# Методологические основы построения защищенных гарантноспособных информационных систем дистанционного обучения высших учебных заведений

**Андрей Александрович Серов**
студент
Национальный исследовательский университет ИТМО
Москва, Россия
serov.serov.11@mail.ru
0000-0000-0000-0000

**Василиса Андреевна Авдонина**
студент
Национальный исследовательский университет ИТМО
Москва, Россия
av.vasilisa.av@gmail.com
0000-0000-0000-0000

**Александра Александровна Свиридова**
студент
Национальный исследовательский университет ИТМО
Москва, Россия
Sviridovaaa290420@ya.ru
0000-0000-0000-0000

**Анна Игоревна Мирошниченко**
студент
Национальный исследовательский университет ИТМО
Москва, Россия
Miroshai@ya.ru
0000-0000-0000-0000

**Илья Георгиевич Карибов**
студент
Кубанский государственный медицинский университет
Краснодар, Россия
Karinovilgeo@ya.ru
0000-0000-0000-0000

Поступила в редакцию 12.04.2022
Принята 17.05.2022
Опубликована 20.06.2022

10.25726/a0841-1021-7964-i

**Аннотация**

Вопросы автоматизации деловых процессов в вузе, в частности, информационно-технологического обеспечения дистанционного получения высшего образования уже на протяжении последних 30 лет являются предметом многих исследований и горячих дискуссий научно-педагогических работников, а также объектом особого внимания со стороны общества. В то же время, развитие событий последних лет, связанных с распространением карантинных мер в связи с пандемией COVID-19,

свидетельствует, что в течение первых трех месяцев карантина наблюдалась ограниченная готовность учебных заведений, в частности, среднего образования, эффективно проводить полноценный учебный процесс. Успехи в этом направлении в вузе недостаточно освещены в научных изданиях, но собственный опыт преподавания автором статьи ряда учебных дисциплин в вузе свидетельствует, что достижения в победных чиновников несколько преувеличены. Следует обратить внимание, что подавляющее большинство известных автору проблемных ситуаций в учебных заведениях, связанных с использованием большого количества различных программных платформ, ориентированных на электронное обучение, обусловлены в первую очередь их неполным соответствием образовательному процессу, который определен законами, а также недостаточным вниманием со стороны разработчиков относительно учета требований к защите информации и кибербезопасности.

**Ключевые слова**
вуз, информационная безопасность, кибербезопасность, защита.

## Введение

В работе (Морозова, 2017) исследованы принципы и методы повышения эффективности автоматизации учреждений образования на основе онтологического подхода, в системном исследовании (Верещагина, 2019) проведен подробный анализ современного состояния дистанционного обучения и применения технологий дистанционного обучения в вузах России, определены технологические решения, способствующие совершенствованию результатов применения технологий дистанционного обучения в вузе.

В работе (Nalan, 2015) проведен анализ систем электронного документооборота с точки зрения процессного подхода для оценки перспектив использования систем автоматизации делопроизводства в вузе, а в работе (Дьяконова, 2012) приведены данные сравнительного анализа двадцатку лучших с точки зрения пользователей программных платформ для организации дистанционного (электронного) обучения, в том числе, для университетского обучения.

Несмотря на то, что системная разработка исходных технических требований к формированию защищенных гарантоспособных информационных систем дистанционного получения высшего образования осталась за пределами многих научных исследований, в рамках данной работы с целью создания предпосылок для построения современного отечественного программно-технического обеспечения и материальной базы вуза представляется целесообразным восполнить этот пробел.

В частности, необходимо проанализировать "узкие места" существующих программных комплексов электронного обучения, сформировать актуальную модель угроз безопасности функционирования защищенной гарантоспособной информационной системы дистанционного обучения вуза, определить и обосновать требования по конкретным методам защиты (Кобзева, 2012).

Также необходимо отметить, что до сих пор ни в одной научной публикации вопрос функциональной безопасности информационных систем дистанционного обучения не рассматривался.

## Материалы и методы исследования

Целью статьи является разработка и исследование методологических основ построения ЗГИС дистанционного обучения в вузе, включая:

- определение основных задач ЗГИС в условиях обеспечения совместимости различных форм обучения (очная, заочная, дистанционная) соискателей высшего образования;
- формирование на основании требований законодательства о высшем образовании онтологии сущностей образовательного процесса как основы построения ЗГИС;
- анализ составляющей гарантоспособности и формирование модели угроз для ЗГИС;
- определение факторов, влияющих на академическую добропорядочность участников образовательного процесса, и механизмов ЗГИС для противодействия этим негативным факторам.

Прежде всего, следует обратить внимание, что понятие «автоматизация вуза», «создание системы электронного документооборота вуза» и «создание защищенной гарантоспособной

информационной системы дистанционного обучения вуза» в значительной степени коррелированны, но не являются тождественными, поскольку имеют целью различные приоритеты в автоматизации бизнес-процессов, разный объем задач и функции создаваемой и/или применяемой автоматизированной системы (Новиков, 2019).

В рамках статьи под понятием «гарантоспособная информационная система дистанционного обучения учреждения высшего образования» подразумевается автоматизированная система, обеспечивающая поддержку образовательного процесса в вузе и с участием участников указанного процесса качественных образовательных услуг в соответствии с требованиями законодательства в течение установленного времени.

При этом образовательный процесс (далее ОП) рассматривается как система научно-методических и педагогических мероприятий, направленных на развитие личности путем формирования и применения его компетенций (Бондарев, 2021), а участниками образовательного процесса (далее УОП) в вузе имеются научные, научно-педагогические и педагогические работники (далее-НПР); соискатели высшего образования (ВО) и другие лица, обучающиеся в учреждениях высшего образования, а также специалисты-практики, которые привлекаются к образовательному процессу в образовательно-профессиональных программах, и другие работники вуза (Введение, 2018).

Вспомним некоторые определения, касающиеся объекта исследования, в частности, согласно (Мельников, 2021), гарантоспособностью компьютерной системы называется ее способность предоставлять услуги, которым можно оправдано доверять.

Гарантоспособность является комплексным свойством, которое включает безотказность, готовность, живучесть, функциональную безопасность, целостность, конфиденциальность, достоверность и обслуживаемость.

Также обратим внимание на определение законодательства (Введение, 2018), дающих основания для построения онтологии основных сущностей образовательного процесса:

– образовательная (образовательно-профессиональная программа (далее ОПП) – единый комплекс образовательных компонентов (учебных дисциплин, индивидуальных заданий, практик, контрольных мероприятий), направленных на достижение предусмотренных такой программой результатов обучения, что дает право на получение определенной образовательной или образовательной и профессиональной квалификации;

– результаты обучения – знания, умения, навыки, способы мышления, взгляды, ценности, другие личные качества, которые можно идентифицировать, спланировать, оценить и измерить и которые личность способна продемонстрировать после завершения образовательной программы (программные результаты обучения) или отдельных образовательных компонентов; компетенций (результатов обучения);

– компетентность – динамическая комбинация знаний, умений, навыков, способов мышления, взглядов, ценностей, других личных качеств, что определяет способность человека успешно социализироваться, проводить профессиональную и/или дальнейшую учебную деятельность.

## Результаты и обсуждение

Исходя из того, что обычная образовательная деятельность осуществляется в специально приспособленных и должным образом обустроенных помещениях (аудиториях, классах, лабораториях, залах, центрах и т. п) и на основании определения закона, что дистанционная форма получения образования является индивидуализированным процессом, что происходит в основном за опосредованного взаимодействия удаленных друг от друга участников образовательного процесса и добавляем в специализированном среде, функционирующего на основе современных информационно-коммуникационных технологий, возможно сделать вывод о необходимости создания соответствующей специальной среды в киберпространстве-учебной среды вуза (По данным Statista, 2018).

Учитывая это, для обеспечения полной совместимости очного и заочного обучения по дистанционным нужно выполнить проектирование виртуальных (электронных) аналогов материальных

объектов обычного образовательного процесса таким образом, чтобы с помощью информационной системы решить следующие задачи:

– обеспечение предоставления ВО образовательных услуг, которым гарантированно возможно доверять;

– содействие академической мобильности, избежанию лишних сложностей при переходе ВО с одной формы обучения на другую;

– повышение эффективности образовательного процесса путем автоматизации рутинных процедур;

– избегание негативного влияния информационной системы дистанционного обучения на психофизическое состояние ВО;

– уменьшение рисков возможных потерь вследствие кибератак на информационную структуру образовательного процесса, а также незаконных умышленных или случайных действий его участников. При этом должна быть обеспечена юридическая сила электронных документов в соответствии с требованиями законодательства (Ищейнов , 2020; Клименко , 2021; Клековкина, 2014).

Целесообразно отметить, что вопрос построения специальной среды в киберпространстве имеет существенные отличия в зависимости от специальности ВО.

Дальнейшее преподавание преимущественно (но не исключительно) ориентируется на подготовку специалистов в области информационных (компьютерных) технологий и кибербезопасности.

Составляющими образовательного (учебного) процесса, в частности, являются:

– корпоративные хранилища знаний и ресурсов (библиотеки учебных информационных ресурсов, прикладных/учебных, специальных программ, моделирующих комплексов и т. п);

– планирующие документы и методическое обеспечение учебного процесса (учебные планы и программы, расписание занятий, рабочие программы учебных дисциплин, методические комплексы для проведения лекций, семинаров, практических и лабораторных занятий и т. п);

– индивидуальные и групповые учетные документы учебного процесса (зачетные книжки, журналы учета учебных групп, зачетные и экзаменационные ведомости, отчеты государственных экзаменационных комиссий и др);

– документы текущего контроля качества усвоения учебных программ (выполнены соискателями высшего образования контрольные работы, тесты, рефераты, курсовые и дипломные работы и прочее).

Обратим внимание, что перевод исключительно в электронный вид планирующих и учетных документов образовательного процесса, а также документов текущего контроля качества усвоения учебных программ по условию создания дружественных интерфейсов и удобных механизмов обобщения данных в программном обеспечении информационной системы дистанционного обучения позволяет сократить время на выполнение рутинных процедур и повысить эффективность работы УОП.

Следует подчеркнуть, что в построенной модели доверие к результатам обучения и/или научных достижений обеспечивается преимущественно академической добродетелью как совокупности этических принципов и правил, которыми должны руководствоваться УОП во время обучения, преподавания и осуществления научной деятельности (Бондарев,2021; Введение, 2018), чего явно недостаточно для достижения гарантоспособности информационной системы в условиях реализации вероятных угроз безопасности антропогенного (далее АС), техногенного (далее ТС) и природного (ПО) характера.

Во-первых, проанализируем возможные последствия реализации определенных видов угроз. Заметим, что до сих пор научным сообществом не принята парадигма рационального построения модели угроз для гарантоспособности информационных систем, поэтому представляется целесообразным исходить из методологических основ построения модели угроз в случаях обеспечения информационной и кибербезопасности.

Исходя из приведенной онтологии сущностей образовательного процесса и несмотря на то, что фактически в настоящее время для дистанционного получения образовательных услуг ВО используют большое разнообразие устройств от относительно простых смартфонов, планшетов и ноутбуков в более

мощных десктопов, возможно сделать вывод, что рациональным выбором для построения учебной среды дистанционной системы будет архитектура типа «клиент-сервер».

Наибольшую ценность в учебной среде имеют корпоративные хранилища знаний и ресурсов, которые требуют обеспечения доступности и целостности, а также учетные документы образовательного процесса (необходимо обеспечить их целостность и аутентичность), что делает их приоритетными объектами страхования в информационной системе.

Угрозы техногенного характера для гарантоспособности информационных систем образовательного процесса по происхождению и возможным последствиям существенно не отличаются от других распространенных типов информационных систем, кроме свойства функциональной безопасности.

Действительно, отказа технического оборудования в сочетании с длительным временем работы за компьютером, могут повысить риски негативного влияния на зрение человека, сердечно-сосудистую систему или психоэмоциональное состояние негативных факторов за счет повышенного уровня яркости изображения или его мерцание, неудовлетворительного внешнего освещения, малой контрастности или нарушение фокусировки, повышенный уровень ультрафиолетового или электромагнитного излучения и т. п. (Мельников, 2021).

Пути решения указанной проблемы выходят за рамки данной работы и требуют специфических медико-лабораторных исследований.

Модель нарушителя безопасности информационной системы дистанционного обучения определенным образом напоминает модель нарушителя в банковской сфере, когда сотрудник банка и преступно настроенное лицо потенциально могут образовывать альянс.

Ради объективности следует признать, что почти каждый из участников образовательного процесса может быть нарушителем академической добропорядочности. Потенциально в поведении должностных лиц вуза или ВО даже могут наблюдаться признаки коррупционных действий, обусловленные попыткой получить неправомерную выгоду за счет необъективной оценки качества усвоения ВО той или иной учебной дисциплины.

ВО, который не выполнил в полном объеме учебную программу, при поддержке сотрудников вуза может пытаться получить положительные оценки путем списывания во время выполнения контрольных мероприятий, академического плагиата в ходе выполнения курсовой или дипломной работы, подмены или незаконной модификации учетных документов, а также иных мошеннических действий.

Решение указанной сложной проблемы лежит в плоскости комплексного подхода к формированию добропорядочности в обществе В то же время анализ технологических составляющих образовательного процесса и опыт построения информационных систем, в которых обеспечивается целостность, конфиденциальность и доступность, а также наблюдаемость процессов позволяет предложить ряд встроенных в ГИС механизмов для противодействия негативным факторам, которые подрывают академическую добропорядочность.

Изучение аналитических обзоров современных программных платформ, предлагаемых для использования в системе дистанционного обучения (Дьяконова, 2012; Бондарев, 2021), позволяет сделать вывод, что вопросы обеспечения информационной безопасности и кибербезопасности в таких системах (платформах) или подробно не рассматриваются, либо не упоминаются вовсе.

Что касается функциональности многих систем, то она не полностью отвечает определенному отечественным законодательством ОП (Бондарев, 2021; Введение, 2018). Большинство программных систем, приведенных в указанных обзорах, ориентированы на профессиональное обучение персонала с целью повышения эффективности реализации бизнес-процессов в рамках выбранных компаниями направлений предпринимательской деятельности. Это свидетельствует об актуальности выбранного направления исследований.

На текущее время методология измерения достигнутого уровня гарантоспособности информационных систем окончательно пока еще не сформирована, поэтому возникает вопрос относительно инструментов и методики оценки соответствующего уровня для информационных систем дистанционного обучения.

Применения известных методов и моделей оценки эффективности обучения персонала в случаях использования различных информационных систем дистанционного обучения в вузе не представляется возможным в связи с узко специфической направленности указанных методов и моделей, в частности, ориентацией их на цели, задачи и конечные результаты корпоративного онлайн-обучения (Ищейнов, 2020). Поэтому вопрос измерения достигнутого уровня гарантоспособности информационных систем дистанционного обучения в вузе требует отдельного исследования.

Методологические основы построения тестовых заданий для контроля качества усвоения учебной дисциплины достаточно глубоко и всесторонне проработаны и изучаются в рамках соответствующих специализаций педагогического профиля (Клименко , 2021; Клековкина , 2014; Мельников, 2021). В то же время, следует отметить, что в приведенных источниках и многих аналогичных по направлению исследованиях вопрос конструирования тестов по уменьшению рисков для академической добропорядочности не рассматривается.

Несмотря на то, что технологической основой системы дистанционного обучения являются компьютерные сети, представляется целесообразным рассмотреть некоторые основные принципы построения тестовых заданий для программных средств (ПО).

Тесты служат для выявления ошибок в ПО, которые возникли на этапе их проектирования. В частности, согласно классической монографии Г. Майерса, тестирование ПО – это процесс выполнения программы с целью выявления ошибок. Там же с соответствующей аргументацией приведены основные принципы тестирования:

1. Описание предполагаемых результатов является частью теста.
2. Следует избегать тестирования ПО ее автором.
3. Необходимо детально изучать результаты тестирования.
4. Не следует выбрасывать отработанные тесты.
5. процесс тестирования в некотором смысле более творческий, чем процесс создания ПО.
6. Тест считается хорошим, если он имеет высокую вероятность обнаружения еще не выявленной ошибки.
7. Тест считается удачным, если он разрешений обнаружить еще не обнаруженную ошибку процесса создания по.
8. Тесты, основанные на требованиях к ПО, должны быть проанализированы на полноту, то есть определено множество требований, которые не были подвергнуты тестированию.

Отметим, что в целом указанные принципы перекликаются с базовыми подходами к формированию тестовых заданий для контроля знаний.

Следующим шагом формирования методологии построения тестовых заданий для защищенных ГИС дистанционного обучения является формирование адекватной модели обучения в рамках отдельной учебной дисциплине и определения места тестов в этой модели.

Каскадная модель-одна из распространенных моделей жизненного цикла по предусматривает, что сформированные системные требования являются основой для формирования требований к ПО, последние вместе с функциональными требованиями к по, выдвигаемыми его заказчиком, являются основанием для определения архитектуры по, которая является совокупностью базовых решений об организации по.

Архитектура ПО, в свою очередь, является основой для создания программного кода по (представления программы на языке компьютера), который подлежит тестированию с целью проверки его соответствия заданным требованиям и отсутствия ошибок проектирования.

Тестирование может происходить по методам «черного ящика», «белого ящика» или их комбинации (Остапенко, 2018). Заметим, что тестирование по методу "черного ящика «происходит в отличие от» белого ящика" в условиях отсутствия информации о логической структуре объекта тестирования и базируется только на анализе входных и выходных данных теста от этого объекта. Не трудно видеть, что по логике тестирование по методу «черного ящика» ситуация согласуется с условиями тестирования результатов обучения.

Результаты тестирования ПО в некоторых случаях могут потребовать корректировки системных требований, которые оговариваются аппаратной и программной платформами (операционной системой) компьютерной сети в части нужных ресурсов (память, быстродействие и т. п). Аналогичная ситуация и в случае тестирования результатов обучения, поскольку при определенных условиях может потребоваться уточнение рабочей программы НД (и/или ассоциированных с ней документов) и, возможно, ООП.

Исходя из определенных законом сущностей ОП, а также виртуальной среды ОП – защищенной гарантоспособной информационной системы дистанционного обучения (ЗГИС ДН) и с учетом соответствующих логических связей как прототипа модели процесса обучения в рамках отдельной учебной дисциплины (НР ОНД), предлагается выбрать каскадную модель ПО.

В предложенной модели НРОНД информационное наполнение виртуальной среды и ее использование осуществляются УОП в соответствии с ОПП и каждой конкретной рабочей программой учебной дисциплины (ВС).

## Заключение

В статье определены методологические основы построения ЗГИС дистанционного обучения в вузе, в частности:

- определены основные задачи ЗГИС в условиях обеспечения совместимости различных форм обучения (очная, заочная, дистанционная) соискателей высшего образования;
- сформировано на основании требований законодательства о высшем образовании онтологию сущностей образовательного процесса как основу построения ЗГИС, центральным элементом которой должна быть виртуальная учебная среда;
- проведен анализ составляющих гарантоспособности и предложена модель угроз для ЗГИС, включая определение факторов, влияющих на академическую добропорядочность участников образовательного процесса;
- предложены механизмы ЗГИС для противодействия негативным факторам, модель обучения в рамках отдельной учебной дисциплины и методику построения тестовых заданий ЗГИС, которая включает оценки рационального количества вопросов в тестовом задании, вероятности правильного ответа на один тестовый вопрос и случайное совпадение ответов для соискателей высшего образования с разными уровнями компетентности (высокий, достаточный, средний), а также рассчитан предел случайного совпадения результатов тестирования, превышение которой может свидетельствовать о нарушении требований академической добропорядочности. Применение указанной методики в составе ЗГИС может способствовать повышению уровня академической добропорядочности.

Дальнейшие исследования представляется целесообразным направить на разработку методов измерения достигнутого уровня гарантоспособности информационных систем дистанционного обучения в ЗВО, исследование эффективных методов защиты ЗГИС, включая принципы построения и защиты электронной зачетной книжки как механизма поддержания норм академической добропорядочности.

## Список литературы

1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учеб. пособие. М., 2021. 252 с.
2. Введение в информационную безопасность: учеб. пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев, В.М. Фомичев, А.П. Дураковский, Т.А. Кондратьева. М., 2018. 228 с.
3. Верещагина Е.А., Жукова Т.А. Edutainment как современная технология обучения иностранных студентов средствам выражения субъективной модальности в русской речи // МНКО. 2019. №5 (78), с. 10-13.
4. Дьяконова О.О. Понятие «Эдьютейнмент» в зарубежной и отечественной педагогике // Сибирский педагогический журнал. 2012. №6. С. 182-185.
5. Ищейнов В.Я. Информационная безопасность и защита информации. теория и практика: учеб. пособие. М., 2020. 272 с.

6. Клековкина А.А., Самигулова Р.З., Абдулкадыров А.С. Основы построения региональных инновационных систем в России // Региональные проблемы преобразования экономики. 2014. № 10. С. 115-122.
7. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления. М., 2021. 180 с.
8. Кобзева Н.А. Edutainment как современная технология обучения // Ярославский педагогический вестник. 2012. №4. С. 192-195.
9. Мельников В.П., Куприянов А.И. Информационная безопасность: учебник. М., 2021. 272 с.
10. Морозова О.Н. Информационные технологии как средство повышения качества обучения магистров // Инженерный вестник Дона, 2017. №2. ivdon.ru/ru/magazine/archive/N2y2017/4191.
11. Новиков В.К., Галушкин И.Б. Информационная безопасность и защита информации. Организационно-правовые основы. М., 2019. 312 с.
12. Остапенко А.Г, Паринов А.В., Калашников А.О. Социальные сети и деструктивный контент. М., 2018. 274 с.
13. По данным Statista.com, число отправляемых писем через электронную почту ежегодно вырастает, для примера: в 2018 году было отправлено 281 млрд писем. http://emailexpert.ru/novosti/v-2020-godu-kazhdyj-den-v-mire-budet-dostavlyatsya-306-milliardov-email-pisem
14. Что такое фишинговые атаки? https://www. trendmicro.com/ru_ru/what-is/phishing/phishing-attacks. html
15. Nalan Aksakal Theoretical View to the Approach of the Edutainment // Procedia - Social and Behavioral Sciences, Vol. 186, 2015, pp. 1232-1239.

**Methodological foundations for the construction of secure, dependable information systems for distance learning of higher educational institutions**

**Andrei A. Serov**
student
ITMO National Research University
Moscow, Russia
serov.serov.11@mail.ru
0000-0000-0000-0000

**Vasilisa A. Avdonina**
student
ITMO National Research University
Moscow, Russia
av.vasilisa.av@gmail.com
0000-0000-0000-0000

**Aleksandra A. Sviridova**
student
ITMO National Research University
Moscow, Russia
Sviridovaaa290420@ya.ru
0000-0000-0000-0000

**Anna I. Miroshnichenko**
student
ITMO National Research University
Moscow, Russia
Miroshai@ya.ru
0000-0000-0000-0000

**Ilia G. Karibov**
student
Kuban State Medical University
Krasnodar, Russia
Karinovilgeo@ya.ru
0000-0000-0000-0000

Received 12.04.2022
Accepted 17.05.2022
Published 20.06.2022

10.25726/a0841-1021-7964-i

**Abstract**

The issues of automation of business processes at the university, in particular, information technology support for distance higher education for the past 30 years have been the subject of many studies and heated discussions of scientific and pedagogical workers, as well as the object of special attention from society. At the same time, developments in recent years related to the spread of quarantine measures in connection with the COVID-19 pandemic indicate that during the first three months of quarantine, there was a limited readiness of educational institutions, in particular secondary education, to effectively conduct a full-fledged educational process. Successes in this direction at the university are insufficiently covered in scientific publications, but the author's own experience of teaching a number of academic disciplines at the university indicates that the achievements of victorious officials are somewhat exaggerated. It should be noted that the vast majority of problematic situations known to the author in educational institutions associated with the use of a large number of different software platforms focused on e-learning are primarily due to their incomplete compliance with the educational process, which is defined by laws, as well as insufficient attention on the part of developers regarding the requirements for information protection and cybersecurity.

**Keywords**

university, information security, cybersecurity, protection.

**References**

1. Bondarev V.V. Vvedenie v informacionnuju bezopasnost' avtomatizirovannyh sistem: ucheb. posobie. M., 2021. 252 s.
2. Vvedenie v informacionnuju bezopasnost': ucheb. posobie dlja vuzov / A.A. Maljuk, V.S. Gorbatov, V.I. Korolev, V.M. Fomichev, A.P. Durakovskij, T.A. Kondrat'eva. M., 2018. 228 s.
3. Vereshhagina E.A., Zhukova T.A. Edutainment kak sovremennaja tehnologija obuchenija inostrannyh studentov sredstvam vyrazhenija sub#ektivnoj modal'nosti v russkoj rechi // MNKO. 2019. №5 (78), s. 10-13.
4. D'jakonova O.O. Ponjatie «Jed'jutejnment» v zarubezhnoj i otechestvennoj pedagogike // Sibirskij pedagogicheskij zhurnal. 2012. №6. S. 182-185.
5. Ishhejnov V.Ja. Informacionnaja bezopasnost' i zashhita informacii. teorija i praktika: ucheb. posobie. M., 2020. 272 s.

6. Klekovkina A.A., Samigulova R.Z., Abdulkadyrov A.S. Osnovy postroenija regional'nyh innovacionnyh sistem v Rossii // Regional'nye problemy preobrazovanija jekonomiki. 2014. № 10. S. 115-122.
7. Klimenko I.S. Informacionnaja bezopasnost' i zashhita informacii: modeli i metody upravlenija. M., 2021. 180 s.
8. Kobzeva N.A. Edutainment kak sovremennaja tehnologija obuchenija // Jaroslavskij pedagogicheskij vestnik. 2012. №4. S. 192-195.
9. Mel'nikov V.P., Kuprijanov A.I. Informacionnaja bezopasnost': uchebnik. M., 2021. 272 s.
10. Morozova O.N. Informacionnye tehnologii kak sredstvo povyshenija kachestva obuchenija magistrov // Inzhenernyj vestnik Dona, 2017. №2. ivdon.ru/ru/magazine/archive/N2y2017/4191.
11. Novikov V.K., Galushkin I.B. Informacionnaja bezopasnost' i zashhita informacii. Organizacionno-pravovye osnovy. M., 2019. 312 s.
12. Ostapenko A.G, Parinov A.V., Kalashnikov A.O. Social'nye seti i destruktivnyj kontent. M., 2018. 274 s.
13. Po dannym Statista.com, chislo otpravljaemyh pisem cherez jelektronnuju pochtu ezhegodno vyrastaet, dlja primera: v 2018 godu bylo otpravleno 281 mlrd pisem. http://emailexpert.ru/novosti/v-2020-godu-kazhdyj-den-v-mire-budet-dostavlyatsya-306-milliardov-email-pisem
14. Chto takoe fishingovye ataki? https://www. trendmicro.com/ru_ru/what-is/phishing/phishing-attacks. html
15. Nalan Aksakal Theoretical View to the Approach of the Edutainment // Procedia - Social and Behavioral Sciences, Vol. 186, 2015, pp. 1232-1239.