

принимают иноязычную речь на слух. Причиной этого является недостаточное уделение внимания прослушиванию живой иностранной речи, либо прямое общение с носителями языка (что не всегда возможно). Ведь именно восприятие иноязычной речи является неотъемлемым условием знания иностранного языка. Межкультурная коммуникация очень важный аспект в изучении иностранных языков и требует особого внимания. Поэтому так важно уделять особое внимание аудированию, чтобы воспринимать и понимать речь носителей языка, которые говорят бегло, не имеют акцента, обладают правильным произношением, так как данный язык является для них родным. Ведь важным аспектом является не только знание грамматики, но и обычное общение в жизни и понимание иностранной речи в целом.

Подводя итоги, хочется сказать, что кабинеты с лингафонным оборудованием в средних и высших учебных заведениях необходимы. Это не только дает возможность студентам развиваться в иноязычном общении, воспринимать иноязычную речь на слух, но и облегчает преподавательскую деятельность.

На сегодняшний день многие российские высшие учебные заведения имеют связи с иностранными университетами, благодаря чему у студентов есть возможность пройти практику за границей. Это вновь указывает на то, что знания иностранного языка необходимы. Причем уровень этих знаний должен быть не только на уровне теории, но и возможности коммуникативного общения на различные бытовые и профессиональные темы.

Обучение — это специально организованный управляемый процесс взаимодействия учителей и учеников, направленный на усвоение знаний, умений, навыков, формирование мировоззрения, развитие умственных сил и потенциальных возможностей обучаемых, закрепление навыков самообразования в соответствии с поставленными целями. Именно от преподавателя зависит насколько будет успешным процесс обучения.

Автор придерживается различных методик преподавания, но настоятельно рекомендует применять методы с использованием лингафонного оборудования. Это позволит достичь высоких результатов.

Список литературы

1. Беседы об уроке иностранного языка : пособие для студентов педагогич. Институты/ Е.И. Пассов [и др.] – Л. : Просвещение, 1975. – 176 стр
2. www.cyberleninka.ru
3. www.dic.academic.ru толкование Лингафонный кабинет

Г.Р. Мустафина, А.Р. Абдуллина

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ ОБЩЕСТВЕ

ФГБОУ ВО БГМУ Минздрава России, г. Уфа

Кафедра дерматовенерологии

с курсами дерматовенерологии и косметологии ИДПО

Аннотация. Новая социальная парадигма — информационное общество — породило новый вид опасности — информационную, обеспечение информационной безопасности в современном российском обществе является основным условием выхода страны из системного кризиса.

Ключевые слова: информационная опасность, информационная война, угроза, кризис.

Введение. Средства массовой информации (СМИ) являются действенным каналом информирования общества о деятельности власти, а также информирования власти и общества о жизни общества и его реакции на действия власти. Развитие информационных технологий явилось условием, приводящим к масштабным ката-

строфам, военным конфликтам, разрушить государственное руководство, финансово-экономическую систему, службу научных центров.

Возникли информационные войны, разрушающие социогенетические механизмы развития обособленных обществ и цивилизаций, сформировавшихся систем ценностей, нравственности. Сознательно искажается информационная картина мира. Из-за ложной информации, смены настоящего ложным социум не способен своевременно дать ответ на разнообразные вызовы, которые угрожают его существованию, но и не в состоянии адекватно воспринимать и осмысливать данные вызовы и угрозы. Непосредственно, в связи с этим вышеуказанная проблема потребует открытия условий возникновения и способы их разрешения.

Цель. Раскрыть содержание понятия «информационная безопасность», обнаружить характерные черты информационного общества, отличительную особенность проявления в нем опасности нашему социуму. Получить обоснование важных принципов и подходов обеспечения информационной безопасности и варианты ее урегулирования в русском обществе.

Материалы и методы. Современное информационное общество является объектом исследования, объединив его объективные и субъективные стороны. Работы лучших представителей общегуманитарной идеи являются главной основой теории и методов, которые раскрывают сущность нашего общества, феноменов опасности/безопасности.

Результаты и обсуждения. Информационная безопасность государства — является главной основой защищенности информационных ресурсов страны и сохранности конституционных прав в информационной сфере общества и личности. основополагающие свойства информационной безопасности:

Информация — обмен данных, между людьми, передаваемый разными способами: письменно, устно, с помощью различных знаков и символов.

Конфиденциальность — состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;

Целостность — избежание несанкционированной модификации информации;

Доступность — избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Из вышеперечисленного следует, что масштаб вопроса обеспечения информационной безопасности на уровне личности, общества и государства, действительно, велик. Информационная опасность проявляется разными формами: создает виртуальный мир, подменяющий настоящее; манипулирует мировоззрением и поведением общества; меняет цели, ценности, создает особый стиль жизни и навязывает свои стандарты, искажает информацию и многое другое. Вышеперечисленные и прочие виды, которыми проявляется информационная угроза определены нуждаемостью личности в информации, возможностью (либо неспособностью) отличать подлинное от ложного, полезное и бесполезное. Субетто А. И. остро говорит в своих работах о введении рыночно-стихийной регуляции в информационные пространства не только единичных социумов, но и цивилизации в глобальных масштабах, который преобразует знания и информацию в товар. Все это дает процесс фабрикации ошибочной информации.

Отмечено, что Россия ставит перед собой цель воссоединить взаимосвязь внешних — системно организованных и динамичных граней жизни общества, и его внутренних «пластов», сохраняющие ценности культурной, общественной идентичности государства. Основной источник угрозы нашего государства — потеря связи «внутреннего» и «внешнего» становится основным источником. Отсюда вытекает, что единственный достоверный путь достижения информационной безопасности — сформировать внутреннее единство российского общества. Создается первостепенная

необходимость защитить наше общество от влияния информационных деструктивных воздействий (диверсий).

В доктрине информационной безопасности Российской Федерации отражены основные угрозы и задачи обеспечения информационной безопасности личности, общества и государства.

Основные угрозы информационной безопасности государства, отмеченные в доктрине информационной безопасности Российской Федерации, принятая президентом в 2000 году [4]. С момента принятия доктрины начались предприниматься активные действия по развитию данного направления.

- Угроза информационного обеспечения политики государства России
- Угроза развития информационной индустрии государства: телекоммуникация, связь, потребности внутреннего рынка, выход продукции на рынок, накопления, сохранения и эффективности ресурсов информации Российской Федерации
- Угроза сохранения безопасности информационных систем, которые уже развернулись на территории государства и новых создающихся. Доктрина предлагает эффективные методы предотвращения развития данных угроз. Однако, мало внимания уделено проблемам сохранения информационной безопасности общества и государства, которые направлены на подрывание строя Конституции Российской Федерации, угроза национальных, расовых, религиозных конфликтов. Обеспечение информационной безопасности общества и государства на современном этапе развития требует комплексного подхода, включая организационные и правовые меры.

Основные задачи государства в целях обеспечения безопасности:

- Усовершенствовать правовую базу информационной безопасности
- Защита прав граждан Российской Федерации в сфере обеспечения информационной безопасности
- Защита интересов общества и государства в сфере обеспечения информационной безопасности
- Просвещение социума, обучение основам защиты и самозащиты от главных угроз в сфере информации
- Принимать участие в разработке мер информационной безопасности на мировом, международном уровне

Основа создания информационной обеспечения безопасности Российской Федерации — восстановление субъектного качества отечественного общества путем консолидации сознательных и активных сторон общества, которые не утратили умение правильно производить оценку содержания и направленности потоков информации, «циркулирующих» в общественной концепции, проектируемые на основе образа новейшей общественной единности с последующим формированием на базе расширенного аутопойесиса с применением элемента гражданского общества.

Выводы и дальнейшие перспективы. Безусловно, изучение различных нюансов и «пластов» вопроса информационной безопасности/опасности не завершен до конца. На сегодняшний день выделены только главные основополагающие моменты и сделаны первые шаги на пути решения данной актуальной проблемы, однако ее последующая общественная и теоретическая значимость не поддается сомнению. Один из значимых выводов, полученных во время изучения вышеизложенной проблемы — осознание необходимости разрешения этой темы на общефилософском уровне.

Данное содействует распространению междисциплинарного изучения этой проблемы, привлекает мировоззренческие основы и категорий, необходимые для познания темы информационной опасности/безопасности в теории общественного управления, теории коммуникации, культурологии, социологии, экономике, истории, прочих науках.

На сегодняшний день наше отечественное общество оказалось перед выбором пути развития своего светлого будущего, однако встречается с трудностями выявления ее идентичности, значимость в современном мире. Выявление плюсов и минусов информационного общества для России является о жизненной и актуально значимой темой. Из вышеперечисленного следует, что необходимо углубить изучение данного вопроса, усовершенствовать систему под изменяющиеся условия развития современного общества.

Список литературы

1. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности – Системы управления информационной безопасностью. Требования. – 2005. – 36 с.
2. ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management [Электронный ресурс]// Интернет-портал – URL: http://www.iso.org/iso/catalogue_detail?csnumber=56742 (Дата обращения: 18.09.2017)
3. Базовая информация о информационной безопасности [Электронный ресурс]// Интернет-портал – URL: <http://bezopasnik.org/article/1.htm> (Дата обращения: 18.09.2017)
4. Доктрина информационной безопасности Российской Федерации/ Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646 Интернет-портал – URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>

Ф.Ф. Мусыргалина, М.М. Туйгунов, Г.А. Идиатуллина, Л.В. Мурзагалина
**ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ ВНЕАУДИТОРНОЙ РАБОТЫ
ОБУЧАЮЩИХСЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ СТОМАТОЛОГИЯ
НА КАФЕДРЕ МИКРОБИОЛОГИИ, ВИРУСОЛОГИИ БАШКИРСКОГО
ГОСУДАРСТВЕННОГО МЕДИЦИНСКОГО УНИВЕРСИТЕТА**
ФГБОУ ВО БГМУ Минздрава России, г. Уфа
Кафедра микробиологии, вирусологии
Кафедра педагогики и психологии

Аннотация. Освещены вопросы организации самостоятельной внеаудиторной работы обучающихся стоматологического факультета на кафедре микробиологии, вирусологии ФГБОУ ВО БГМУ Минздрава России. Определены этапы организации и проведения внеаудиторной самостоятельной работы обучающихся, а также условия, которые должны быть выполнены для эффективности самостоятельной внеаудиторной работы обучающихся.

Ключевые слова: самостоятельная внеаудиторная работа обучающихся, микробиология, вирусология, педагогика, психология.

Основным документом, определяющим содержание и совокупность требований к реализации учебной программы специальности высшего образования, является Федеральный государственный образовательный стандарт. В ФГОС последнего поколения акцент делается на характеристике профессиональной деятельности выпускников и основных требованиях по освоению программ высшего образования, которые предъявляются к обучающемуся. Разнообразие самостоятельной работы обучающихся, подбор эффективных методов требует от педагога высшей школы дополнительных усилий, увеличивает трудозатратность на подготовку таких заданий, способствует усилению ответственности педагогов при подготовке заданий для самостоятельной работы. В свою очередь, обучающийся реализует индивидуальную стратегию развития, получает дополнительную стимуляцию к личностному и профессиональному росту, проявляет инициативу и творческую активность.