1 – кесте. Ўақытты синхронлаўға ҳәм санақты синхронлаўға тийкарланған OTP протоколларының анализи

Синхронла-ныўшы шама	Қәўипсизлик	Пайдаланыўда
Ўақытқа	*Артық:* OTP мәниси қысқа ўақыт ушын бар.	*Артық:* OTPды қурылма экранынан аңсатлық пенен оқыў мүмкин.
	Кем: OTP мәниси гүзетиўши тәрепинен аңсатлық пенен алыныўы мүмкин.	*Кем:* OTP мәниси ол киритилгенге шекем өзгериўи мүмкин.
Санақ	*Артық:* OTPды генерация қылыў ушын бузғыншы қурылманы басқарыўы талап етиледи.	*Артық:* OTP мәниси пайдаланыў-шының сораўына қарай генерация қылынады; белгили ўақыттан кейин оның мәниси өзгерип қалмайды.
	Кем: OTPды таза OTP пайдаланыўға шекем пайдаланыў мүмкин болады.	*Кем:* OTPды генерация қылыў ушын пайдаланыўшы “генерация қылыў” түймесин басыўы талап етиледи.

SMS (инглиз тилинде *Short Message Service* — «қысқа хабар хызмети») арқалы узатыў – банк – финанс тараўында төлемлерди әмелге асырыўда кең қолланылыўшы ҳәм барлық түрдеги мобил қурылмалар ушын зәрүр болған усыл есапланса да, қатаң қәўипсизлик машқаласына ийе. Яғный, SMS хабарларды ашық ҳалатта жиберилиўи ямаса SS7 маршрутлаў протоколындағы қәўипсизлик машқалалары себепли, оларда жиберилген OTP ды аңсатлық пенен қолға киргизиў мүмкин.

c) Сервер тәрепинен генерация қылынған OTPлар қарыйдарға веб браузерге арнаўлы көринисте усынылады.OTPды жеткизиўдиң бул усылына вебге тийкарланған усылды киргизиў мүмкин. Бул усыл пайдаланыўшының тосыннан усынылған сүўретлери арасынан алдыннан таңланғанларын таныў қәбилетине тийкарланған. Пайдаланыўшы дәслеп дизимнен өтиўде усынылған нәрселердиң (пышық, машина, гүллер ҳәм жасырын топарын таңлайды. Аутентификациядан өтиў даўамында система оған тосыннан таңланған нәрселерди (әлбетте, алдын таңлаған нәрселери де олар арасында болады) усынады. Ҳәр бир усынылғанлардың арқа фонында тәкирарланбас цифр бар болады. Пайдаланыўшы тәрепинен усынылғанлар арасынан алдыннан таңланғанлары белгиленеди ҳәм бул жағдайда арқа фонындағы цифрлар тосыннанлық OTPды пайда етеди [5:3].

Буннан тысқары, Confident Technologies тәрепинен ислеп шығылған вебке тийкарланған OTP системасында аутентификациядан өтиў ўақтында мобил телефонға сүўретлерди таңлаў имканиятын бериўши силтемени жибереди. Бул силтемеге мүрәжат болғанда веб браузерге сүўретлер арасынан кереклисин таңлаў ҳәм OTPды генерация қылыў әмелге асырылады.

Қолланыўда кең пайдаланыўы көзқарасынан SMSке жибериўге тийкарланған жеткизиў усылы қалғанлары ажыралып турса да, онда қәўипсизлик машқалалары критикалық жағдайларда пайдаланыўды шеклейди. Қурылма көринисиндеги токенлер жоқары қәўипсизликти тәмийинлесе де, оның жоқары баҳалылығы ҳәм барқулла бирге алып жүриў зәрүрлиги себепли қолайсызлықларға себеп болады. Ҳәзирги күнге келип мобил қурылмалардың кең тарқалыўы ҳәм инсанлардың ажыралмас жолдасына айланыўы программалық көринистеги токенлерден пайдаланыў имканиятын асырады. Бирақ, мобил операциялық системалардың қәўипсиз емеслиги ямаса “желке арқалы қараў” сыяқлы ҳүжимлер нәтийжесинде қосымша қәўипсизлик шараларын көриў талап етиледи [1:8].

Почта арқалы жибериў ямаса қағазда жазған ҳалда алып жүриў сәйкес түрде қосымша билимди (почта паролин) ямаса барқулла қасында қәўипсиз сақлаў зәрүрлигин талап етеди. Вебке тийкарланған усыллар болса ҳәзирги күнде кирип киятырған жаңа түсиниклер болып, инсан ядында аңсат сақлаў усылынан пайдаланыўға ҳәрекет етеди.

Әдебиятлар

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. -М.: ИД ФОРУМ, ИНФРА-М. 2011.
2. Knuth D. E. Art of computer programming, Seminumerical algorithms, AddisonWesley Professional, 2. 2014.
3. Alzomai M.H. Identity management: strengthening one-time password authentication through usability: dis. Џ Queensland University of Technology, 2011.
4. Takasuke TSUJI, A One-Time Password Authentication Method, MasterЎs thesis, January 31, 2003.
5. Каримов М.М., Арзиева Ж.Т., Худойкулов З.Т. Муҳаммад Ал-Хоразмий Авлодлари. Илмий-амалий ва ахборот-таҳлилий журнал 4(10) 2019, 3-б.

РЕЗЮМЕ

Ушбу мақолада бир мартали пароллар асосида бир йўналишли аутентификация протоколларининг таҳлили келтирилган. Бир йўналишли бир мартали паролларга асосланган аутентификация усулларида OTPларни етказиш усулларининг қиёсий таҳлили келтирилган.

РЕЗЮМЕ

В статье представлен анализ протоколов односторонней аутентификации на основе одноразовых паролей. Представлен сравнительный анализ способов передачи OTP в методах аутентификации на основе одноразовых паролей.

SUMMARY

The article deals with the state presented the analysis of protocols of single authentication on the basis of single passwords. A comparative analysis is presented OTP transmission methods in autnentification methods based on one-time passwords.

“АМАЛИЙ МЕХАНИКА” ФАНИНИ ЎҚИТИШДА ИННОВАЦИОН ТАЪЛИМ ТЕХНОЛОГИЯЛАРИДАН ФОЙДАЛАНИШ ИСТИҚБОЛЛАРИ

З.Р.Асраев – *таянч докторант*

Бухоро муҳандислик-технология институти

Таянч сўзлар: инновация, инновацион таълим технологиялари, замонавий таълим технологиялари, интерфаол усуллар, кичик гуруҳларда ишлаш, ахборот-коммуникация технологиялари.

Ключевые слова: инновация, инновационные образовательные технологии, современные образовательные технологии, интерактивные методы, работа в малых группах, информационно – коммуникационные технологии.

Key words: innovation, innovative educational technologies, modern educational technologies, interactive methods, work in small groups, information and communication technologies.

Ўзбекистон Республикаси таълим йўналишларининг малакавий талабларидан келиб чиққан ҳолда техник йўналишлар бакалаврларини тайёрлаш бўйича ўқув дастурларини амалга ошириш шартларига қўйилган талаблардан бири бу талабаларнинг касбий компетентлигини шакллантириш учун соҳада инновацион таълим

технологияларидан кенг фойдаланишдир.

Ҳозирги вақтда таълимнинг интерактив шаклларини жорий этиш етук кадрларни тайёрлашни такомиллаштиришнинг энг муҳим инновацион йўналишларидан биридир. Амалиёт шуни кўрсатадики, олий ўқув юртлари битирувчилари зарурий билимга эга, аммо улар ҳар доим ҳам уни амалда самарали қўллай олмайдилар.

Интерфаол таълим - ўқув фаолиятини ташкил этишнинг махсус шакли бўлиб, у ўқув материалини ўзлаштиришда, ахборот ва билим алмашишда ўқувчиларнинг биргаликдаги фаолиятидан иборат. Интерфаол таълим анъанавий ўқитиш шаклларига нисбатан ўқитувчи ва талабанинг ўзаро муносабатларини ўзгартиради. Ҳозирги вақтда талабалар фанни яхши ўзлаштиришлари учун ўқитувчининг ўқитадиган фан соҳасидаги компетентлиги зарур, аммо етарли шарти эмас. Замонавий ўқитувчи қуйидагиларга эга бўлиши керак [1]:

- талабаларни фанни ўрганишга ундаш;
- келажакдаги амалий фаолиятда зарур бўлган аниқ билимларни мустақил ўзлаштиришга ўргатиш;
- шахсий хусусиятларни ва келажакдаги касбий фаолиятнинг ўзига хос хусусиятларини ҳисобга олиш.

"Инновация" атамаси лотинча innovati сўзидан келиб чиққан бўлиб, янгилик деган маъноно англатади. “Инновация” тушунчасига иккита ёндашув мавжуд: инновация жараён сифатида (А.В. Лоренс, М. М. Поташник, В. А. Сластенин, О. Г. Хомерики) ва инновацион янгилик сифатида ўзи (К. Ангеловски, А. Ф. Балакирев, С. Д. Ильенкова) [2].

А.В. Хуторской инновацион жараённинг учта таркибий қисмининг бирлигини таъкидлайди: инновацияларни яратиш, ўзлаштириш ва қўллаш. Айнан шу уч қисмли инновацион жараён илмий тадқиқот объекти ўқув жараёни бўлган дидактикадан фарқли равишда педагогик инновацияда энг кўп ўрганиш объекти ҳисобланади [3].

Педагогик инновация – педагогик фаолиятдаги янгиликлар, ўқитиш ва тарбия мазмуни ва технологиясидаги ўзгаришлардир. Педагогик инновациялар таълим ва тарбия самарадорлигини оширишга қаратилган: мақсад ва мазмун билан таништириш, ўқитувчи ва ўқувчининг биргаликдаги фаолиятини ташкил этиш [2,3].

Энг сўнгги инновацион тенденциялар қаторида замонавий таълимда устун бўлиши керак бўлган педагогик жараённинг шахсга йўналтирилганига асосланган педагогик технологияларни таъкидлаш керак. Ўқитувчи ва талабанинг шахсга йўналтирилган ўзаро таъсири таълим жараёнининг энг муҳим таркибий қисмига айланиб бормоқда. Таълим жараёни ўқитувчининг ўқувчилар билан мулоқотига асосланади. Кўпгина психологлар ва ўқитувчиларнинг фикрига кўра, муваффақиятли мулоқот учун учта омил асосий аҳамиятга эга: маърузачининг ишончлилиги; хабарларнинг тушунарлилиги, уни қанчалик тўғри тушунганлиги ҳақидаги фикр-мулоҳазаларни сўраш. Бундай ҳолда, мулоқот этикасининг умум инсоний қоидаларини ҳисобга олиш керак. Лекин мулоқотнинг педагогик шартларига мансуб бўлган асосий омил ўқитувчининг фанни чуқур билишидир. Ўқитувчи олий ўқув юртидаги ўқув жараёнининг марказий шахсидир. У мустақил равишда таълим мақсадларини қўяди, ўз фаолияти воситаларини танлайди, ўқувчиларнинг нафақат келажакдаги касбига, балки умуман фанга қизиқишини ривожлантиради. Айнан ўқитувчининг фанни равон эгаллаши ўқувчиларда билимга бўлган қизиқишни оширишга, ўқитувчи ва унинг талабларини ҳурмат қилишга ундайди [4].

Замонавий таълим жараёни техник, хусусан, компьютер ва дастурий таъминот инновациялари ҳисобига такомиллаштирилмоқда. Айнан шунинг учун ҳам дастлаб билимларни оммалаштириш ва кенг аудиторияни ўқитишга жалб қилиш учун мўлжалланган аудио ва видео визуал усуллар ўқитишда тобора кўпроқ фойдаланилмоқда. Мутахассисларни касбий тайёрлашда техник ўқув қўлланмаларини кенг жорий этиш, Интернет тармоғидан фойдаланиш, ўқув жараёнида электрон маълумотлар базалари билан ишлаш талабаларнинг билим фаоллигини оширади, бу эса ўқув материалини сезиларли даражада ўзлаштириш учун вақтни максимал даражада тежаш имконини беради. Аудио ва видео визуал усуллар барча фанларни ўқитиш учун улкан имкониятларга эга. Шу билан бирга, у ўқитувчидан компютер билимлари ва технологияларига эга бўлишни, фанга тизимли ва ижодий қарашни талаб қилади. Усулнинг самарадорлиги ўқиш вақтининг минимал сарфланиши ва талабалар ва ўқитувчиларнинг саъй-ҳаракатларини тежаш билан белгиланади [5].

Шуни таъкидлаш керакки, интерфаол технологиялар фойдаланувчига ҳар қандай вақтда фанларни ўрганишда ўқитувчи (шунингдек, курсдошлар) ёрдамини олиши мумкинлигига ишонч ҳосил қилади, талабаларга катта ҳажмдаги назарий материални ўзлаштириш, назорат фаолиятини ёки курс лойиҳасини мустақил бажариш имконини беради. Шу билан бирга ўқитувчи ўқувчининг мустақил дарсдан ташқари ишларини холисона кузатиб бориш имкониятига эга бўлади [6].

Бухоро муҳандислик-технология институти “Амалий механика” кафедраси ўқитувчилари ўқув жараёнида инновацион таълим технологияларидан фаол фойдаланмоқда. Ушбу мақола мазкур ишларнинг циклини давом эттириб, "Амалий механика" курси бўйича дарсларни ўтказишда замонавий инновацион технологиялардан фойдаланишга бағишланган.

“Амалий механика” курсини ўрганиш маърузалар, лаборатория, амалий машғулотлар ва мустақил ишлар (умумийлаштирилган типик масалаларни ечиш, ўқув тажрибаларини ўрнатиш, ҳисоблаш ва график ишларни бажариш ва лойиҳа фаолияти ва бошқалар) орқали тизимли равишда амалга оширилади.

Амалий механикани ўрганишни ташкил этиш жараёнида ўқитувчи бир нечта жиддий муаммоларни ҳал қилади:

- дарсга тизимли тайёргарлик кўраётган ўқувчилар билан бирга машғулотларда мунтазам иштирок этмаган ўқувчиларнинг ишларида фаол иштирок этишини таъминлайди;
- ўқув материалини ўзлаштириш жараёни устидан доимий назоратни ўрнатади;
- ўқувчилар эътиборини маълумотни оддий такрорлашга эмас, балки топшириқнинг бир нечта ёндашувларини ижодий излашга қаратади.

Л.Я.Калашникованинг фикрича, "Амалий механика" курсининг маърузалари бўлажак технологик таълим бакалаврининг умумтехник тайёргарлигида муҳим ўрин тутади [7].

"Амалий механика" курси бўйича маърузалар ўқув материали мазмунининг асосларини очиб беради, фан ва техниканинг моддий ишлаб чиқариш соҳасидаги муносабатлари ҳақидаги назарий билимларни умумлаштиради ва тизимлаштиради. Бундан ташқари, улар талабаларни технологик таълимнинг бўлажак бакалаврларининг касбий фаолияти учун умумтехник билимларнинг аҳамиятига ишонтирадилар, уларни илмий- техник адабиётларга йўналтирадилар; умумтехника фанлари бўйича ўз билим ва кўникмаларини мустақил равишда чуқурлаштиришга интилишни уйғотади.

“Амалий механика” курсини ўрганиш жараёнида ўқитишнинг турли хилдаги маъруза шаклларидан (ахборотли, муаммоли, маъруза-визуаллаштириш,

маъруза-конференция, маъруза-маслаҳат) фойдаланилади. Курснинг назарий материалини яхшироқ ўзлаштириш учун маърузаларда илмий маълумотларни янада қулайроқ шаклда тақдим этиш имконини берадиган ва талабаларнинг билимини фаоллаштиришга ёрдам берадиган таркибий - мантиқий схемалар қўлланилади. Маърузалар кўргазмали қуроллар, слайдлар, виртуал кўргазмалар ёрдамида олиб борилади. Амалий машғулотларда эса кичик гуруҳларда ишлаш, муаммоли топшириқлар, лойиҳаларни тайёрлаш каби усуллар қўлланилади.

Кичик гуруҳларда ишлаш энг машҳур стратегиялардан бири ва кўплаб интерфаол усулларнинг ажралмас қисмидир. “Амалий механика” фанидан кичик гуруҳларда дарс ташкил этишда ўқитувчи барча талабаларнинг, шу жумладан уятчан ўқувчиларга ишда иштирок этиш имкониятини беради. Янги материални масалалар ечиш билан тушунтирилгандан сўнг, талабаларга масалалар тўплами (тахминан 7-10 та қисқа масала ва саволлар) берилади. Ушбу масалалар энг қобилиятли талабалар томонидан 15-20 дақиқада ечиш учун мўлжалланган. Ечимни биринчи бўлиб тугатган ўқувчилар ишни тугатмаган ўқувчиларга гуруҳларни ташкил қилиш йўли билан ўтадилар ва биргаликда масалалар ечишни якунлайдилар.

“Амалий механика” фанини ўқитишда ахборот-коммуникация технологияларидан фойдаланиш ниҳоятда самаралидир. Ахборот технологияларини қўллаш орқали талабалар ўз касбий фаолиятида эгаллаган кўникмалардан муваффақиятли фойдаланадилар. Ахборот-коммуникация технологиялари янги дидактик муаммоларни ҳал этиш, ўқитиш сифати ва самарадорлигини ошириш имконини беради. Улар ёрдамида матн, товуш, график ва видео маълумотлардан янгича фойдаланиш мумкин ва бу ижодкорликка бўлган қизиқишни оширади, ўқувчиларнинг билиш фаолиятини рағбатлантиради.

Амалий механика курси бўйича талабаларни касбий тайёрлашда инновацион ўқитиш усулларининг афзалликлари қуйидаги устуворликлар билан белгиланади:

- ўқувчилар янги материални ўқув жараёнининг фаол иштирокчилари сифатида ўзлаштирадилар;
- бўлажак мутахассислар ахборотни қайта ишлашнинг замонавий технологиялари бўйича кўникмаларга эга бўладилар;
- маълумотнома маълумотлари, техник ва меъёрий ҳужжатларни мустақил ўрганиш ва таҳлил қилиш, уларга киритилган ўзгаришларни кузатиб бориш кўникмасини ривожлантиради;
- олинган маълумотларнинг самарадорлиги ва долзарблиги: ўқувчилар ўз касбий фаолиятларида рўй берадиган қийин амалий вазиятларни ҳал қиладилар;
- интерфаол ўқитиш усуллари ўқувчиларга ўқитувчи билан доимий алоқада бўлиш имконини беради. Улар таълим жараёнини янада профессионаллаштиради.

Шундай қилиб, талабаларнинг замонавий таълим технологияларидан фойдаланган ҳолда эгаллайдиган билим ва кўникмалари уларни касбий фаолиятда қўллаш имконини беради, бу эса ҳар бир талабанинг имкониятларини, унинг меҳнат бозорида рақобатбардошлигини тўлиқ рўёбга чиқаришга олиб келади.

Адабиётлар

1-5. Использование современных образовательных технологий при изучении механики Косогова Ю.П., Пинчук Э.В., Годунов С.Ф., Пирожков Р.В. Элект. научный журнал Инженерный вестник Дона, №3 2016. ivdon.ru/ru/magazine/archive/n3y2016/3748.

6. Иванченко В.Н. Инновации в образовании: общее и дополнительное образование детей: учебно-методическое пособие. -Ростов н/Д: «Феникс», 2011. – С. 341.

7. http://www.eidos.ru/journal/2005/0910–19.htm интернет-журнал «ЭЙДОС».

8. Волосова Е.В. Внедрение инновационных технологий в современный процесс обучения. Научные труды SWorld. 2013. Т. 25. № 3.- С. 66-69.

9. Тайэбех Д. Психолого-педагогические условия внедрения в учебно-воспитательный процесс инновационных методов и технологий обучения. Вестник Педагогического университета. 2012. № 5-1 (48). -С. 48-51.

10. Абидов К.З. Создание математических моделей реальных процессов на основе компьютерных технологий. Международная научно-практическая конференция: Реальность – сумма информационных технологий. –Курск: 08-10 сентября. 2016. -С. 32-34.

РЕЗЮМЕ

Мақолада олий ўқув юртларида “Амалий механика” фанини ўрганишда инновацион ўқитиш методлари мажмуасини жорий этиш бўйича маълум тажрибалар келтирилган. Таърифланган инновацион ўқитиш технологиялари "Амалий механика" курсини ўқитишда талабаларнинг ўқув - билиш фаолиятини сезиларли даражада фаоллаштиришга имкон беради.

РЕЗЮМЕ

В работе представлен определённый опыт реализации совокупности инновационных методов обучения при изучении прикладной механики в высших учебных заведениях. Описанные инновационные технологии обучения позволяют в значительной степени активизировать учебно-познавательную деятельность студентов в обучении курса «Прикладная механика».

SUMMARY

The paper presents exact experience in the implementation of a set of innovative teaching methods in the study of applied mechanics in higher educational institutions. The described innovative teaching technologies make it possible to significantly intensify the educational and cognitive activity of students in teaching the course "Applied Mechanics".

STEREOMETRIYALÍQ MÁSELELERDI SHESHIWDEGI ÁHMIYETLI BAYLANÍS

S.M.Daniyarova – *doktorant*

Ájiniyaz atındaǵı Nókis mámleketlik pedagogikalıq institutı

Tayanch so’zlar: geometriya, fazo, geometrik figura, burchak, bog’lanish.

Ключевые слова: геометрия, пространство, геометрическая фигура, угол, связь.

Key words: geometry, space, geometric figure, angle, connection.

Mektep oqıwshılarında keńislik túsinikleriniń qáliplesiwi bilim beriw sistemasındaǵı baslı máselelerden esaplanadı. Eger oqıwshılarda keńislik túsinikleri jaqsı qáliplesken hám rawajlanǵan bolsa, olardıń geometriyanı ózlestiriwi ańsat boladı hám olar bir qansha qızıqlı máselelerdi óz betinshe sheshe aladı [1].

Ilim menen texnikanıń rawajlanıwına say oqıwshılardıń keńislik túsiniklerin qáliplestiriw olardı ámeliy is-háreketke, qásip-óner tarawında miynet etiwge, fizika, astronomiya, kosmonavtikanıń házirgi mashqalaların túsinip jetiwge eń zárúrli elementleri bolatuǵınlıǵı túsinikli [2].

N.F.Chetveruxin «Jaqsı keńislikli oylaw jańa mashinalardı dóretetuǵın konstruktorǵa, jer astı baylıqların izertlewshi geologqa, jańa qalalardıń jayların quratuǵın arxitektorǵa , xirurgqa, xudojniklerge hám t.b. júdá zárúr» dep ekenligin atap kórsetedi.

Mektep oqıwshılarında keńislik túsinikleriniń qáliplesiwi hám rawajlanıwında geometriyalıq figuralardıń sızılmaların jasaw úlken áhmiyetke iye. Oqıwshılardıń keńislik túsinigi qansha joqarı bolsa, olarǵa geometriyanı úyretiw sonshelli ańsat, olardıń aldına hár qıylı qıyın hám qızıqlı máselelerdi qoyıw múmkin. Tilekke qarsı, keńislik geometriyalıq faktlerin modellestiriwde hám olardı taxtada súwretlewde oqıwshılardıń qıynalatuǵınlıǵın bayqaymız. Keyingi jıllarda mektep pitkeriwshileriniń matematikalıq tayarlıǵındaǵı bul kemshilikler jiyi-jiyi bilinedi. Bul