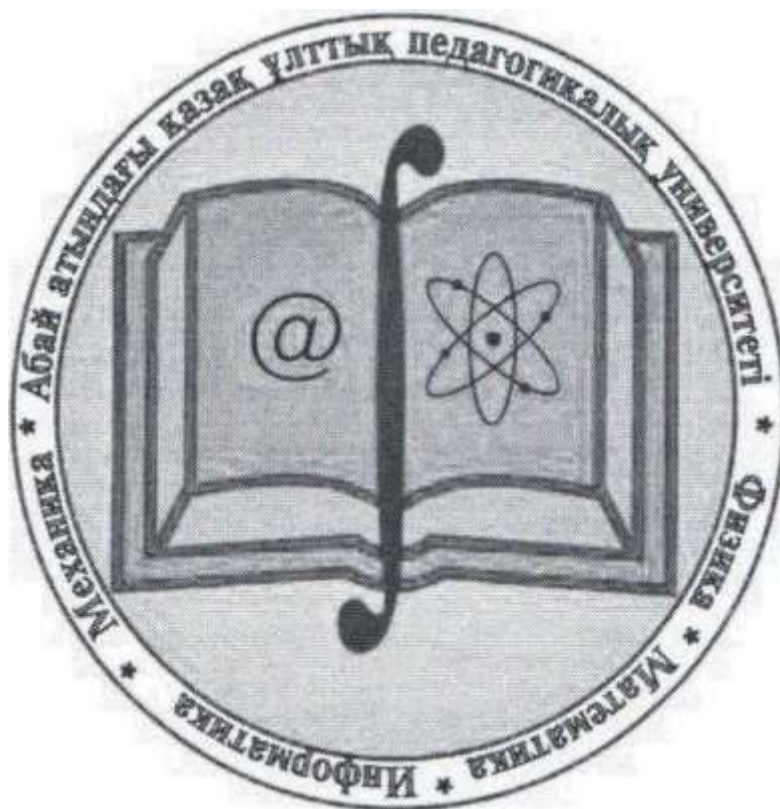




Абай атындағы
Казак ұлттық педагогикалық университет!

Казахский национальный педагогический
университет имени Абая

ХАБАРШЫ ВЕСТНИК



№ 1 (53)

2016

Алматы

**Казахский национальный
педагогический университет
имени Абая
ВЕСТНИК
серия “Физико-математические науки”**

№ 1 (53)

**Главный редактор
Академик НАН РК Г.У. Уалиев**

Редакционная коллегия:

зам.главного редактора:

д.п.н. Е.Ы. Бидайбеков,

к.ф.-м.н. М.Ж. Бекпатшаев

ответ, секретарь

к.п.н. Г.А. Абдулкаримова

члены:

Dr.-ing. Holm Altenbach(Germany),

Dr. S.A.Hasan (Pakistan),

Dr. Yasuhide Fukumoto(Japan),

Phd.d Shuo-Hung Chang, (Taiwan),

д.п.н., академик РАО А.Е. Абылкасымова,

д.ф.-м.н. М.А. Бектемесов,

д.ф.-м.н. А.С.Бердышев,

д.п.н. В.В. Гриншкун (Россия),

к.ф.-м.н. Ф.Р. Гусманова,

д.т.н. А.Д.Джураев(Узбекистан),

д.ф.-м.н., чл.-кор. РАН СМ. Кабанихин

(Россия),

д.ф.-м.н. Б.А. Кожамкулов,

д.ф.-м.н., чл.-кор. НАН РК В.Н. Косов,

д.ф.-м.н. К.К. Коксалов,

д.т.н. М.К. Кулбеков,

д.п.н., академик РАО М.П. Лапчик

(Россия),

д.ф.-м.н. К-М. Мукашев,

д.ф.-м.н. С.Т. Мухамбетжанов,

д.т.н. Г.Я. Пановко (Россия),

д.п.н. Б.Д. Сыдыков,

д.ф.-м.н., академик НАН РК Н.Ж. Такибаев,

д.ф.-м.н. К.Б. Тлебаев,

д.т.н. А.К. Тулешов,

д.ф.-м.н. З.Г. Уалиев,

д.ф.-м.н., чл.-кор. НАН РК Л.М. Чечин,

к.ф.-м.н. Е.Б. Шалбаев,

к.т.н.ШМ. Хамраев

©Казахский национальный

педагогический университет

им. Абая, 2016

Зарегистрирован в Министерстве
информации Республики Казахстан,

№4824-Ж - 15.03.2004

(периодичность-4 номера в год)

Выходит с 2000 года

Редакторы:®.Р. Гусманова,

Г.А. Абдулкаримова

Компьютерная верстка:

Г.А. Абдулкаримова

Ф.Р. Гусманова

Подписано в печать 18.03.2016 г.

Формат 60x84 1/8.

Об 9,95 уч.-изд.л.

Тираж 300 экз.

050010, г.Алматы, пр.Достык, 13,

КазНПУ им.Абая

Отпечатано в типографии

"TOO Palitra Press "

г.Алматы, ул.Хамиди 4а

Д.А. Кинжебаева, А.С. Сарсекеева Анализ движения
системы «электрический двигатель - механизм IV класса с
высшем ведомых звеньев» при разгоне 117

В. Н. Косов, С.А. Красиков, О.В. Федоренко,
Г. Акылбекова Создание модуля опытного устройства
для разделения природных газов..... 123

М. Кошербай, Д.А. Кинжебаева «КОМПАС - 3D V15»
багдарламасы арқылы шахмат фигураны жасау

технологиясы 128

Д.Р. Сатывалдиев, Ж. Сагындыков, К.М. Мукашев

Новые образовательные технологии при изучении
физических и химических понятий с применением

анимационно - электронных учебников 135

Г. Уалиев, З.Г. Уалиев Динамический анализ механизмов
независимого движения 139

*ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОҚЫТУ
ЭДІСТЕМЕСІ. БІЛІМ БЕРУ ДІАКПАРА ТТАН ДЫРУ
ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ
ИНФОРМАТИКИ. ИНФОРМАТИЗАЦИЯ
ОБРАЗОВАНИЯ*

О. С. Ахметова, С.А. Исаев, М.Т. Шуйнбаева

Организация проектно-исследовательской деятельности при
изучении информатики в младших классах **К.В. Баскаков,**

А.Ю. Пыркова Технология

фрагментированного программирования JJQ

И.У. Бекбулатова, С.А. Бахтыбаева, Г.П. Мейрбекова,

Г.Ж. Ниязова Булпык технологиялардың бшм берудеп

мумкшдштер! 158

D.A. Berdysheva Automated analysis in education 163

К.М. Беркимбаев, И.У. Бекбулатова, Г.Ж. Ниязова,

Б.Т. Керимбаева Болашак мугалшшщ коммуникативтш элеуетш

калыптастыру мэселелер! i6g

М.О. Беркинбаев, Ш.И. Байметова, Э.Х. Сарыбаева,

С. А. Бактыбаева Электрондық опыту

жуйе« 174

куралдарын колдану элеуеп 174

К.С. Бертаева, С.А. Исаев, О.С. Ахметова Влияние

повышения уровня ИКТ-компетентности учителя на

развитие функциональной грамотности учащихся у 80

Ф.Р. Гусманова, Г.А. Абдулкаримова Ойындар

теориясының концепциясының неппшде онтайлы

шештмдердi кабылдаудагы аныкгалмагандыктыщ кауш-

катермен озара байланысы 185

М.Н. Калимолдаев, А.А. Абдилдаева,

М.А. Ахметжанов, М.Ж. Сақыпбекова Электр энергетикалык

жуйесше акдараттык жуйе куру **С.Н. Конева** Особенности

применения Intranet- технологий в условиях кредитной системы

обучения 1

Р.Р. Мусабиев, П.Б. Сейсенбекова Казак тшш синтездеу

урфлицНе интонациялык модельдердщ колданылуы 203

Л.Б. Рахимжанова, Д.Н. Исабаева Ролевая игра при

обучении алгоритму электронной цифровой подписи RSA

..... 208

Н.С. Уалиев, А.А. Сакабаев Обеспечение защиты

информации при интеграции информационно-

образовательных сред в мобильные Web-приложения 213

К.З. Халыкова Болашак информатикфа мамандарын даярлау

процесшде студенттердщ зерттеу iс-эрекетш уйымдастыру

К.З. Халыкова, Р.А. Ильясова, М. Булатаева Action Script 3

объекте багытталган программалау тшш оқытудын

ереKinenifcrepi

П.Т. Шекербекбаева, Ұ-К- Амантаева Электрондық оку куралын

жасау технологиялары мен эдаешн 231

**ИНФОРМАТИКА. ИНФОРМАТИВНЫ ОЦЫТУ ЭДІСТЕМЕСІ.
БІЛІМ БЕРУДІ АКПАРАГІАНДЫРУ
ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ
ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ**

Abstract. This article discusses the speech synthesis and speech synthesis model. On the basis **BI** the synthesis of the Kazakh language the advantages of intonation models are investigated. An individual analysis of each of the models Intsint, Fudjisaki AM., Tilt models for modeling speech synthesis is performed. More suitable for the synthesis of the Kazakh language is a model Fudjisaki.

Keywords: Intsint model, Fudjisaki model, AM model, Tilt model, intonation, synthesizer.

УДК 37.022

Л.Б. Рахимжанова, Д.Н. Исабаева¹

**РОЛЕВАЯ ИГРА ПРИ ОБУЧЕНИИ АЛГОРИТМУ ЭЛЕКТРОННОЙ
ЦИФРОВОЙ ПОДПИСИ RSA**

(г. Алматы, Казахский национальный государственный университет им. аль - Фараби,
Казахский национальный педагогический университет им. Абая)

Аннотация. Цель данной статьи рассмотреть методику применения ролевой игры **пр** - обучении электронной цифровой подписи RSA. Для эффективного использования метода **ролевой** игры необходимо мотивировать студентов, вызывать у них интерес и желание к **обучению** путем пояснения важности изучения алгоритма электронной цифровой подписи в своей **будущей** профессиональной деятельности. Преподавателю необходимо основательно подготовиться **с** проведению ролевой игры, определить, кто исполняет роли создателей подписей и кто **ролл** распознавателей (проверяющих подлинность) подписи, проводить занятие в дружеской, | креативной обстановке. Студенту дается возможность увидеть свои ошибки и признать **их** с помощью моделируемой профессиональной ситуации, например получение ЭЦП клиента **банка**

Ключевые слова: Ролевая игра, электронная цифровая подпись, обучение, методика обучения.

Ролевые игры как метод в образовании был известен с конца 1940-х, но было достаточно проблем с его использованием. И лишь с 1970-х он широко используется в качестве части поведенческой терапии для подготовки к профессиональной деятельности, приобретения социальных навыков обучения. В странах СНГ ролевые игры широко используются при проведении различных тренингов при принятии на работу, для изучения иностранного языка. Например, при театральной постановке на иностранном языке актеры вынуждены знать иностранный язык для общения с собеседником, возникает необходимая мотивация для учащихся при такой ролевой игре для использования языка как родного.

Из приведенного примера ясно, что человек учится и развивается только тогда- когда попадает в безвыходную ситуацию. При этом мозг включает режим выживания и начинает работать так, как будто есть угроза спокойствию, жизни, здоровью следовательно, он обучается незнакомому. Получается, что метод ролевой игры при обучении применяется, в том числе, и для того, чтобы создать эти «тяжелые обстоятельства». Таким образом, ролевые игры - это метод для необходимого изучения вопросов в указанных ситуациях, являющийся технологией активизации и ускорения- обучения.

С другой стороны, эффективность обучения по таксономии Блума, заключается в том, что учащиеся должны выполнять задания сами и уметь объяснять решения другим. как видно из рисунка 1, в 80 % своей учебной деятельности. А что так помогает в этом.

как не ролевая игра. Ролевое общение реализуется в ролевой игре - виде общения, который организуется в соответствии с разработанным распределенными ролями и межролевыми отношениями [1].

При изучении иностранного языка Н.А. Комина в [2] сформулировала следующие

Эффективность видов обучения

I проведения ролевой игры:

формирование участников о предстоящей игре;



работка элементов языкового материала в предречевых упражнениях;

Рисунок 1. Эффективность видов обучения.

работка языкового материала в речевых упражнениях;

оведение ролевой игры.

ключите льный этап:

денка речевой деятельности участников;

зализ типичных речевых и языковых ошибок;

осуждение коммуникативного поведения участников игры.

ютрим методику использования ролевой игры при обучении алгоритму

ж цифровой подписи (ЭЦП) RSA в курсе «Криптографические методы
формации».

>,готовительный этап. Прежде всего, если сравнить образно: это как шие электроинструментов в столярной. Инструменты не панацея, и они хорошо, только, если умело их использовать, но при небрежном обращении гтрументы могут быть опасны. Даже старомодные типы пил и молотков могут щерб. если не знать или не

помнить принципы безопасности при их [и. Как плотники должны быть специалистами в области многих компонентов а, так и учитель должен быть хорошо обучен и компетентен в различных (той роли (Рисунок 2). Проведение ролевых игр требует от преподавателя й предварительной подготовки, немаловажно, чтобы учащиеся поверили, что им о правильно, естественно и убедительно сыграть свою роль, щаете алгоритма ЭЦП RSA учителю надо определить, какие роли будут играть гудентов, какие создателей подписей и какие распознавателей подписи.

Ъ 1 (53)

2016

**ИНФОРМАТИКА. ИНФОРМАТИКАНЫ ОЦЫТУ ЭДІСТЕМЕСІ.
БІЛІМ БЕРУДІ АКПАРЛМ АНДЫРУ
ИНФОРМАТИКА, МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ
ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ**

Определить поэтапное выполнение алгоритма. Объяснить к каким последствиям могут привести неправильное создание ЭЦП, а еще хуже не распознавание неправильной подписи.

Далее в ролевой игре нужно правильно выбрать лидера. Это импровизационная процедура, и импровизация требует чувство относительной безопасности. Это как роль хирурга, который знает, как подготовить пациента к операции. Необходимо провести "разминочные" общения студентов, в процессе которых они узнают друг друга в более доверительной манере и все участвуют в теме. Преподавателю надо научиться разогреть аудиторию и сохранить этот настрой на всю ролевую игру.

Трансформация роли: п р е п о д а в а т е л я



Рисунок 2. Трансформация роли преподавателя.

При изучении RSA лидер сразу выявляется среди студентов, это те, кто: предлагают различные подписи, при этом анализирую весь алгоритм, чтобы получить вг очень сложную ЭЦП.

Из-за не разогретой преподавателем аудитории обязательно найдется студент, который имел неприятные переживания с ролью и в результате играет ее без энтузиазма. Конечно, при назначении роли преподаватель может навязать действие, обратившие - с одному "Ты будешь определять функцию Эйлера для произведения выбранных проста^х, чисел", и к другому, "Хорошо, а ты парень тот, кто определит секретный ключ - действуй"! Но если вдруг студентам не хватает информации, то те, которых «бросили» в за ситуацию будут чувствовать себя, как будто их бросили в пруд и им придется сре-л научиться плавать. Во избежание такого результата, преподавателю, как **драматургу** нужно вначале поговорить с каждым из игроков, взять у них интервью "в роли", узн их мысли о связанных аспектах их роли, мягко вовлечь их в ситуации, дать возможн оа творческому подходу.

Проведение ролевой игры. При неправильном распределении ролей, преподаватель дал ход своим собственным импульсам, возникает так назы групповая проблема. Необходимо изучить некоторые проблемы группы с упором реальную личную проблему каждого индивида. Так, например, если у студента съ проблема со знанием простых чисел, то он легко может выдать секретный сопернику из-за давления или неуверенности.

Предотвратить эти ошибки не намного сложнее, чем выучить правила техники безопасности для электроинструментов в магазине мебели, для этого должны быть вовремя приняты меры, чтобы научить решать такие вопросы, и такие действия должны периодически повторяться (Таблица 1) [3].

Таблица 1. Роли в алгоритме RSA

Роль создателей ключей	Роль подписывающих сообщение	Роль подтверждающих ЭЦП
1. Выбираются два случайных простых числа p и q таких, что $p \sim q$. 2. Вычисляется их произведение $n = p \cdot q$. 3. Вычисляется функция Эйлера для n $\phi(n) = (p-1) \cdot (q-1)$. 4. Выбирается открытая экспонента e такая, что $1 < e < \phi(n)$ и $(e, \phi(n)) = 1$. 5. Вычисляется секретная экспонента d , удовлетворяющая условию $(e \cdot d) \bmod \phi(n) = 1$. $K_o = (e, n)$ - открытый ключ, $K_c = (d, n)$ - секретный ключ подписи.	1. Сжимается сообщение M с помощью хеш-функции h в целое число m : $t = h(M)$. 2. Вычисляется цифровая подпись $S = m^d \bmod n$. 3. Пара (M, S) передается получателю как электронный документ M , подписанный цифровой подписью S . 4. Подпись S формируется обладателем секретного ключа (d, n) .	1. Получатель (M', S) вычисляет хеш-образ сообщения M' : восстанавливает хеш-образ $m = S^e \bmod n$. находит результат хеширования t'' принятого сообщения M' с помощью такой же хеш-функции h : $m' = h(M')$. 2. Если $h(M') = S^e \bmod n$, то получатель признает пару (M, S) подлинной.

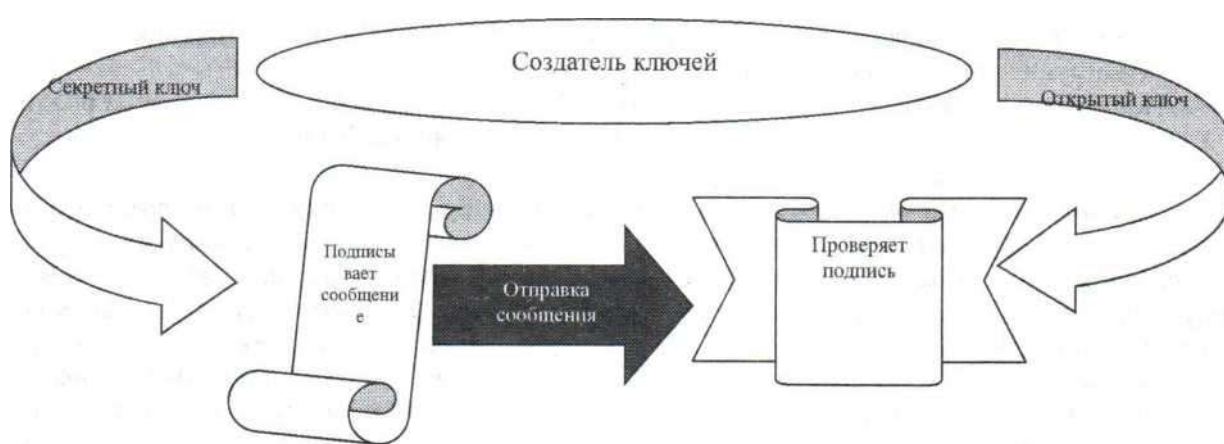


Рисунок 3. Схема проведения ролевой игры

Заключительный этап. При подведении итогов одна из ошибок студентов связана с общей тенденцией предполагать, что межличностные навыки легче, чем технические навыки - хотя на самом деле они еще более сложны. Так люди склонны думать, что они

могут участвовать в профессиональной ситуации, прежде чем они действительно достигли уровня мастерства при голой компетенции. Допустим, студент оказался в профессиональной ситуации, получил не подлинную подпись или не то сообщение, хотя он уверен, что все верно. В реальной ситуации, например, получение неправильной ЭЦП клиента банка стоит финансовых потерь банка.

Задача управляющего игрой не в резкой, а доброжелательной форме постепеш: указывать на ошибки.

Таким образом, для эффективного изучения алгоритма RSA при использовании метода ролевой игры необходимо:

- мотивировать студентов, вызывать у них интерес и желание к обучению путем пояснения важности изучения алгоритма электронной цифровой подписи в своей будущей профессиональной деятельности;

- преподавателю основательно подготовиться к проведению ролевой **игры** определить, кто исполняет роли создателей ключей, роли подписчиков сообщения, и роли распознавателей (проверяющих подлинность) подписи;

- проводить занятие в дружелюбной, креативной обстановке;

- активизировать деятельность студента путем вызванного интереса индивидуального участия, что дает возможность не только узнать о материале, но интегрировать знания в действие, путем решения проблемы, исследуя альтернатива поиска новых и творческих решений;

- студенту увидеть свои ошибки и признать, что совершает он их не мало. Для ? с помощью ролевой игры моделируется профессиональная ситуация, напр получение ЭЦП клиента банка.

Ролевые игры это лучший способ развить навыки инициативы, межличн связи, решения проблем, самосознания, совместной работы в командах, и это, всего, конечно, не только обучение простым фактам, многие, если не большинстве которых будут устаревшими или не будут иметь значения в течении несколько лет. помощь молодым людям быть готовыми к вызовам XXI века.

1. Шатилов С.Ф. Методика обучения немецкому языку в средней школе. - Просвет 1977.-295с.
2. Комина Н.А. Методика использования ролевой игры в учебном процессе, мир лингви и коммуникации. - № 3 (8) - Тверь, 2007
3. Афанасьева М. Криптография: Методическое пособие по выполнению лабораторных j - Чувашский государственный университет им. И.Н. Ульянова, 2014 г.

Лидатна. Мацапананыц максаты RSA электрондыц цифрлыц цолтацбаны оцъгтуда **рвдт** ойындарды цолдану эдІстемеЫ царастырылады. Ролд'ис ойындар **sdic'm tuiMdi** цолданудт студенттердиц оцуга цызыгушылыгы мен ттеглн болашагыц кзегби к'-эрекегтндегл электрондыц цифрлыц цолтацбаныц алгоритмы оцып-уйренудиц мацыздылыгын тусіндіру аркел-я: ынталандыру керек. Оцытушыга **рвдт** ойынды жург'гзуге дайындалу цажет, сондай-ак **кши** жазбаны жасаушы жэне ки цолтацбаны танушы (цолтацбаны тексеруий) аныцтау, сабакэчы достыц жэне сыни ортада журглзу керек. Студентке вз цателшн кору жэне вз цателжтгрж улгтенген кэс 'юи жагдай квмегтен тани быу, мысалы банк клиенттиц электрондыц цифрлв ктти алу мумктдт оерііеді.

Тушн **евздер:** **рвдтЫ** ойын, электрондыц цифрлыц цолтацба, оцыту, оцыту **adicmeMeci**

Abstract The purpose of this article to examine the methodology of application of role-pla. .nr. games in the training algorithm RSA electronic signature. To make effective use of the method of **robl** playing games is necessary to motivate students, arouse their interest and desire to learn by explainrm:

the importance of studying the algorithm of electronic digital signature in their future careers. Teachers need to thoroughly prepare for the role play to determine who takes the role of creators of signatures and who the role resolvers (authenticates) signatures, conduct classes in a friendly, creative atmosphere. The student is given the opportunity to see their mistakes and admit them through simulated professional situations, such as getting the customer with electronic bank.

Keywords: Role play, digital signature, training, methodology of training.

УДК 374.1:004.087

Н.С. Уалиев, А.А. Сакабаев

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИНТЕГРАЦИИ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНЫХ СРЕД В МОБИЛЬНЫЕ WEB-ПРИЛОЖЕНИЯ

(г. Талдыкогран, Жетысуский государственный университет им. И.Жансугурова, *- магистрант)

Аннотация. В данной статье описываются конкретные прикладные методы по реализации комплексной защиты информации при разработке информационно-образовательной среды, для использования ее на мобильных устройствах в виде адаптивного веб-приложения. В том числе, приведено теоретическое обоснование достоинств от реализации и применения информационно-образовательных сред в виде адаптивных веб-приложений. Отмечены базовые принципы обучения на основе мобильных устройств.

А также в статье выявлены и раскрыты основные виды современных угроз для мобильных устройств. С учетом специфики работы информационно-образовательных сред на мобильных устройствах отображены наиболее важные аспекты, к которым необходимо уделить пристальное внимание при анализе и выборе программных продуктов для реализации веб-приложений.

Ключевые слова: защита информации, мобильное web-приложение, мобильные платформы, информационно-образовательная среда.

В эпоху стремительного развития мобильных коммуникативных технологий, к современному образованию, в условиях его уровня роста и активного развития, предъявляются повышенные требования, связанные прежде всего с результатами освоения основных образовательных программ. Возникает острая потребность в квалифицированной подготовке специалистов, которые будут способны в своей профессиональной деятельности использовать информационно-образовательные среды и продукты.

В то же время, в условиях перехода к концепции личностно-ориентированного подхода в обучении и имманентного образования возникает острая необходимость применения в образовательных целях не только средств ИКТ, но и современных видов носителей информации, выработанных на мобильной основе. Именно качественный симбиоз интегрированных образовательных сред и современных Smart устройств дает возможность реализации модернизации методик образования, обозначенных в Послании Президента Республики Казахстан - Н.А. Назарбаева народу Казахстана «Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства», в котором четко поставлена задача «интенсивно внедрять инновационные методы, решения и инструменты в отечественную систему образования, включая дистанционное обучение и обучение в режиме онлайн, доступные для всех желающих.» А также необходимости