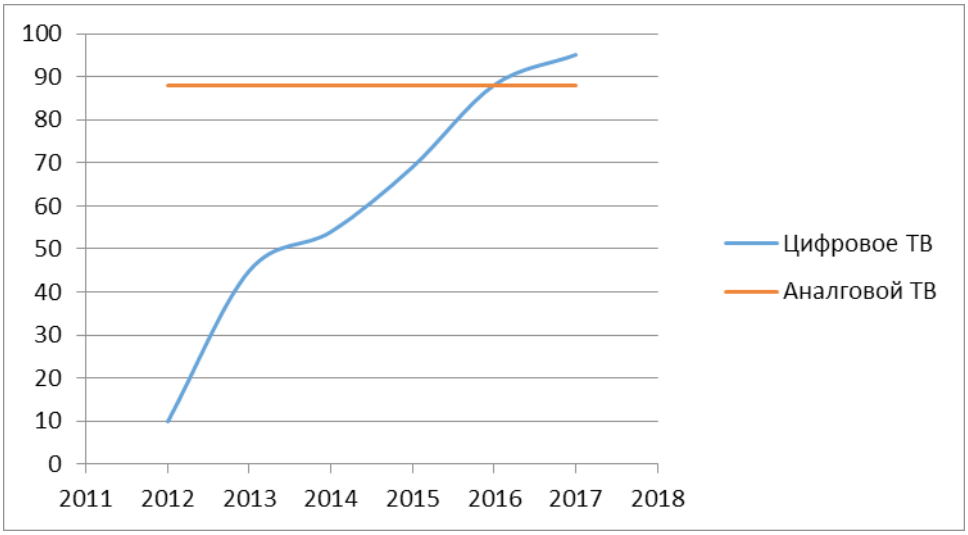
Главное преимущество цифрового телевидения — это сама картинка. Цифровая обработка изображения в процессе передачи и приема позволяет достичь гораздо более высокого качества. Прежде редко у кого дома телевизор показывал идеальную картинку, чаще изображение сопровождалось рябью, разного рода помехами, дергалось, пропадало. В новом формате влияние помех на четкость существенно минимизировалось. При этом уже два национальных телеканала вещают в формате высокой четкости HD. Один из них негосударственный телеканал, начавший вещание буквально в прошлом месяце. Другие телеканалы также планируют поэтапный переход к вещанию в HD качестве. Для подготовки к данному переходу требуется не только оснащение этих телеканалов новейшим оборудованием для создания HD контента, но и поэтапное отключение аналогового вещания для освобождения необходимого частотного диапазона для новых HD каналов.

Внедрение цифрового телевидения в стране способствовало появлению новых телеканалов - как государственных, так и негосударственных. За последние пять лет создано 8 государственных и 5 негосударственных телеканалов.

Это касается и звука, который раньше мог быть с посторонними шумами и шипением. Преимущество цифрового формата — возможность передавать стереозвук и звук в формате 5.1. Теперь к телевизору можно подключить пять обычных и одну низкочастотную колонку, создав домашний кинотеатр с так называемым эффектом присутствия.

Большинство современных телевизоров, в частности, выпускающиеся в Узбекистане, имеют встроенный цифровой тюнер, который поддерживает стандарт DVB-T2. В дополнение к нему потребуется лишь обычная антенна.

Немного статистики по переходу Узбекистана на цифровое вещание. По итогам первого квартала 2017 года уровень охвата населения Узбекистана цифровым телевещанием составил 95%. Этот показатель достигнут благодаря установке по всей стране 369 передатчиков цифрового телевидения.



Рисиунок 1. Развитие цифровое ТВ в Узбекситане

Стратегией действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах отдельным пунктом отмечена установка оборудования для цифрового вещания. До конца года будет установлено еще 25 мощных цифровых телепередатчиков в крупных городах и районных центрах и 293 передатчиков малой мощности в удаленных и труднодоступных населенных пунктах.

Для обеспечения постепенного и планомерного перехода горных массивах Республики Узбекистана к цифровому вещанию необходимо решение нескольких важных вопросов, которые составляют основу разработки графика перехода.

К основным вопросам из них относятся:

- требуемое количество телерадиовещательных каналов, организуемых на сети;
- обеспечение необходимого процента охвата населения телерадиовещанием в цифровом формате;
- выбор организации сети цифрового телевещания (одночастотный или многочастотный);
- состояние и возможности телекоммуникационной сети подачи цифрового потока (поток в 34 Мбит/с) до радиотелевизионных станций на всей территории Сурхандарьинской области;
- наличие и возможности финансирования данного проекта перехода.

Необходимо при разработке и реализации вышеназванного графика отметить следующее:

1. Государственная комиссия по радиочастотам совместно с ГУП Центр электромагнитной совместимости принимают решение по использованию частотного ресурса (телеканалов), согласованию с соседними Администрациями связи частотных каналов на приграничных станциях, как в Республике Узбекистан, так и в соседних государствах.

2. Принимая во внимание, что на ГУП Центр радиосвязи, радиовещания и телевидения возлагается задача распространения государственных телерадиопрограмм, в том числе и внедрение цифрового вещания в новом формате, поэтому планируется использование, в первую очередь, действующих радиотелевизионных станций и существующих антенно-мачтовых сооружений этого предприятия.

3. Наличие развитой цифровой телекоммуникационной сети у филиала «Телекоммуникация Транспорт Тармоғи» акционерной компании «Узбектелеком» предполагает обеспечение подачи одного или нескольких цифровых потоков (поток со скоростью 34 Мбит/с) до радиотелевизионных станций ГУП ЦРРТ, или до станций самого филиала, если там будут установлены цифровые телепередатчики.

По этим требованием можно определит 2 варианта перехода наземное цифровое телевещание в Сурхандарьинской области:

Одночастотный;

Многочастотный

СИСТЕМА МОБИЛЬНОГО ЦИФРОВОГО ТЕЛЕВИДЕНИЯ DVB-H

Абдуллаев Улугбек Махмудович

Ассистент, Ташкентский университет информационных технологий имени Мухаммад ал-Харазми, Узбекистан

Сегодня существует 8 форматов вещания, ориентированных на прием мобильными терминалами.

Во-первых, это форматы DVB-T и DVB-H. Во-вторых, MediaFLO, закрытая система разработки компании Qualcomm. В третьих, группа форматов, базирующихся на системе радиовещания DAB. К ней относятся Movio System (бывшая Live Time), разработанная British Telecom, корейские форматы T-DMB и S-DMB, а также европейский профиль формата T-DMB. И, наконец, существует японский стандарт эфирного вещания ISDB-T по своей гибкости пригодный для любых видов вещания на любые терминалы. Первоначально мы планировали сделать общий обзор всех форматов мобильного вещания, но затем решили вынести DVB-H в отдельный материал, так как эта система выглядит наиболее перспективной в плане распространения в Европе и, соответственно, наиболее вероятной для применения в России.

Система DVB-H разработана на базе DVB-T, что обеспечивает их частичную совместимость. Она заключается в том, что трансляции DVB-H за исключением одного режима модуляции могут приниматься приемниками DVB-T, и в одном мультиплексированном потоке возможно совмещение трансляций DVB-H и DVB-T.

В то же время в DVB-H введен ряд добавлений на физическом уровне и заметно изменен канальный уровень.

Крупнейшим Европейским проектом по разработке международной системы цифрового телевизионного вещания является проект Цифрового Видео Вещания - Digital Video Broadcasting (DVB), который был начат в сентябре 1993 г. Штаб-квартира DVB Project находится в Женеве (Швейцария). В результате работы международного консорциума DVB Project были приняты следующие стандарты цифрового ТВ:

DVB-C (C - Cable - кабель) для цифрового кабельного ТВ вещания;

DVB-S (S - Sattelrte - спутник) для спутникового ТВ вещания;

DVB-T (Terrestrial - наземный) для наземного ТВ вещания

Таким образом, DVB представляет собой совокупность подстандартов необходимых для унификации средств и оборудования ТВ вещания, их элементной базы и программного обеспечении. Это является необходимым условием успешного внедрения цифрового телевидения в разных странах мира. Следует отметить, что стандарт DVB наряду со странами СНГ принят у нас в Узбекистане.

На сегодняшний день существует ряд разновидностей стандартов **DVB, назначения которых представлены** в таблице 1.

Таблица 1.

Разновидности стандартов DVB по сфере применения

Название группы	**Значение**	**Описание**	**Модуляция**
DVB-S	Спутниковое ТВ вещание	Передача компрессированного видео и аудио, а также дополнительной информации через спутник.	QPSK, 8-PSK, 16-QAM
DVB-C	Кабельное ТВ вещание	Передача компрессированного видео и аудио, а также дополнительной информации через кабельные сети.	16-QAM, 32-QAM, 64-QAM, 128-QAM или 256-QAM,
DVB-T	Наземное эфирное ТВ вещание	Передача компрессированного видео и аудио, а также дополнительной информации через сети наземного эфирного телевидения (стационарный приём).	16-QAM или 64-QAM (или QPSK) совместно с COFDM
DVB-H	Мобильное ТВ вещание	То же, что DVB-T, только для мобильного приёма.	OFDM

DVB-H (Digital Video Broadcast Handheld, **DVB "ручной, портативный") это стандарт мобильного телевидения**, утвержденный декабре 2004 г. Европейской Ассоциация по Телекоммуникационным Стандартам (European Telecommunications Standards Institute, ETSI) для обеспечения уверенного приема ТВ программ на мобильные приемные устройства, установленные на автомобилях, поездах или сотовые телефоны.

При построении системы мобильного телевидения необходимо учитывать следующие особенности условий приема на мобильные терминалы:

- необходимо обеспечить прием сигналов на малогабаритные антенны портативных терминалов

не только вне зданий, но и за бетонными стенами, что требует значительного увеличения плотности потока мощности (ППМ) вещательного сигнала;
- прием сигналов на терминалы установленные на автомобилях и другом транспорте может приводить к значительным допплеровским искажениям передаваемых импульсов;
- ограниченные запасы энергии источников питания мобильных терминалов.

Таким образом к системе DVB-H предъявляются следующие требования:
- экономия тока потребления аккумуляторной батареи мобильного терминала. Эта задача явилась определяющей при формировании концепции мобильного вещания;
- устойчивый мобильный прием в движении, в том числе на больших скоростях;
- возможность приема при многолучевом распространении сигнала, особенно в комнатных условиях;
- полная совместимость с уже существующими сетями DVB-T;
- согласование с возможностями мобильного приемного терминала: -уменьшенная разрешающая способность (320x240 пикселей), поскольку нет смысла на небольшом экране пытаться воспроизвести картинку с хорошим разрешением, поэтому можно передавать в 10-15 раз больше телепрограмм, чем при DVB-T.

Заключение

Пока мы являемся свидетелями только первых шагов цифрового мобильного телевидения. Важным фактором, ограничивающим развитие сетей мобильного телевидения, является необходимость развертывания отдельной специфической вещательной инфраструктуры и, как следствие, довольно значительные инвестиции со стороны операторов сервиса.

Не надо забывать также, что одного наличия технических возможностей, способных обеспечить качественную «картинку» на экране установленного в салоне автомобиля телевизора не достаточно. Необходим еще и качественно новый контент телевизионных каналов. У затянутых сериалов и нудных бесед нет никаких шансов привлечь вечно спешащую аудиторию. Невозможно спрогнозировать, сколько времени зритель проведет перед экраном — ведь он находится не на диване, а в пути. Поэтому передачи должны быть короткими и емкими.

Можно с уверенностью предсказать, что вскоре на рынке появятся новые устройства с поддержкой DVB-H, зона уверенного покрытия увеличится и мобильное телевидение войдет в наш обиход.

Список литературы

1. ЦИФРОВОЕ ТЕЛЕВИДЕНИЕ. Гаврилов И.А., Рахимов Т.Г., Пузий А.Н., Носиров Х.Х., Кадиров Ш.М.
2. Реализуемость в России технологии мобильного цифрового телевизионного вещания DVB-H. http://www.rfcmd.ru/analytics/005.
3. А. Бителева. Система вещания DVB-H. Теле-Спутник - 6(128) Июнь 2006 г.
4.http://www.iksmedia.ru/articles/3434320-Czifrovoe-mobilnoe-televidenie-goto.html#ixzz4YFj0PUoi.

УДК 681.586

КОММУТАЦИЯ БЕЗ БУФЕРИЗАЦИИ

Абдухалилов Б.З.

Первым шагом, который производит коммутатор перед тем, как принять решение об отправки кадра, является его получение и анализ содержимого. В данном случае будет рассмотрен режим работы без коммутации буферизации.

The first step, which makes the switch before decide to send the frame, it is the acquisition and analysis of content. In this case it will be considered the cut-through.

Коммутацию без буферизации (на английском cut-through) разработала и реализовала, в первом коммутаторе Ethernet, фирма Kalpana в 1990 году. Во время работы в этом режиме коммутатор копирует в буфер только MAC-адрес назначения (первые 6 байт после префикса) и сразу начинает передавать кадр, не дожидаясь его полного приема. При использовании коммутации без буферизации уменьшается задержка, однако вместе с тем не производится проверка на наличие ошибок. Поскольку коммутатор не проверяет наличие ошибки, он пересылает повреждённые кадры по всей сети. При пересылке повреждённые кадры значительно уменьшают пропускную способность канала. В итоге сетевая плата назначения отклоняет повреждённые кадры. Данный метод коммутации может быть использован только в том случае, когда порты коммутатора работают на одинаковой скорости.

Можно выделить два варианта коммутации без буферизации:

Коммутация с быстрой пересылкой. Коммутация с быстрой пересылкой предоставляет минимальный уровень задержки. При данной коммутации пакет пересылается сразу же после прочтения адреса назначения. Поскольку при коммутации с быстрой пересылкой переадресация начинается до получения всего кадра целиком, могут возникнуть случаи, когда пакеты передаются с ошибками. Это происходит редко, и сетевой адаптер назначения отклоняет пакет, содержащий ошибки, после его получения. В режиме быстрой пересылки задержка измеряется с момента получения первого бита до передачи первого бита. Коммутация с быстрой пересылкой является типичным способом коммутации без буферизации. Схема, описывающая эту коммутацию, изображена на рисунке 1.

Рисунок 1. cut-through (коммутация без буферизации)

Коммутация с исключением фрагментов. При коммутации с исключением фрагментов коммутатор сохраняет первые 64 байта кадра перед его отправкой. Коммутацию с исключением фрагментов можно рассматривать как компромиссный вариант между коммутацией с буферизацией и коммутацией с быстрой пересылкой. Причина, по которой при коммутации с исключением фрагментов сохраняют только первые 64 байта кадра, заключается в том, что большинство сетевых ошибок и коллизий происходят именно в первых 64 байтах. Коммутация с исключением фрагментов пытается повысить эффективность коммутации с быстрой пересылкой, выполняя небольшую проверку ошибок в первых 64 байтах кадра, чтобы перед пересылкой кадра убедиться в отсутствии коллизии. Коммутация с исключением фрагментов представляет собой компромисс между большой задержкой с высокой целостностью (коммутация с буферизацией) и малой задержкой с меньшей целостностью (коммутация с быстрой пересылкой). Схема, описывающая коммутацию с исключением фрагментов, приведена на рисунке 2.

Рисунок 2. Fragment-free (Коммутация с исключением фрагментов)

Некоторые коммутаторы настроены на использование коммутации без буферизации для каждого порта до тех пор, пока не будет достигнуто указанное пользователем предельное количество ошибок, после чего автоматически устанавливается коммутация с буферизацией. После того, как частота повторения ошибок снизится до установленного предельного значения, порт автоматически переключится на использование коммутации без буферизации.

Из всего выше сказанного можно вынести, что коммутацию без буферизации довольно полезный режим в случаях необходимости большой скорости передачи, однако из-за отсутствия проверки появляются случаи возникновения пакетов с ошибкой.

Использованная литература.

1. Брайан Хилл. Глава 9. Основные сведения о коммутаторах // Полный справочник по Cisco = Cisco: The Complete Reference. — М.: «Вильямс». — С. 1088.
2. Дэвид Хьюкаби, Стив Мак-Квери. Руководство Cisco по конфигурированию коммутаторов Catalyst = Cisco Field Manual: Catalyst Switch Configuration. — М.: «Вильямс», 2004. — С. 560.
3. Игорь Баскаков. Построение коммутируемых компьютерных сетей. // МГТУ им. Н. Э. Баумана.

УСТАНОВКА ОПЕРАЦИОННОЙ СИСТЕМЫ UBUNTU ПО СЕТИ

Кудратов Султон Гулямович

Ташкент Узбекистан

Ubuntu, как и многие другие дистрибутивы Linux, можно легко установить по сети. Для этого вам всего лишь потребуется сетевое соединение с компьютером, который будет служить сервером для установки. BIOS вашего компьютера должен для этого поддерживать загрузку по сети.

Настройка сервера для установки

Прежде всего вам потребуется компьютер с Ubuntu или с другим дистрибутивом Linux (данная инструкция написана для Ubuntu), с которого вы будете устанавливать систему (сервер загрузки по сети), и ISO образ Alternate диска с необходимой версией Ubuntu.

Настройка сервера сетевой загрузки

Для загрузки по сети потребуется установить на сервер TFTP, HTTP и DHCP сервисы, чтобы позволить второму компьютеру подключиться и загрузить все необходимые файлы.

Для установки всего необходимого лучше использовать aptitude, которая не входит в стандартную поставку Ubuntu начиная с версии 10.10. Поэтому сначала ставим aptitude через любую программу установки пакетов или командой

```
sudo apt-get install aptitude
```

Далее ставим всё необходимое:

```
sudo aptitude -R install apache2 atftpd tftpd-hpa dhcp3-server
```

Ключ -R нужен для того, чтобы atftpd поставился без inetd сервера, который вам совершенно не нужен.

Теперь пора настроить все компоненты.

TFTP сервер

Демон, использующий эти файлы - **/etc/hosts.allow** и **/etc/hosts.deny** для ограничения доступа.

Откройте файл /etc/default/atftpd в любом текстовом редакторе с правами суперпользователя, например, так:

```
sudo nano /etc/default/atftpd
```

Измените первую строчку с

```
USE_INETD=true
```

На

```
USE_INETD=false
```

Кроме этого запомните каталог, который находится в конце строчки OPTIONS. Скорее всего это будет /srv/tftp, но в старых Ubuntu может быть и /var/lib/tftpboot. Редактируем файл /etc/default/tftpd-hpa:

```
sudo nano /etc/default/tftpd-hpa
```

вписываем, запомненный каталог

```
TFTP_DIRECTORY="/srv/tftp"
```

Теперь просто запустите atftpd:

```
sudo /etc/init.d/atftpd start
```

Теперь создайте в каталоге из OPTIONS папку ubuntu. Далее везде будем считать, что используется каталог /srv/tftp:

```
mkdir /srv/tftp/ubuntu
```

После этого необходимо смонтировать ваш ISO образ во вновь созданный каталог. Сделать это можно примерно такой командой:

```
sudo mount -o loop /home/tux/ubuntu-11.04-alternate-i386.iso /srv/tftp/ubuntu/
```

Если у Вас нет ISO образа диска, но есть записанный Alternate диск, то просто вставьте его в CD/DVD привод. Диск автоматически монтируется в /media/cdrom. Дальше просто нужно создать симлинк для TFTP сервера:

```
sudo ln -s /media/cdrom /srv/tftp/ubuntu
```

На этом настройка TFTP закончена.

DHCP сервер

Всё, что осталось - это настроить правильным образом DHCP сервер. Откройте в любом текстовом редакторе с правами суперпользователя файл /etc/dhcp3/dhcpd.conf, например, командой

```
sudo nano /etc/dhcp3/dhcpd.conf
```

В этом файле необходимо изменить следующие настройки:

```
# Имя вашего внутреннего домена. Если вам это ни о чём не говорит - просто не меняйте.
option domain-name "domain.uz";
# Ваш DNS сервер, который должен использоваться на подключаемом компьютере. Чаще всего тут стоит IP адрес роутера.
option domain-name-servers 192.168.0.1;
# Просто раскомментируйте эту строчку
authoritative;

# Теперь надо определить сеть для DHCP сервера:
# Сначала желаемая подсеть и маска подсети.
subnet 192.168.0.0 netmask 255.255.255.0 {
 # Диапазон выдачи сервером адресов
 range 192.168.0.100 192.168.0.199;
 # Роутер для доступа к интернету
 option routers 192.168.0.1;
 # Какой файл загружать при сетевой загрузке - укажите именно в таком виде.
 filename = "ubuntu/install/netboot/pxelinux.0";
}
```

После этого нужно сказать нашему DHCP серверу слушать один из интерфейсов. Для этого откройте файл /etc/default/dhcp3-server и добавьте в параметр INTERFACES имя нужного интерфейса. Например, вот так:

```
INTERFACES="eth0"
```

Теперь нужно запустить DHCP сервер и можно будет приступать к установке. Однако перед запуском убедитесь, что в вашей сети нету ещё каких-нибудь работающих DHCP серверов. Чаще всего DHCP бывает запущен на роутерах, в этом случае надо зайти на роутер и остановить на нём этот сервис.

Итак, для запуска DHCP сервера достаточно выполнить команду

```
sudo /etc/init.d/dhcp3-server start
```

Теперь необходимо перевести второй компьютер в режим загрузки по сети. После этого Вы должны увидеть экран установки Ubuntu.

Список литературы:

1. http://help.ubuntu.ru/wiki/
2. www.linux.org.ru/forum/linux-install/11464703
3. Jordan Spencer. Interview: Arch Linux Team (англ.). OSNews (11 января 2010 года). — Интервью с членами команды разработчиков Arch Linux.

РАЗРАБОТКА МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ С ПРИОРИТЕТНЫМ ОБСЛУЖИВАНИЕМ

Парсиев С.С.

Заведующий кафедрой "Аппаратное и программное обеспечение системы управлений в телекоммуникации»" ТУИТ, к.т.н., доцент

Аннотация. *В статье разработаны математические модели приоритетного обслуживания разнородной нагрузки в телекоммуникационной сети .Данные модели позволят учитывать специфику совместной передачи разнородной информации и правильно оценить основных параметров телекоммуникационной сети.*

Ключевые слова: *телекоммуникационная сеть, речевой пакет, приоритетное обслуживания, дисциплина очереди, времени обслуживания, функция распределения.*

Современное развития информационного общества и информационных систем различного назначения, а также набирающие интенсивность модернизации и технологического развития экономики Узбекистана предъявляют ряд новых требований к телекоммуникационным системам по видам, объемам и качеству передаваемой информации, доступности обслуживания. Основными из них являются [1]:

- интегрированное предоставление услуг и, соответственно, многокомпонентность (мультимедийность) передаваемой информации (голос, видео, данные);
- мобильность пользователей и обслуживания, интерактивность и широкополосность доступа, многосвязное взаимодействие;
- возможность гибкого создания и внедрения новых услуг;
- обеспечение минимальной себестоимости предоставляемых услуг за счет унификации сетевых решений и эффективности использования сетевых ресурсов.

В целом данные факторы определяют эволюционный переход от построения узкоспециализированных выделенных (по видам связи) сетей к мультисервисным сетям связи с пакетной IP, MPLS (ATM) коммутацией, реализуемым на основе концепции NGN. Последние обеспечивают предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений на основе разделения функций переноса, коммутации, управления вызовами и услугами. Это достигается [1]:

- четырехуровневой архитектурой построения сетей NGN, включающей уровень доступа, транспортный уровень, уровень управления вызовами, уровень услуг, а также применением на каждом уровне открытых стандартов;
- обеспечением QoS при передаче разнородной информации на основе введения классов качества.

Изложенные особенности развития инфокоммуникационных услуг и телекоммуникационных систем требуют адекватного развития моделей и методов исследования процессов функционирования и оптимизации построения сетей связи. Разработку данных моделей и методов для сетей будем вести в области приоритетных систем обслуживания пакетов различных классов качества, ограничениями ресурсов (объем буфера, число каналов и их пропускная способность).

При приоритетном обслуживании каждому поступающему сообщению (пакету) ставится в соответствии некоторое число – его приоритет, определяющий очередность выбора пакетов на обслуживание, так что пакеты с одинаковым приоритетом обслуживаются в порядке поступления, а пакеты с более высоким приоритетом – раньше, чем пакеты с более низким. Указанные типы систем массового обслуживания (СМО) именуются соответственно как системы с абсолютным и относительным приоритетом.

В системах СМО с абсолютным приоритетом существуют различные дисциплины обслуживания прерванных пакетов, которые рассматриваются в [4, 5].

Дисциплина очереди может учитывать ограничения на длину очереди или на время пребывания в системе, когда при достижении определенных размеров очереди (переполнении буфера), либо при превышении установленного времени пребывания, пакеты теряются. Подобные СМО называются системами с ограниченным ожиданием.

Основным методом расчета качественных характеристик сети NGN , в нашем случае, модель СМО $/\vec{M}_k/\vec{G}_k/\vec{1}/_\infty$ с абсолютным приоритетом на случай Р приоритетов с ненадежным обслуживающим прибором [4, 6].

Пусть пакеты с Р приоритетами поступают в однолинейную СМО и образуют пуассоновских потоков с интенсивностью $\lambda_k,\ k=\overline{1,P}$. Суммарный поток является пуассоновским с интенсивностью $\sigma=\sum_{к=1}^{p}\lambda_к$.

В такой СМО протекает два основных независимых процесса [, 5]:

- процесс ожидания, характеризуемый случайным временем t_{wk} с функцией распределения (ФР) $W_k(t)$;

- процесс обслуживания, характеризуемый случайным временем t_{hk} с ФР $H_k(t)$.

Согласно [4] в силу аддитивности случайное время доставки пакета с к –м приоритетом $t_{gk}=t_{wk}+t_{hk}\ ,k=\overline{1,p}$

ФР времени пребывания пакета в системе

$$V_k(t)=W_k(t)*H_k(t)\ , (1)$$

где * - стилтьевсовская свертка.

Из выражения (1) получается среднее время пребывания пакета к-го приоритета в звене передачи

$$T_k=\int_0^\infty t\cdot dV_k(t)\ (2)$$

Для нахождения времени обслуживания t_{hk} пакетов к-го приоритета в звене передачи воспользуемся преобразованием Лапласа- Стильтьеса (ПЛС) с ФР $H_k(t)$ времени обслуживания пакетов к –го приоритета в момент времени t [4].

Согласно (1)

$$Q_k(v)=\int_0^\infty e^{-vt}\,dV_k(t)=\omega_k(v)\cdot h_k(v)\ (3)$$

где v – интенсивность старения информации $v=\frac{1}{T_z}$, где $\mathrm{T_z}$ – среднее время старения;

$\omega_k(v)$ – ПЛС от ФР $W_k(t)$ времени ожидания начала обслуживания пакетов к-го приоритета в момент времени t;

$h_k(v)$ – ПЛС от ФР $\mathrm{H_k(t)}$ времени обслуживания пакетов к-го приоритета в момент времени t.

Формализуя процесс передачи в звене сети NGN с помощью СМО типа $/\vec{M}_k/\vec{G}_k/\vec{1}/_\infty$ с абсолютным приоритетом получим выражение ПЛС от ФР времени ожидания начала обслуживания к-го приоритета (формула Полячека-Хинчина) [6, 7]:

$$\omega_k(v)=\left\{\frac{1-\sum_{i=1}^{p}\rho_i}{\sigma\varphi_1+e(\sigma)[1-\sigma\varphi_1]}\left[e(\sigma)\left(v+\sigma_{k-1}\left(1-h_{k-1}(v)\right)\right)\right.\right.$$
$$\left.+\sigma\left(1-e(\sigma)\right)\left[1-\varphi(v+\sigma_{k-1}\left(1-h_{k-1}(v)\right)\right]\right]$$
$$\left.+\sum_{i=k+1}^{p}\lambda_i\left[1-B_i\left(v+\sigma_{k-1}\left(1-h_{k-1}(v)\right)\right)\right]\right\}$$
$$/\,v-\lambda_k B_k\left(v+\sigma_{k-1}\left(1-h_{k-1}(v)\right)\right),\ (4)$$

где

$$h_0(v)=\sigma_0=0;\sigma=\sum_{i=1}^{p}\lambda_i;\sigma_{k-1}=\sum_{i=1}^{k-1}\lambda_i;$$

В частности, если время исправной работы и время восстановления являются экспоненциально распределенным случайными величинами с параметрами с и d, то

$$e(\sigma)=\int_0^\infty e^{-\sigma t}\,dE(t)=\int_0^\infty e^{-\sigma t}\,d(1-e^{-ct})=\frac{c}{\sigma+c};$$

$$\varphi(v) = \int_0^\infty e^{-vt}\, dD(t) = \int_0^\infty e^{-vt}\, d(1 - e^{-dt}) = \frac{d}{v + d};$$

$$\varphi_1 = \int_0^\infty t\, dD(t) = d \int_0^\infty t\, e^{-dt} dt = \frac{1}{d};$$

где

v — интенсивность старения пакета;

d — интенсивность восстановления канала;

c — среднее время исправной работы обслуживающего прибора.

$$h_{k-1}(v) = \frac{1}{\sigma_{k-1}+c}\left\{\sum_{i=1}^{k-1}\lambda_i B_i\left(v + (\sigma_{k-1} + c)\cdot\left(1 - h_{k-1}(v)\right)\right) + c\varphi(v)\right\}, \quad (5)$$

$B_i(v)$ – ПЛС ФР времени обслуживания для i - го приоритета

$$B_i(v) = \int_0^\infty e^{-vt}\, dB_i(t) \quad (6)$$

$$B_i(t) = \begin{cases} 0, & t < t_i \\ I, & t < t_i \end{cases} \quad (7)$$

г д е

$$t_i = \frac{L_i + H_i}{C_M}, \quad (8)$$

L_i, H_i — объем информационной и служебной части пакетов i - го приоритета соответственно; C_M — скорость модуляции в цифровом канале связи.

Таким образом, на базе известных ФР времени передачи и времени ожидания с помощью ПЛС получены математические модели приоритетного обслуживания разнородного трафика в звене передачи сети NGN, учитывающие специфику передаваемых пакетов информации.

Полученные модели позволяют учитывать широкий набор факторов:

- многомерный входящий поток пакетов;
- комбинированную приоритетную процедуру обслуживания пакетов речевой - информации, данных и других потоков информации;
- надежностные характеристики сети;
- времени ожидания начала обслуживания в очереди, с учетом отказов звена передачи данных;
- времени обслуживания пакета;

Разработанные математические модели приоритетного обслуживания разнородного трафика в звене передачи телекоммуникационной сети с различными дисциплинами обслуживания, пригодны для расчета параметров сети с произвольным числам приоритетов, а также их можно использовать при определении эффективных областей применения приоритетного обслуживания в телекоммуникационной сети.

Список литературы

1. Назаров А.Н., Сычев К. И. Модели и методы исследования процессов функционирования и оптимизации построения сетей связи следующего поколения, «Электросвязь», №3, 2011 г.
2. Клейнрок Л. Вычислительные системы с очередями. – М.: Мир, 1979, - 600 с.
3. Проектирование и техническая эксплуатация сетей передачи дискретных сообщений: Учеб. пособие для вузов / М.Н. Арипов и др. Под ред. Г.П. Захарова. М.: Радио и связь, 1988.
4. Захаров Г.П. Методы исследования сетей передачи данных. М.: Радио и связь, 1982.
5. Захаров Г.П., Симонов М.В.. Яновский ГГ. Службы и архитектура широкополосных цифровых сетей интегрального обслуживания // Технологии электронных коммутаций. Том 41. М.: Экотрендз, 1993.
6. Климов Г.П. Стохастические системы обслуживания. М.: Наука, 1966.
7. Гнеденко Б. В., Даниелян Э. А., и др. Приоритетные системы обслуживания. Изд., МГУ, 1973, с. 439.

ТЕСТИРОВАНИЕ МЕДИАОБРАЗОВАТЕЛЬНОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ

Бекназарова Саида Сафибуллаевна

Доктор технических наук

Убайдуллаев Хусанбой Илхомжон угли

доцент, старший преподаватель

Жаумытбаева Мехрибан

магистр

Ташкентский Университет информационных технологий, Национальный университет Узбекистана, Ташкент, Узбекистан,

***Аннотация**. В статье рассматривается процесс тестирования программного обеспечения мультимедийного медиаобразовательного мобильного приложения на основе распределения запросов клиентов.*

***Ключевые слова**: тестирование, программное обеспечение мультимедийный, медиаобразовательный процесс, мобильное приложение, запрос клиентов.*

Имеется программный комплекс (ПК) медиаобразовательного портала http:// mediaedu.uz типа клиент-сервер. Сервер обслуживает запросы от N клиентов. В ПК равномерно по области определения входных данных (ООД) (A, B) расположены Er ошибок. Сервер сложнее клиентов с точки зрения разработки ПК в S раз. S – коэффициент сложности сервера по отношению к клиентам. Каждый k-ый (k = 1, 2, …, N) клиент порождает пуассоновский поток данных к серверу интенсивностью λ обр. Данные от клиента распределены по области определения данных (ООД) по нормальному закону с характеристиками mk и s k, где mk распределено между клиентами равномерно по всей области входных данных, 3s k – распределено равномерно на меньшем из участков отсекаемых mk на оси области данных (это нужно для имитации неравномерности использования ООД при малом количестве клиентов).

На рисунке (см. Рисунок 1 – «Распределение запросов k-го клиента на области данных») изображено распределение запросов одного клиента по области всех возможных запросов к серверу, а также показано равномерное распределение ошибок по ООД. При попадании запроса клиента или ответа сервера в область ООД, содержащую ошибку, считается, что ошибка обнаружена и соответствующий модуль выводится из эксплуатации для ее исправления:

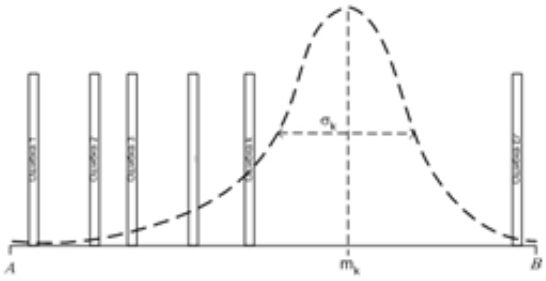


Рисунок 1 – «Распределение запросов k-го клиента на области данных»

На запрос клиента сервер отвечает данными, которые распределены равномерно по всей области определения данных (A, B).

Входными данными для розыгрыша являются:

P – количество программистов, обслуживающих систему;

K - количество программ-клиентов (далее просто клиенты);

α - ширина одного запроса клиента как доля от ООД (от 0 до 1, где 1 – это вся ООД);

Δ t - шаг итерации (сутки);
s - коэффициент сложности сервера по сравнению с программой-клиентом;
λ обр - интенсивность потока обращений одного клиента к серверу (1/сутки);
λ испр - интенсивность потока исправления ошибки одним программистом (1/сутки);
λ внес - интенсивность внесения ошибки при исправлении одним программистом (1/сутки) или
рвнес – вероятность внести ошибку при исправлении одним программистом;
M - количество итераций;
K – количество розыгрышей для усреднения;
Er - начальное количество ошибок.

В программе также есть возможность оценить первоначальное количество ошибок по следующему алгоритму: Принимаем ООД за единицу. Каждый клиент в запросе генерирует долю α от ООД. За время Δ t клиент обратиться к серверу (Δ t * λ обр) раз. За время Δ t все клиенты обратятся к серверу (Δ t * λ обр * K) раз. И объем данных, который будет затронут в ООД при этом равен (Δ t * λ обр * K * α). Так как в нашей модели ошибки распределены равномерно по ООД, то за время Δ t будет обнаружено (Δ t * λ ош), где ош – первоначальная интенсивность ошибок в системе. Если бы за время Δ t клиенты затронули всю ООД, то было бы обнаружены все Er ошибок. Поэтому можно записать следующую пропорцию: $\frac{\Delta t \cdot \lambda_{обр} \cdot K \cdot \alpha}{\Delta t \cdot \lambda_{ош}} = \frac{1}{Er}$. Отсюда находим Er: $Er = \frac{\lambda_{ош}}{\lambda_{обр} \cdot K \cdot \alpha}$. При этом считаем, что каждый из K клиентов обратился к серверу с запросом с данными непересекающимися в ООД. Но на самом деле это не так, т.к. чаще сего клиенты обращаются к серверу с однотипными запросами, поэтому полагаем K = 1. И тогда окончательная формула для оценки первоначального количества ошибок будет: $Er = \frac{\lambda_{ош}}{\lambda_{обр} \cdot \alpha}$;

Программа предупреждает, если задается интенсивность такая, что на интервал времени Δ t * λ) должно быть меньше единицы) – для соблюдения условия ординарности потока событий.

МОДЕЛЬ ИЗУЧЕНИЯ МЕДИАКУРСА НА ОСНОВЕ ЦЕПИ МАРКОВА

Бекназарова Саида Сафибуллаевна,
Убайдуллаев Хусанбой Илхомжон угли,
Жаумытбаева Мехрибан

Доктор технических наук, доцент, магистр, соискатель

Ташкентский Университет информационных технологий имени Мухаммада Аль-Хорезмий, Ташкент, Узбекистан

***Аннотация**: В статье рассмотрен процесс выбора изучения глав медиакурса на основе Цепи Маркова*
***Ключевые слова**: медиакурс,модель, цепи Маркова*

Пусть медиакурс состоит из глав. Очевидно, если каждая глава выбирается с положительной вероятностью, т. е. $p_i>0$ при всех i=1,..., т, то любое состояние достижимо из каждого другого состояния. Всего имеется т! различных состояний (i_1, ..., i_m) и все они будут возвратными. Если $p_i = 0$ при некотором i то все состояния вида(i_1, ..., i_m), где i_1=**i (глава с номером i находится в начале медиакурса), являются невозвратными**, так как после первого же шага для изучения выбирается некоторая глава с номером j, отличным от i, и глава с номером i, никогда не вынимаемая из списка, опускается ниже.

Наилучший выбор. Очевидно, через некоторое число шагов, не больше т (т — число всех имеющихся предметов), система попадает в состояние e_{m+1}, в котором остается навсегда. Таким образом, все состояния, кроме $e_{m+}1$, являются невозвратными.

Случайные блуждания. Рассмотрим случайное блуждание, при котором частица из каждой целочисленной точки i на следующем шаге с вероятностью p переходит в соседнюю точку j=i - 1, а с вероятностью q — в точку j=i - 1. Каждое состояние достижимо из любого другого состояния и (см. формулу (1.0))

$$p_{ii}(k)=\begin{cases}0, для k=2n+1,\\ C_{2n}^{n}p^{n}q^{n}, для k=2n.\end{cases}$$ Используя формулу Стирлинга, при n→∞ получаем

$$C_{2n}^{n}p^{n}q^{n}=\frac{(2n)}{(n!)^{2}}p^{n}q^{n}\approx\frac{\sqrt{4\pi n}\cdot(2n)^{2n}e^{-2n}}{(\sqrt{2\pi n}\cdot n^{n}\cdot e^{-n})^{n}}p^{n}q^{n}=\frac{1}{\sqrt{\pi n}}(4pq)^{n}$$

где

$$4pq=(p+q)^{2}-(p-q)^{2}=1-(p-q)^{2}\le 1,$$

причем знак равенства имеет место лишь при p = q=$\frac{1}{2}$. Таким образом, при n→∞

$p_{ii}(2n)\approx\frac{1}{\sqrt{\pi n}}(4pq)^{n}$, откуда следует, что ряды

$$\sum_{n}p_{ii}(2n) \text{ и } \sum_{n}\frac{1}{\sqrt{\pi n}}(4pq)^{n}$$

сходятся или расходятся одновременно. При p ≠ q, когда 4pq<1, ряд $\sum_{n}p_{i}(2n)$ сходится, и следовательно, каждое состояние i является невозвратным. Интуитивно ясно, что, например, при p>q блуждающая частица постепенно будет уходить все дальше и дальше в положительном направлении, рано или поздно навсегда покидая любое фиксированное состояние i. **При неограниченно продолжающемся симметрич-**

ном случайном блуждании, когда p = q=$\frac{1}{2}$, частица бесконечное число раз возвращается в каждое из состояний.

Рассмотрим теперь случайное блуждание, при котором частица из неотрицательной целой точки i

на следующем шаге с вероятностью p_i смещается в соседнюю точку j = i + 1, а с вероятностью $q_i = 1—p_i$ переходит в нулевую точку j = 0. Очевидно, если все вероятности p_i таковы, что $0<p_i<1$, то все состояния являются достижимыми одно из другого. Все они будут возвратными или невозвратными.

Предположим, что система находится в состоянии i=0. Вероятность того, что за последующие п шагов она ни разу не вернется в исходное положение i = 0, равна произведению $p_0p_1 ...p_{n-1}$ — вероятности того, что система последовательно пробегает цепочку состояний 0→1→...→п. Легко видеть, что вероятность за бесконечное число шагов ни разу не вернуться в исходное состояние **i = 0 равна бесконечному произведению**

$\prod_{k=0}^{\infty} p_k = \lim p_0 p_1 ... p_n$. Если это бесконечное произведение сходится к нулю: $\lim p_0p_1 ...p_п = 0$, то состояние i = 0 (а вместе с ним и все остальные) является возвратным. В противном случае вероятность возвращения есть $\upsilon = 1 - \lim p_0 p_1 ... p_n < 1$ и состояние i=0 (а вместе с ними все остальные) является невозвратным.

К этому результату можно прийти и другим путем, непосредственно рассматривая вероятности υ_k впервые вернуться в исходное состояние 0 ровно через **k шагов. Очевидно, частица впервые возвращает**ся в состояние 0 на k-м шаге, если она на первых k — 1 шагах последовательно переходит из состояния i—1 в i (с вероятностями p_{i-1}, i=1, ..., k — 1), и потому

$\upsilon_1 = 1 - p_0$, $\upsilon_k = p_0 p_1 ... p_{k-2}(1 - p_{k-1})$; k= 2, 3, ...

Вероятность возвращения в исходное состояние 0 по определению равна сумме $\sum_{k=1}^{\infty} \upsilon_k$ есть

$\upsilon = \sum_{k=1}^{\infty} \upsilon_k = 1 - p_0 + [p_0(1 - p_1] + ... = 1 - \lim \prod_{n=0}^{\infty} p_n$.

Рассмотрим цепь Маркова с конечным числом состояний ε_1, ε_2, ..., ε_m, каждое из которых достижимо из любого другого состояния. Более того, предположим, что существует такое N. что за N шагов система с положительной вероятностью может перейти из каждого состояния ε_i в любое

$\min p_j (N) = \delta > 0$

ЛОКАЛЬНО-КОММУНИКАЦИОННЫЕ СЕТИ

Кудратов Султон Гулямович
Ташкент Узбекистан

Локальная вычислительная сеть (ЛВС) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Существует множество способов классификации сетей. Основным критерием классификации принято считать способ администрирования. То есть в зависимости от того, как организована сеть и как она управляется, её можно отнести к локальной, распределённой, городской или глобальной сети. Управляет сетью или её сегментом сетевой администратор. В случае сложных сетей их права и обязанности строго распределены, ведётся документация и журналирование действий команды администраторов.

Компьютеры могут соединяться между собой, используя различные среды доступа: медные проводники (витая пара), оптические проводники (оптические кабели) и через радиоканал (беспроводные технологии). Проводные, оптические связи устанавливаются через Ethernet, беспроводные — через Wi-Fi, Bluetooth, GPRS и прочие средства. Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней.

Чаще всего локальные сети построены на технологиях Ethernet или Wi-Fi. Следует отметить, что ранее использовались протоколы Frame Relay, Token ring, которые на сегодняшний день встречаются всё реже, их можно увидеть лишь в специализированных лабораториях, учебных заведениях и службах. Для построения простой локальной сети используются маршрутизаторы, коммутаторы, точки беспроводного доступа, беспроводные маршрутизаторы, модемы и сетевые адаптеры. Реже используются преобразователи (конвертеры) среды, усилители сигнала (повторители разного рода) и специальные антенны.

Маршрутизация в локальных сетях используется примитивная, если она вообще необходима. Чаще всего это статическая либо динамическая маршрутизация (основанная на протоколе RIP).

Иногда в локальной сети организуются рабочие группы — формальное объединение нескольких компьютеров в группу с единым названием.

Сетевой администратор — человек, ответственный за работу локальной сети или её части. В его обязанности входит обеспечение и контроль физической связи, настройка активного оборудования, настройка общего доступа и предопределённого круга программ, обеспечивающих стабильную работу сети.

Технологии локальных сетей реализуют, как правило, функции только двух нижних уровней модели OSI - физического и канального. Функциональности этих уровней достаточно для доставки кадров в пределах стандартных топологий, которые поддерживают LAN: звезда, общая шина, кольцо и дерево. Однако из этого не следует, что компьютеры, связанные в локальную сеть, не поддерживают протоколы уровней, расположенных выше канального. Эти протоколы также устанавливаются и работают на узлах локальной сети, но выполняемые ими функции не относятся к технологии LAN.

Связь с удалённой локальной сетью, подключенной к глобальной сети, из дома/командировки/удалённого офиса часто реализуется через VPN. При этом устанавливается VPN-подключение к пограничному маршрутизатору.

Особенно популярен следующий способ организации удалённого доступа к локальной сети:

Обеспечивается подключение снаружи к маршрутизатору, например по протоколу PPPoE, PPTP или L2TP (PPTP+IPSec).

Так как в этих протоколах используется PPP, то существует возможность назначить абоненту IP-адрес. Назначается свободный (не занятый) IP-адрес из локальной сети.

Маршрутизатор (VPN, Dial-in сервер) добавляет proxyarp — запись на локальной сетевой карте для IP-адреса, который он выдал VPN-клиенту. После этого, если локальные компьютеры попытаются обратиться напрямую к выданному адресу, то они после ARP-запроса получат MAC-адрес локальной сетевой карты сервера и трафик пойдёт на сервер, а потом и в VPN-туннель.

Список литературы:

1. Новиков Ю. В., Кондратенко С. В. Основы локальных сетей. Курс лекций. — М.: Интернет-университет информационных технологий, 2005. — ISBN 5-9556-0032-9.
2. Самойленко В.В. Локальные сети. Полное руководство. — К., 2002. — ISBN 966-7140-28-8.
3. Локальные вычислительные сети: Справочник. В 3-х кн / Под.ред. С.В.Назарова. — М.: Финансы и статистика, 1994. — Т. Кн.1. Принципы построения, архитектура, коммуникационные средства. — 208 с. — 10 000 экз. — ISBN 5-279-01171-1.

DESIGN OF NEW SECURITY ALGORITHM USING HYBRID CRYPTOGRAPHY ARCHITECTURE

Mardiyev Ulugbek Rasulovich, Xolimtayeva Iqbol Ubaydullayevna

Tashkent, Uzbekistan

Abstract*. A computer network is any set of computing nodes which has the ability of exchanging data by interacting with each other meaningfully, allowing resource sharing in a proper manner. The collection of computers is interconnected by communication channels, which need to be secure for better information exchange. This field of networking consists of specialist area of network security adopted by network administrator to prevent and monitor unauthorized access, modification and denial of computer network [10]. These algorithms are required to provide data security and users authenticity. To improve the strength of these security algorithms, a new security algorithm can be designed using combination of both symmetric and asymmetric cryptographic techniques [4]. This algorithm provides three cryptographic primitives such as integrity, confidentiality and authentication. This can be achieved by the combinatorial effect of Elliptic Curve Cryptography implemented by ECDH and ECDSA, Dual RSA and Hash algorithm implemented by Message Digest 5. This new security algorithm has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.*

Keywords *Network Security; Elliptic Curve Cryptography; Dual RSA; Message Digest 5; ECDH; ECDSA*

INTRODUCTION

Cryptography is the science which uses mathematics to encrypt and decrypt data. This science enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. The science of Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, and determination. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptography basically works on the principles of mathematics that generate different algorithms known as Cryptographic Algorithms.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key [10]. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. In asymmetric cryptography, the encryption and decryption keys are different on both the sides. A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant, the functionality of a key lies in its being a string of bits determining the mapping of the plain text to the cipher text [10].

TYPES OF CRYPTOGRAPHIC ALGORITHMS

ECC (Elliptic Curve Cryptography)

While using ECC, we deal with various properties of points on curve, and functions. The only aim is to use elliptic curves as an encryption tool which converts the information m into the point P on the curve E [2]. Assuming that the data m is already in the integer or any ASCII format, we have a curve E : $y^2 = x^3 + ax + b(mod\ p)$. This will work only if $m^3 + am + b$ modulo p. Since only half of the numbers modulo p are squares, we only have about half a chance of this occurring. Thus, we embed the information m into a value that is a square.

We assume some value K such that 1/2K is an acceptable failure rate for embedding the information into a point on the curve. Also, we make sure that for the value of K, (m + 1) K < p.

Now, let xj = mK + j for j = 0, 1, 2, . . . ,K – 1, we compute x3j + axj + b. The square root yj (mod p) is calculated. If there is a square root, we let our point on E representing m be P m = (xj, yj). So, for each value of j we have a prob-

ability of about 0.5 that xj is a square modulo p [1].

Thus, the probability that no xj is a square is about 1/2K, which was the acceptable failure rate. In this way, the rate of failure of embedding the information in E decreases.

ECDH – Elliptic Curve Diffie Hellman

Using ECDH in the hybrid algorithm generates the key which is far secured than any other algorithm. The key generated is kept as a shared key between two parties, such that, it can be used for the private key algorithms [2]. Both ends have a key pair consisting of a private key d which is less than a random number n, and a public key Q = d * G, where G is the Generator point of the elliptic curve. Here, (dA, QA) is the private key - public key pair of A and (dB, QB) be the private key - public key pair of B [13]. The computation goes as,

1. The end A computes K = (xK, yK) = dA * QB
2. The end B computes L = (xL, yL) = dB * QA
3. Since dAQB = dAdBG = dBdAG = dBQA.
4. Hence the shared secret is xK

The security in encrypting the key is that is practically impossible to find the private key dA or dB from the public key K or L.

ECDSA – Elliptic Curve Digital Signature Algorithm

The ECDSA is known to be the variant of DSA, which sends a signed message from A to B, on the elliptic curve parameters [1]. For signing a message m by sender A, using A's private key dA

1. Calculate e = HASH (m)
2. Select a random integer k from [1, n í 1]
3. Calculate r = x1 (mod n), where (x1, y1) = k * G
4. Calculate s = k í 1(e + dAr) (mod n)
5. The signature is the pair (r, s)

DUAL RSA

The RSA decryption computations are performed in p and q and then combined via the Chinese Remainder Theorem (CRT) to obtain the desired solution in Z N , instead of directly computing the exponentiation in Z N . This decreases computational costs of decryption in two ways. First, computations in Zp and Zq are more efficient than the same computations in Z N since the elements are much smaller. From Lagrange's Theorem, we can replace the private exponent d with dp = d mod (p - 1) for the computation in Zp and with dq = d mod (q - 1) for the computation in Zp, which reduce the cost for each exponentiation when d is larger than the primes. It is common to refer to dp and dq as the CRT-exponents [4].

Since the method requires knowledge of p and q, the key generation algorithm needs to be modified to output the private key (d, p, q) instead of (d, N). Given the private key (d, p, q) and a valid cipher text C ε Z N , the CRTdecryption algorithm is as follows:

1) Compute $C_p = C^{dp} mod\ p$
2) Compute $C_q = C^{dq} mod\ q$
3) Compute $M_0 = (C_q - C_p).p^{-1} mod\ q$
4) Compute the plaintext $M = C_p + M_0$. P

When the primes p and q are roughly the same size, the computational cost for decryption using CRT-decryption is theoretically 1/4 the cost for decryption using the original method [7]. Using RSA-Small-e along with CRT-decryption allows for extremely fast encryption and decryption that is at most four times faster than standard RSA.

MD5 Algorithm

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is a nonlinear function; one function is used in each round. Mi denotes a 32-bit block of the message input, and Ki denotes a 32-bit constant, different for each operation. s is a shift value, which also varies for each operation.

MD5 processes a variable length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. The remaining bits are filled up with a 64-bit integer representing the length of the original message [5].

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation [12]. Many message digest functions have been proposed and are in use today. Here are just a few like HMAC, MD2, MD4, MD5, SHA, SHA-1. Here, we concentrate on MD5, one of the widely used digest functions.

HYBRID ALGORITHM ARCHITECTURE

It is desired to communicate data with high security. At present, various types of cryptographic algorithms

provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. This new security protocol has been designed for better security using a combination of both symmetric and asymmetric cryptographic techniques.

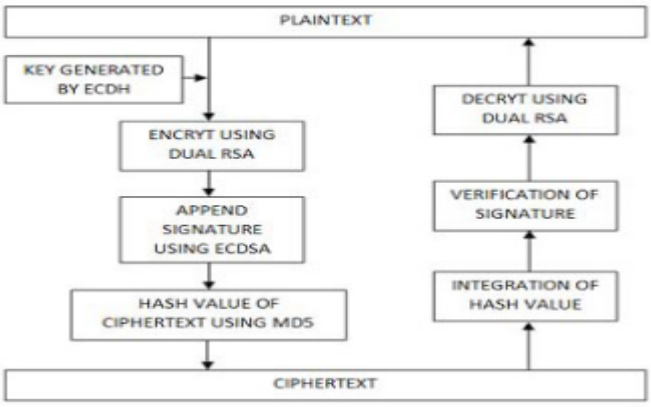


Figure 1. Hybrid Architecture for Cryptography

As shown in the figure, the Symmetric Key Cryptographic Techniques such as Advanced Elliptic Curve Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, Dual RSA used for Authentication. The above discussed three primitives can be achieved with the help of this Security Protocol Architecture. The Architecture is as shown in the Figure 1. As shown in the figure, the Symmetric Key Cryptographic Techniques such as Elliptic Curve Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, Dual RSA used for Authentication. The new Security Protocol has been designed for better security. It is a combination of both the Symmetric and Asymmetric Cryptographic Techniques. It provides the Cryptographic Primitives such as Integrity, Confidentiality and Authentication.

The given plain text can be encrypted with the help of key that is generated by the type Elliptic Curve Cryptography, i.e., ECDH. The encryption algorithm used is Dual RSA, which takes as the original information and the key. The derived cipher text is appended with the digital signature for more authentication, generated by the ECDSA algorithm. Simultaneously, the hash value of this encrypted cipher text is taken through the Message Digest 5 algorithm. Now the generated cipher text and the signature can be communicated to the destination through any secured channel. On the other side, i.e., on decryption end, the hash value is first evaluated and integrated. This is compared with the signature, for the verification of the digital signature appended at the end of message. Thereafter, the decryption of cipher text is done by Dual RSA. Hence, the plaintext can be derived.

The intruders may try to hack the original information from the encrypted messages. He may be trapped both the encrypted messages of plain text and the hash value and he will try to decrypt these messages to get original one. He might get the hash value and it is impossible to extract the plain text from the cipher text, because, the hash value is derived from the Dual RSA and appended signature, and the plain text is encrypted with Dual RSA, with the key generated by ECDH algorithm. Hence, the message can be communicated to the destination with highly secured manner. The new hash value is calculated with MD5 for the received originals messages and then it is compared with decrypted hash message for its integrity. By which, we can ensure that either the original text being altered or not in the communication medium. This is the primitive feature of this hybrid protocol.

CONCLUSION

In this paper, we proposed a robust and lightweight protocol that has security function using blind factor and ECC scheme. Our tag lightweight protocol may solve several problems as practical implement, short response time and efficient computation and the strength of cryptosystem.

The attractiveness of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability or storage are constrained.

The new Hybrid Public Key Cryptographic algorithm has been developed for better performance in terms of computation costs and memory storage requirements. From the output, it is noted that Dual-RSA and ECC, improved the performance of algorithm in terms of computation cost and memory storage requirements.

REFERENCES

[1] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation of Elliptic Curve Cryptography over Binary Fields, 2000, Available at http://citeseer.ist.psu.edu/hankerson00software.html

[2] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http://www.secg.org/download/aid-386/sec2_final.pdf

[3] E. Jochemsz and A. May, "A polynomial time attack on standard RSA with private CRT-exponents", 2007.

[4] M. J. Hinek, "Another look at small RSA exponents," in Topics in Cryptology-CT-RSA 2006, ser. Lecture Notes in Computer Science, D. Pointcheval, Ed. New York: Springer, 2006, vol. 3860, pp. 82–98.

[5] Ravindra Kumar Chahar and et.al., " Design of a new Security Protocol", IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134, 2007.

[6] S. D. Galbraith, C. Heneghan, and J. F. McKee, "Tunable balancing of RSA", 2005. Updated version of ACISP 2005.

[7] D. Bleichenbacher and A. May, "New attacks on RSA with small CRTexponent in Public Key Cryptography", PKC 2006, volume 3968 of Lecture Notes in Computer Science, pages 1–13. Springer-Verlag, 2006.

[8] B. den Boer and A. Bosselaers, "Collisions for the compression function of MD5", Advances in Cryptology, Eurocrypt „07, pages 293-304, Springer-Verlag, 2007.

[9] N. Gura, A. Patel, A. Wander, H. Eberle, and S.C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs". Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), 6th International Workshop, pages 119–132, 2004.

[10] William Stallings, " Cryptography and Network Security – Principles and Practices", 3rd Edition, Pearson Education Asia – 2003.

[11] Schneier, B., " Applied Cryptography", 2nd Edition, Wiley, 1996.

[12] Rivest, R., " The MD5 message-digest algorithm", RFC 1321, 1992.

[13] D. Johnson, "ECC, Future Resiliency and High Security Systems," Certicom White Paper, March 1999.

ИЗДАНИЕ МОНОГРАФИИ (учебного пособия, брошюры, книги)

Если Вы собираетесь выпустить монографию, издать учебное пособие, то наше Издательство готово оказать полный спектр услуг в данном направлении

Услуги по публикации научно-методической литературы:
- орфографическая, стилистическая корректировка текста («вычитка» текста);
- разработка и согласование с автором макета обложки;
- регистрация номера ISBN, присвоение кодов УДК, ББК;
- печать монографии на высококачественном полиграфическом оборудовании (цифровая печать);
- рассылка обязательных экземпляров монографии;
- доставка тиража автору и/или рассылка по согласованному списку.

Аналогичные услуги оказываются по изданию учебных пособий, брошюр, книг.

Все работы (без учета времени доставки тиража) осуществляются в течение 20 календарных дней.

Справки по тел. (347) 298-33-06, post@nauchoboz.ru.

Уважаемые читатели!

Если Вас заинтересовала какая-то публикация, близкая Вам по теме исследования, и Вы хотели бы пообщаться с автором статьи, просим обращаться в редакцию журнала, мы обязательно переправим Ваше сообщение автору.

Также приглашаем Вас к опубликованию своих научных статей на страницах других изданий - журналов «Научная перспектива», «Научный обозреватель», «Журнал научных и прикладных исследований».

Наши полные контакты Вы можете найти на сайте журнала в сети Интернет по адресу www.ran-nauka.ru. Или же обращайтесь к нам по электронной почте mail@ran-nauka.ru

С уважением, редакция журнала «Высшая Школа».

Издательство «Инфинити».
Свидетельство о государственной регистрации ПИ №ФС 77-38591.
Отпечатано в типографии «Принтекс». Тираж 500 экз.
Цена свободная.