

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ РА ЎРТА МАХСУС ТАЪЛИМ
ВАЗИРЛИГИ

НАМАНГАН МУҲАНДИСЛИК-ПЕДАГОГИКА
ИНСТИТУТИ

"Кадрлар тайёрлаш миллий дастури" ни
амалга оширишнинг II-сифат босқичи
вазифаларига бағишланган
магистрантларнинг анъанавий
III - илмий-амалий конференцияси

МАТЕРИАЛЛАРИ

I - ҚИСМ

НАМАНГАН - 2003 й

бўлинади: синтактик (матн ичидаги хатоликлар) ва алгоритмик. Синтактик хатоликларни (белгиларнинг алмашганлиги, тушириб қолдирилганлиги ва хоказолар) осон топилади. Алгоритмик хатоликларини топиш мушкулроқ кечади. Маълумотларни киритиш бир-икки бор такрорлангандан сўнг ҳам дастур тўғри ишласа, хатоликларини текшириш бўлими яқунланган ҳисобланади.

Тестдан ўтказиш босқичи ўта муҳим бўлиб, яратилган дастурдан бошқалар ҳам фойдаланиши ҳисобга олинади. Бу босқичда дастурни қанча кўп маълумотни кўтара олиши ва унда киритилиши мумкин бўлган нотўғри маълумотлар текширилади.

Юқорида келтирилган босқичлар ёрдамида ўқув жараёнига тегишли бўлган исталган жараёни автоматлаштириш мумкин.

Энди ўқув жараёнини автоматлаштириш масаласини кўриб чиқамиз:

Ушбу дастурдан фойдаланувчи жорий семестр ўқув жараёнининг боришини назорат қила олиши учун қуйидаги маълумотлар киритилиши лозим:

- гуруҳлар, талабаларнинг рўйхати;
- ўрганилаётган фанлар рўйхати;
- кафедра ўқитувчиларининг рўйхати;
- ҳар бир гуруҳнинг назарий ва амалий машғулотлари ҳақида маълумотлар;
- ҳар бир ўтказилган машғулот бўйича топширилган имтиҳонлар (синовлар) натижалари.

Дастур шундай тузилиши лозимки, тузилган дастур ёрдамида фойдаланувчи қуйидаги маълумотларни олсин:

- «Гуруҳнинг имтиҳон варақаси» номли ҳужжат;
- ҳисоб-китоб йўли билан олинган талабаларнинг ўртача бали;
- имтиҳон топширмаган талабалр сонига қараб гуруҳдаги ўртача баҳони ҳисоб-китоб қилган ҳолда топширилган имтиҳонлар натижаларининг таҳлили;
- кафедра томонидан жорий семестрда ўтказилаётган машғулотлар соатларининг умумий миқдори ҳамда ўқитувчиларнинг ўртача вазифаси.

Фойдаланувчини мазкур ахборот билан таъминлаш учун маълумотлар базасида талабалар гуруҳлари, гуруҳлар таркиби, кафедралар ва уларнинг ўқитувчилар таркиби, талабалар ўрганилаётган фанлар ҳақида сўров маълумотлари, гуруҳларда ўтказилаётган машғулотлар ва талабаларнинг жорий семестрдаги ўзлаштирувчилари ҳақидаги ҳисобот маълумотлари сақланиши лозим.

Ўқув жараёнининг боришини ахборот объектлари билан таснифланиши қуйидаги жадвалда келтирилган:

Ахборот объекти	Реквизит номи	Аломат	Калит белгиси
1	2	3	4
ГУРУҲ	Гуруҳ рақами Талабалар сони Гуруҳдаги ўртача кириш рақами	ГР ТСОН ГКБАЛЛ	Оддий калит
ТАЛАБА	Гуруҳ рақами Талабанинг рўйхатдаги рақами Фамилияси, исми, шарифи Тутилган йили Манзилгоҳи Талабанинг ўртача кириш бали	ГР ТРР ФИШ ТУҒИ АДРЕС ТКБАЛЛ	Мураккаб калит
ФАН	Фан коди Фан номи Жами соатлар Маъруза соатлари Амалиёт соатлари Семестрлар сони Курс дастури	ФК ФН СОАТЛАР МАЪРС АМАЛС СЕМС ДАСТ	Оддий калит
1	2	3	4
КАФЕДРА	Кафедра коди Кафедра номи Телефон Мудирнинг Ф.И.Ш. Мудир фотосурати	КАФК КАФН ТЕЛ МУД ФОТО	Оддий калит
ЎҚИТУВЧИ	Рўйхат рақами Ўқитувчи Ф.И.Ш. Илмий даражаси Илмий унвони Кафедра коди	ТАБР ФИШ ИЛМДАР ИЛМУН КАФК	Оддий калит

Маълумотларни муҳофаза қилишда критографик усуллардан фойдаланиш афзалликлари

Магистрант Х.Мансуров, акад. М.Комилов, талаба Ф.Ирисқулов

Интернет технологияларининг яратилиши турли манбалардан тез ва осон йўл билан ахборот олиш имкониятларини ҳамма учун оддий фуқародан тўғри йирик ташкилотларгача мисли кўрилмаган даражада ошириб юборди. Давлат муассасалари, фан-таълим муассасалари, тижорат корхоналари ва алоҳида шахслар ахборотни электрон шаклда яратиб сақлаш бошлади. Бу муҳит аввалги физикавий сақлашга нисбатан катта қулайликлар туғдиради: сақлаш

жуда ихчам, узатиш эса бир онда юз беради ва тармоқ орқали бой маълумотлар базаларига мурожаат қилиш имкониятлари жуда кенг. Ахборотдан самарали фойдаланиш имкониятлари ахборот миқдорининг тез кўпайишига олиб келди. Бу албатта оммавий ахборот ва ҳамма билиши мумкин бўлган ахборот ҳақида гап борганда ўта ижобий ҳодиса. Лекин, пинхона ва махфий ахборот оқимлари учун интернет технологиялари қулайликлар билан бир қаторда янги муаммолар келтириб чиқарди. Интернет муҳитида ахборот ҳавфсизлигига таҳдид кескин ошди:

- ахборот ўвирлаш;
- ахборот мазмунини бузиб қўйиш, эгасидан изнсиз ўзгартириб қўйиш;
- тармоққа ва серверларга ўрринча суқулиб кириш.

Ахборот ҳавфсизлигини таъминлаш қуйидаги уч асосий муаммони ечишни назарда тутади. Булар:

- пинхоналик;
- бутунлик;
- қобиллик.

НИСТ 7498-2 халқаро стандарти асосий ҳавфсизлик хизматларини белгилайди. Унинг вазифасига очик тизимлар алоқаси моделининг ҳавфсизлик йўналишларини аниқлаш киради. Булар:

1. Аутентификация. Компьютер ё тармоқ фойдаланувчисининг шахсини текшириш;
2. Киришни бошқариш. Компьютер тармоғидан фойдаланувчининг руҳсат этилган киришини текшириш ва таъминлаш;
3. Маълумотлар бутунлиги. Маълумотлар массиви мазмунини тасодифий ё қасддан беруҳсат усуллар билан ўзгартиришларга нисбатан текшириш;
4. Ахборот пинхоналиги. Ахборот мазмунини изнсиз ошқор бўлишдан ҳимоялаш;
5. Инкор эта олинмаслик. Маълумотлар массивини жўнатувчи томонидан уни жўнатганлигини ёки олувчи томонидан уни олганлигини тан олишдан бўйин товлашининг олдини олиш.

Тармоқни компьютер тажовузларидан ҳимоялаш доимий ва ўз-ўзидан ечилмайдиган масаладир. Лекин қатор оддий ҳимоя воситалари ёрдамида тармоққа суқулиб киришларнинг кўпчилигини олдини олиш мумкин.

Тажовузкорлар кўпинча тармоққа унинг аҳамиятга молик жойларидан ўтувчи трафигини тинглаш орқали, трафикдан фойдаланувчиларни ва уларнинг паролларини ажратиб олиш ёрдамида суқулиб кирадилар. Шунинг учун олисдаги машиналар

билан боғланишлар парол билан ҳимояланганда шифрланиши шарт. Бу айниқса, боғланиш интернет каналлари орқали амалга оширилганда ёки аҳамиятли сервер билан боғланилганда эҳрур. Интернет муҳити билан бирлашган интранетда ахборот оқимини ва ресурсларни энг ишончли ҳимоялаш воситаси носимметрик ва симметрик криптолизимлардан биргаликда фойдаланишдир.

Криптографик тизим, ё қисқача, криптолизим шифрлаш ҳам шифрни очиш алгоритмлари, бу алгоритмларда ишлатиладиган калитлар, шу калитларни бошқарув тизими ҳамда шифрланадиган ва шифрланган матнларнинг ўзаро боғланган мажмуасидир.

Криптолизимдан фойдаланишда матн эгаси шифрлаш алгоритми ва шифрлаш калити воситасида аввало дастлабки матнни шифрланган матнга ўтиради. Матн эгаси уни ўзи фойдаланиши учун шифрлаган бўлса (бунда калитларни бошқарув тизимига хожат ҳам бўлмайди) сақлаб қўяди ва керакли вақтда шифрланган матнни очади. Очилган матн асли (дастлабки матн)га айнан бўлса сақлаб қўйилган ахборотнинг бутунлигига ишонч ҳосил бўлади. Акс холда ахборот бутунлиги бузилган бўлиб чиқади. Агар шифрланган матн ундан қонуний фойдаланувчига (олувчига) мўлжалланган бўлса у тегишли манзилга жўнатилади. Сўнгра шифрланган матн олувчи томонидан унга аввалдан маълум бўлган шифр очиш калити ва алгоритми воситасида дастлабки матнга айлантирилади.

Бунда калитни қандай ҳосил қилиш, алоқа қатнашчиларига бу калитни махфийлиги сақланган холда етказиш, ва умуман, ишгирикчилар орасида калит узатилгунга қадар ҳавфсиз алоқа каналини ҳосил қилиш асосий муаммо бўлиб туради. Бунда яна бошқа бир муаммо аутентификация муаммоси ҳам кўндаланг бўлади. Чунки, дастлабки матн(хабар) шифрлаш калитига эга бўлган кимса томонидан шифрланади. Бу кимса калитнинг ҳақиқий эгаси бўлиши ҳам, бегона (мабодо криптолизимнинг сири очилган бўлса) бўлиши ҳам мумкин.

Алоқа ишгирикчилари шифрлаш калитини олишганда у чиндан ҳам шу калитни яратишга ваколатли кимса томонидан ё тажовузкор томонидан юборилган бўлиши ҳам мумкин.

Бутунги кунда ахборот ҳавфсизлигини таъминлашда анъанавий қўлланилиб келган ёндашувлар ва воситалар етарли бўлмай қолди. Бундай шароитда ахборот ҳимоясининг энг ишончли ва синалган усули бўлган криптографиянинг аҳамияти янада ошди.

Криптология икки илмий ирмоққа ажралади. Булар криптография ва криптоахлидир.

Криптография - криптография амаллари асосида ахборот ҳавфсизлигини таъминлаш фани бўлиб, асосан тўрт хил ҳавфсизлик муаммоси ечимларини топиш билан шугулланади. Булар:

- пинхонийлик;
- ахборот бутунлиги;
- аутентификация;

- ахборот эгасини аутентификацияси - ахборот юборган шахснинг асл шахслигини текшириш;
- ахборот асл нусхасини аутентификацияси - олинган ахборот ўз аслига айнанлигини текшириш.
- алоқа қатнашчилари назорати:
 - инкор этаолмаслик - ахборот йўллаганликни ё уни (умуман ё ўз вақтида) қабул қилиб олганликни бўйнига олмасликни оддини олиш.

Криптография амалларининг энг асосийлари шифрлаш ва шифрни очишдир. Шифрлаш - шифрлаш калити иштирокида берилган (дастлабки) ахборотни бегона олиб тушунмайдиган шаклга, яъни шифрланган ахборотга айлантиришдир. Шифрни очиш - шифрланган ахборотни уни очиш калити ёрдамида дастлабки ахборотга айлантиришдир. Шифрни бузиб очиш - шифрланган ахборотни шифрни очиш калитини билмаган ҳолда дастлабки ахборотга айлантиришдир.

Шифрлаш пинҳонийликни таъминлаб, ахборотни бегоналардан махфий сақлаш имконини беради. Шифрланадиган ахборот, умуман олганда матн, овоз ёзуви ва тасвир шаклида, ё бўлмаса аралаш шаклда берилиши мумкин. Амалиётда шифрланадиган ахборот асосан матн шаклида берилади ва шифрланган матнга айлантирилади.

Криптография усуллари алоқа тизимининг ҳавфсизлигини таъминлаш учун қўлланилганда у алоқа мазмунининг, яъни узатилаётган ахборотнинг ўзинингига ҳимоялайди, алоқа мавжудлигини, шу жумладан алоқанинг кимлар орасида ва қандай интенсивликда содир бўлаётганини эса ҳимоя қилолмайди.

Ахборот узатиш ва сақлаш жараёнларининг рақамлаштирилиши узлукли (нутқ) ва узлуксиз (матн, факс, тасвир, анимация) ахборотларни ҳимоялаш учун ягона алгоритмлардан фойдаланиш имконини беради. Бундан буён шифрланадиган ахборот матн шаклида берилиши назарда тутилади.

Симметрик криптоотизимларда ахборот алмашиш уч босқичда юз беради:

- ахборот жўнатувчи уни олувчига ўзаро махфий калитни, яъни икковларидан ўзга ҳеч кимга маълум бўлмаган калитни топширади;
- жўнатувчи ўзаро махфий калит билан ахборотни шифрлаб уни олувчига жўнатади;
- қабул қилиб олувчи ахборотни олиб унинг шифрини ўзаро махфий калит билан очади. Умуман олганда иккала томон бу калитдан бир неча бор қайта фойдаланишлари мумкин.

Шу калитдан алоқа учун қайта фойдаланилганда ёки калит ахборот эгасининг ўзи ишлатадиган матнни шифрлаш учун тузилган бўлса, албатта, шифрланадиган ахборот миқдори билан тенг калитдан фойдаланиш ҳар доим ҳам қулай бўлавермайди. Биринчи босқичга хожат бўлмайди. Агар ҳар кун ва ҳар бир алоқа сеанси учун янги

ноёб калит ишлатилса, криптоотизимнинг ҳавфсизлиги юқорироқ бўлади.

Носимметрик криптоотизимларда ахборот алмашиш қуйидаги босқичларда юз беради:

- ахборот қабул қилиб олувчи томон уни тайёрлаб жўнатувчига ўзининг шахсий ошқора калити маълум бўлишига эришади, бу калит бошқа кимсаларга ҳам маълум қилиниши мумкин;
- жўнатувчи томон ахборотни уни қабул қилиб олувчининг шахсий ошқора калити билан шифрлаб уни олувчига жўнатади;
- қабул қилиб олувчи томон шифрланган ахборотни олиб, унинг шифрини ўзининг шахсий махфий калити билан очади. Бу шифрланган ахборотни ошқора калит эгасидан ўзга ҳеч ким очаолмайди, чунки уларда бунга мос махфий калит йўқ.

Умуман олганда, битта ошқора калитдан бир неча киши кўп мартаба фойдаланиб, ягона манзилга-шу ошқора калит эгасига турли ахборотлар жўнатишлари мумкин. Кўпчилик шу ошқора калитдан унинг эгаси рақамли имзо чеккан ҳужжатларнинг унга тегишли эканига ишонч ҳосил қилиш мақсадида ҳам фойдаланиши мумкин. Чунки, бу ошқора калит билан фақатгина унинг эгаси ўз махфий калити билан имзолаган ҳужжатлардаги имзоларнигина шифрини очиш мумкин.

Амалиётда икки хил тизимни биргаликда ишлатиш юқори самара беради: симметрик тизимдан кўп ҳажмли ахборотларни шифрлашда, носимметрик тизимдан симметрик тизим калитини шифрлаб тарқатишда фойдаланиш қулай.

Чегаравий масалаларни ечишда С.К.Годуновнинг ортоганал хайдаш усули афзалликлари

Магистрант М.Дадамирзаев, доц.С.Ирисқулов

Амалий масалаларнинг математик моделлари кўпинча қуйидаги биринчи тарғибли дифференциал тенгламалар системаси учун ёзилган чегаравий масала орқали ифодаланади:

$$\frac{dy}{dx} = [A(x)]y + b(x) \quad (1)$$

чегаравий шартларни умумий ҳолда қуйидагича ёзиб оламиз:
 $x = x_0$ (интеграллаш оралигини чап чегараси) нуқтада

$$|C_0|y = |C_0|y^{(n)} \quad (2)$$

$x = x_1$ (интеграллаш оралигини ўнг чегараси) нуқтада

$$|C_1|y = |C_1|y^{(n)} \quad (3)$$

бу ерда

17. Магистрант А. Маматханов. Меҳнат ресурсларидан фойдаланиш самарадорлигини ошириш	50
18. Магистрант: Исаков Б., доц. С. Хошимов. Замонавий фермер хўжаликлари бошқарувида ахборот таъминоти тизимини тутган ўрни	59
19. Магистрантлар Р.Мирзаолимов, Х.Эралиев, доц. Д. Эшонхўжаев. Иқтисодий эркинлаштириш шароитида қишлоқ хўжалик корхоналарини бошқаришни такомиллаштириш хусусида	61
20. Магистрантлар Х.Эралиев, Р.Мирзаолимов, доц. Р.Исmoilов. Банкротлик ва уни олдини олиш тўғрисида (Вилоят саноат корхоналари мисолида)	64
21. Магистрант Ж.Рахимов, доц. С.Назимов. Наманган вилоятида иш жойларини ташкил этишни бошқариш ва уни ривожлантириш	67
22. Магистрант Р.Каримов. Наманган вилояти саноат корхоналарида меҳнатни илмий ташкил этиш ва бошқарувни такомиллаштириш	70
23. Магистрант Э. Тошпулатов. Автокорхоналарда иқтисодий самарадорлик кўрсаткичлари ва уларни оширишнинг аҳамияти	72
24. Магистрантлар Э.Тошпулатов, Х.Каримова. Автотранспорт комплекси иншоотлари қурилиши муддатини қисқартириш самарадорлиги	75
25. Магистрант Э. Тошпулатов. Автотранспорт корхоналарининг самарадорлигини ошириш масаласи	77
26. Магистрант Ф.Ўринов. Ишлаб чиқаришга инвестицияларни жалб қилиш	82
27. Магистрант Ш. Хошимов, доц. Д.Эшонхўжаев. Қишлоқ хўжалигида менежмент тизими самарадорлиги ва уни ошириш имкониятлари (Наманган вилояти қишлоқ хўжалиги корхоналари мисолида)	84
28. Магистр Ш. Дедамирзаева, проф. Т.Мирзамахмудов. Қишлоқ хўжалигида моддий техника таъминотини такомиллаштиришни бошқариш	87
29. Магистрант Ш. Эшонхўжаева, проф.Т. Мирзамахмудов. Қўшма корхоналарни ташкил этиш ва бошқариш самарадорлигини ошириш	90
30. Магистрант Г. Мирзаабдуллаева, доц. С. Бузрукхонов. Иқтисодий эркинлаштириш шароитида мулкдорлар синфини ривожланиши	94
31. Магистрант Н.Шарипова. Регионал бозорда баҳо белгиланишининг баъзи хусусиятлари	96

32. К. Ишматов, А. Каюмов. Магистр методик тайёргарлигининг педагогик асослари	99
33. Магистрант Н. Курбонов, проф. И. Алимов (Тошкент), Г. Жўраев. Иссиқлик тарқалиши стационар тенгламаси учун биринчи чегаравий масала	101
34. Магистрант Б. Абдулхафизов, доц. М.Олимов, К.Ишматов. Академик лицейларда ўқув-тарбиявий жараён самарадорлигини оширишда янги ахборот технологияларнинг роли	105
35. Магистрант О.Камолитдинов, доц. М.Джурабоев. Физико-химические свойства природной воды и их изменение электрическими воздействиями	108
36. Магистрант Д. Юсупов, доц. М.Тошмирзаев. Термохимия қурилмаси	112
37. Магистрантлар Т.Жўраев, Н.Курбонов, проф. И.Алимов, доц. А.Имомов. Параболик типдаги тенгламани ечиш учун алгоритм дастурлар боғламини яратиш технологияси	114
38. Магистрант Б. Эргашев, И. Алимов, О. Жакбаров. Газ фильтрацияси жараёнини математик моделини ва ҳисоблаш алгоритминини қуриш	117
39. Магистрант Р. Хакимов, доц. Ё. Тиллабоев. Чегаравий қатлам масалаларини ечишда сонли усуллардан фойдаланиш имкониятлари ҳақида	122
40. Магистрант Б. Эргашев, доц. С. Ирискулов. Амалий дастур боғламини яратиш технологияси ҳақида	124
41. Магистрант С.Ўришова, доц. П.Каримов. Касб-хунар коллежларида ўқув жараёнини бошқаришни маълумотлар базасини такомиллаштириш	126
42. Магистрант К. Мансуров, акад. М. Комилов, талаба Ф.Ирискулов. Маълумотларни муҳофаза қилишда криптографик усуллардан фойдаланиш афзалликлари	129
43. Магистрант М. Дадамирзаев, доц.С. Ирискулов. Чегаравий масалаларни ечишда С.К.Годуновнинг ортогонал хайдаш усули афзалликлари	133
44. Талаба И.Ахмаджанов, доц. М.Олимов. Еалқани эгилиш ва сурилишини эластик ва неэластик ҳолатини аниқлаш алгоритми ҳақида	137
45. М. Исманова, К. Исманова, доц. С. Ирискулов. «Аниқ интегралларни тақрибий ҳисоблаш»ни ўргатувчи дастур таъминоти яратишнинг бир усули ҳақида	137
46. Магистрант Х. Қаноатов, доц. Х. Хошимов. Сабзавотлардан жон ишлаб чиқариш технологиясини такомиллаштириш	140