федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический университет имени М.Е. Евсевьева»

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Защита информации в компьютерных сетях
Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Профиль подготовки: Информатика. Математика
Форма обучения: Очная

Разработчики:
Зубрилин А. А., канд. филос. наук, зав. кафедрой
Лапин К. С., канд. физ.-мат. наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 10 от 19.05.2016 года

Зав. кафедрой _____Вознесенская Н. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 15 от 21.06.2018 года

Зав. кафедрой _____Вознесенская Н. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 31.08.2020 года

Зав. кафедрой _____Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - формирование педагога, способного организовывать безопасную работу на персональном компьютере и в компьютерной сети, умеющего противостоять информационным угрозам, включая технические, технологические, психологические, социальные; способного использовать естественнонаучные и математические знания для реализации образовательных программ по информатике и использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

Задачи дисциплины:

- формирование знаний в области российского правового регулирования информационной безопасности для реализации образовательных программ по информатике;
- выработка представлений о способах обеспечения защиты компьютера и противостоянии методам социальной инженерии с использованием естественнонаучных и математических знаний для ориентирования в современном образовательном пространстве;
- освоение программных средств обеспечения информационной безопасности при работе на персональном компьютере и в компьютерной сети, включая формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения с использованием возможностей образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса;
- обучение основам криптографии, как одного из важных средств шифрования данных для реализации образовательных программ по информатике.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.03.01 «Защита информации в компьютерных сетях» относится к вариативной части учебного плана.

Дисциплина изучается на 3 курсе, в 6 семестре.

Для изучения дисциплины требуется: знание возможностей сервисов сети Интернет

Изучению дисциплины «Защита информации в компьютерных сетях» предшествует освоение дисциплин (практик):

Теоретические основы информатики.

Освоение дисциплины «Защита информации в компьютерных сетях» является необходимой основой для последующего изучения дисциплин (практик):

Методика обучения информатике;

Компьютерные сети;

Интернет-технологии.

Область профессиональной деятельности, на которую ориентирует дисциплина «Защита информации в компьютерных сетях», включает: образование, социальную сферу, культуру.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;
- развитие.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций и трудовых функций (профессиональный стандарт Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими общекультурными компетенциями (ОК):

ОК-3. способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

ОК-3. способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	знать: - математические методы шифрования информации для формирования способности использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве; - естественнонаучные и математические факты, в том числе способы защиты информации для ориентирования в современном информационном пространстве; уметь: - защищать информацию от несанкционированного пользования для безопасного ориентирования в современном информационном пространстве; владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях для ориентирования в современном информационном пространстве с помощью естественнонаучных и математических знаний

ПК-1. готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

педагогическая деятельность

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	знать: - понятия, связанные с научной областью «Информационная безопасность» с целью реализации образовательных программ по информатике; - возможные технические, технологические, социальные угрозы, связанные с компьютерной техникой с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - меры соблюдения информационной безопасности при работе на компьютере в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - виды информационных угроз, возникающих при работе в компьютерных сетях с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - программные средства и сервисы Интернет для обеспечения информационной безопасности с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - способы шифрования данных для реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - правовые и законодательные акты в области обеспечения информационной безопасности для реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; уметь: - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере;

	владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов.
ПК-4. способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов	
педагогическая деятельность	
ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов	знать: - технические, технологические, социальные угрозы, возникающие при работе в информационной образовательной среде; - способы шифрования данных с целью формирования способности использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения информатике; уметь: - обнаруживать вредоносное программное обеспечение на компьютере и выявлять сетевые атаки при использовании возможностей образовательной среды; - устранять последствия воздействия на компьютер вредоносного программного при использовании возможностей образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса; - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности компьютера в процессе достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса; - применять программы для шифрования конфиденциальной информации при использовании возможностей образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов; владеть: - средствами обеспечения информационной безопасности при работе в информационно-образовательной среде для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Шестой семестр
Контактная работа (всего)	**36**	**36**
Лекции	18	18
Практические	18	18
Самостоятельная работа (всего)	**36**	**36**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Проблемы информационной безопасности в современном обществе:

Общие вопросы информационной безопасности. Международные стандарты информационного обмена. Понятие информационной угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Закон об информации. Судебные прецеденты и ответственность за нарушение закона. Концепция информационной безопасности РФ. Информационная безопасность личности, общества, государства. Теория информационной безопасности и ее основные направления. Ведущие положения теории информационной безопасности в области информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Виды возможных нарушений информационной безопасности. Несформированность информационной культуры пользователей. Хакерские атаки. DoS- и DDoS-атаки. Сетевой шпионаж (сниффинг, нюкеры). Эксплойты.

Причины возникновения информационных угроз. Анализ способов нарушения информационной безопасности. Использование защищенных компьютерных систем. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Информационные ресурсы по информационной безопасности. Правовые вопросы, связанные с информационной безопасностью. Нормативные руководящие документы, касающиеся государственной тайны. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности.

DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому компьютеру. Комплексная защита сетевого компьютера от информационных угроз. Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Программные средства компьютера по обнаружению вторжения и защите от него.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях:

Понятие о видах вирусов. Антивирусная защита компьютера. Классификация компьютерных вирусов. Классические компьютерные вирусы. Файловые вирусы. Макровирусы. Троянские кони. Руткиты. Сетевые черви. Программные средства для обеспечения антивирусной защиты компьютера. Технологии построения защищенных информационных систем. Место информационной безопасности экономических систем в национальной безопасности страны. Риски и ценность информации. Криптография как наука. Методы криптографии. Алгоритмы и стандарты шифрования. Симметричное и асимметричное шифрование. Электронная цифровая подпись. Современные технологии аутентификации. Вопросы организации информационной безопасности при работе с информационными ресурсами и сервисами сети Интернет. Методы психологического воздействия на пользователя сети Интернет. Социальная инженерия. Антивирусные программные средства офисного и домашнего назначения для обеспечения информационной безопасности. Парольная защита. Программы шифрования данныхСоциальная инженерия и ее методы. Электронная валютаСоциальные сети как информационная угроза. Дети и Интернет. Политика информационной безопасности и ее организация в локальной сети

5.2. Содержание дисциплины: Лекции (18 ч.)

Модуль 1. Проблемы информационной безопасности в современном обществе (10 ч.)

Тема 1. Общие вопросы информационной безопасности (2 ч.)

Информационная безопасность как научная область. Направления обеспечения информационной безопасности в современных условиях.

Тема 2. Теория информационной безопасности и ее основные направления (2 ч.)

Теоретические вопросы организации информационной безопасности. Пути организации информационной безопасности на предприятии.

Тема 3. Виды возможных нарушений информационной безопасности (2 ч.)

Информационная угроза. Уровни нарушения информационной безопасности: аппаратный, программный, человеческий фактор.

Тема 4. Причины возникновения информационных угроз и меры защиты от них (2 ч.)

Информационная угроза. Виды информационных угроз. Способы защиты от информационных угроз.

Тема 5. Назначение и задачи обеспечения информационной безопасности на уровне государства (2 ч.)

Государственная защита информации. Законы, регулирующие обеспечение информационной безопасности на уровне государства. Ответственность за нарушение законов.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях (8 ч.)

Тема 6. Понятие о видах вирусов. Антивирусная защита компьютера (2 ч.)

Компьютерные вирус: определение, природа возникновения. Способы попадания вирусов в компьютерную систему. Классификация вирусов. Способы защиты от вирусов

Тема 7. Технология построения защищенных информационных систем (2 ч.)

Технология определения путей организации защиты информационной системы.

Отбор программных средств для организации защиты. Аутентификации пользователей. Распределение прав в информационной системе.

Тема 8. Криптография как наука (2 ч.)

Криптография и ее место в обеспечении информационной безопасности предприятия. Способы шифрования данных. Программы для шифровки и расшифровки данных.

Тема 9. Программные средства компьютера по обнаружению несанкционированного вторжения и защите от вторжения (2 ч.)

Проактивные системы защиты компьютера. Системы контроля целостности данных. Борьба с потенциально опасными программами.

5.3. Содержание дисциплины: Практические (18 ч.)

Модуль 1. Проблемы информационной безопасности в современном обществе (10 ч.)

Тема 1. Информационные ресурсы по информационной безопасности (2 ч.)

Общие вопросы информационной безопасности. Информационные ресурсы по информационной безопасности.

Тема 2. Правовые вопросы, связанные с информационной безопасностью (2 ч.)

Правовое регулирование в области информационной безопасности.

Законы о преступлениях в сфере информационных технологий.

Авторское право. Пути доказательства авторства.

Тема 3. Правовые вопросы, связанные с информационной безопасностью (2 ч.)

Интеллектуальная собственность. Способы защиты интеллектуальной собственности. Лицензионное программное обеспечение. Компьютерное пиратство и законодательная ответственность за него.

Тема 4. Нормативные документы, касающиеся государственной тайны (2 ч.)

Государственная тайна. Ответственность за разглашение государственной тайны. Состояние законодательства РФ в области сохранения государственной тайны.

Примеры нарушения государственной тайны.

Тема 5. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности (2 ч.)

Несанкционированный доступ к аппаратным средствам компьютера и средства ограничения доступа.
Взлом экранной заставки Windows и пароля BIOS. Способы предотвращения взлома.

Взлом операционной системы посредством носителей информации. Способы защиты. Ограничение доступа к USB-накопителям.

Разграничение доступа в локальных сетях. Взлом учетных записей пользователей локальной сети. Способы предотвращения взлома.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях (8 ч.)

Тема 6. Парольная защита (2 ч.)

Пароль как средство ограничения доступа к ресурсу. Требования к выбору пароля. Хранители паролей.

Программы восстановления (взлома) паролей. Брутфорс

Тема 7. Социальная инженерия и ее методы (2 ч.)

Обзор методов социальной инженерии.

Методы и методики психологического воздействия на личность (универсальный сеанс связи, сообщение о проверке почты, сообщение от имени администратора, квитанция о доставке, обличение и др.).

Антропогенные инструменты защиты от методов социальной инженерии (привлечение к вопросам безопасности, изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения).

Обратная социальная инженерия.

Тема 8. Социальная инженерия и ее методы (2 ч.)

Фарминг как инструмент скрытого перенаправления на поддельные сайты. Фишинг и вишинг как инструмент получения конфиденциальной информации. Мошенничество в Интернете.
Правила поведения пользователей в сети Интернет при работе с информационными ресурсами.

Тема 9. Программы шифрования данных (2 ч.)

Шифрование данных и его назначение. Алгоритмы и стандарты шифрования. Архивирование файлов с паролем как инструмент защиты от несанкционированного доступа. Криптография и ее методы шифрования информации. Восстановление данных. Грамотное удаление информации с компьютера. Специализированные программные средства по удалению.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1 Вопросы и задания для самостоятельной работы

Шестой семестр (36 ч.)

Модуль 1. Проблемы информационной безопасности в современном обществе (18 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Подготовка ситуационных задач по информационной безопасности на основании статей соответствующих законов и нормативных актов РФ. Возможные разделы:

Раздел «АВТОРСКОЕ ПРАВО»

ГК РФ ч. IV:

Статья 1255. Авторские права

Статья 1256. Действие исключительного права на произведения науки, литературы и искусства на территории Российской Федерации

Статья 1265. Право авторства и право автора на имя

Статья 1266. Право на неприкосновенность произведения и защита произведения от искажений

Статья 1267. Охрана авторства, имени автора и неприкосновенности произведения после

смерти автора

Статья 1270. Исключительное право на произведение

Статья 1274. Свободное использование произведения в информационных, научных, учебных или культурных целях

Статья 1286. Лицензионный договор о предоставлении права использования произведения

Статья 1286.1. Открытая лицензия на использование произведения науки, литературы или искусства

Статья 1290. Ответственность по договорам, заключаемым автором произведения

Статья 1295. Служебное произведение

Статья 1296. Произведения, созданные по заказу

Статья 1297. Произведения, созданные при выполнении работ по договору

Статья 1299. Технические средства защиты авторских прав

Статья 1301. Ответственность за нарушение исключительного права на произведение

Статья 1302. Обеспечение иска по делам о нарушении авторских прав

УК РФ:

Статья 146. Нарушение авторских и смежных прав

Статья 147. Нарушение изобретательских и патентных прав

КоАП РФ:

Статья 7.12. Нарушение авторских и смежных прав, изобретательских и патентных прав

ФЗ РФ «Об авторском праве и смежных правах»:

Статья 17. Право доступа к произведениям изобразительного искусства. Право следования

Статья 26. Воспроизведение произведения в личных целях без согласия автора с выплатой авторского вознаграждения

Статья 39. Использование фонограммы, опубликованной в коммерческих целях, без согласия производителя фонограммы и исполнителя

Статья 48. Нарушение авторских и смежных прав. Контрафактные экземпляры произведения и фонограммы

Статья 49. Гражданско-правовые способы защиты авторского права и смежных прав

Раздел «ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ»

ГК РФ:

Статья 1246. Государственное регулирование отношений в сфере интеллектуальной собственности

УК РФ

Статья 159.6. Мошенничество в сфере компьютерной информации

Раздел «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

УК РФ

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Раздел «ПРЕСТУПЛЕНИЯ ПРОТИВ ГОСУДАРСТВЕННОЙ ВЛАСТИ»

Закон РФ «О государственной тайне»

Статья 5. Перечень сведений, составляющих государственную тайну

Статья 16. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями

Статья 19. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений

Статья 21. Допуск должностных лиц и граждан к государственной тайне

Статья 21.1. Особый порядок допуска к государственной тайне

Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне

Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

УК РФ:

Статья 283. Разглашение государственной тайны

Статья 275. Государственная измена

Статья 276. Шпионаж

КоАП РФ:

Статья 7.31. Нарушение порядка ведения реестра контрактов, заключенных заказчиками, реестра контрактов, содержащего сведения, составляющие государственную тайну, реестра недобросовестных поставщиков (подрядчиков, исполнителей)

Алгоритм разработки задачи:

1. Выбрать и изучить статью из нормативного акта.

2. Проанализировать материалы сайтов, например, http://itsec.ru, на предмет наказания за нарушения в сфере информационной безопасности.

3. Разработать ситуационную задачу и привести ее решение с указанием нормативных актов, на которые осуществлялась опора.

Пример задачи:

Гражданин Иванов создал антивирусное программное средство под названием «EFVIv» и зарегистрировал на него свои права. 20.09.2017 этот гражданин заключил договор с компанией «Saransk-IT» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «Saransk-IT» перепродала для распространения версию программы «EFVIv» другой компании без ведома автора.

Имеет ли место в данной ситуации нарушение авторского права гражданина Иванова?

Решение.

Согласно Статьи 1270 ГК РФ:

Автору произведения или иному правообладателю принадлежит исключительное право использовать произведение в соответствии со статьей 1229 настоящего Кодекса в любой форме и любым не противоречащим закону способом (исключительное право на произведение), в том числе способами, указанными в пункте 2 настоящей статьи. Правообладатель может распоряжаться исключительным правом на произведение.

2. Использованием произведения независимо от того, совершаются ли соответствующие действия в целях **и**звлечения прибыли или без такой цели, считается, в частности:

2) распространение произведения путем продажи или иного отчуждения его оригинала или экземпляров;

Таким образом, в данном случае имеет место нарушение авторского права гражданина Иванова.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях (18 ч.)

Вид СРС: *Выполнение индивидуальных заданий

СХЕМА ОФОРМЛЕНИЯ ОПИСАНИЯ ПРИЛОЖНЕНИЯ
ДЛЯ ОРГАНИЗАЦИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОМПЬЮТЕРЕ

Общие сведения (20 баллов)

Название приложения:

Производитель:

Сайт производителя:

Необходимость инсталляции (да/нет)

Требования к операционной системе и аппаратным ресурсам ПК:

Обновление (ручное/автоматическое)

Тип приложения (бесплатное, условно-бесплатное, лицензионное)

Функциональные возможности:

Описание приложения (35 баллов)

Скриншот приложения

Описание пунктов меню приложения
Настройка приложения (45 баллов)
Описание настройки приложения на работу
Описание этапов работы с приложением по обеспечению информацион-ной безопасности на компьютере
Список приложений для рассмотрения
Межсетевые экраны (со встроенным и без встроенного антивируса)
AVG Internet Security
ViPNet Personal Firewall
BitDefender Total Security
Norton Internet Security
F-Secure Internet Security
Antiy GhostBusters
eScan Internet Security Suite
Agnitum Outpost Firewall Pro
Jetico Personal Firewall
Core Force
Privatefirewall
PC Tools Firewall Plus
Программы проактивной защиты и защиты от шпионских программ
WinPatrol
Ad-Aware
SUPERAntiSpyware
Spyware Doctor
AVZ
Windows Defender
Spybot - Search & Destroy
Spyware Terminator
HijackThis
Spy Sweeper
SpywareBlaster
Системы обнаружения вторжения
Anti-keylogger
Protector Plus

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ОК-3	3 курс, Шестой семестр	Зачет	Модуль 1: Проблемы информационной безопасности в современном обществе.
ПК-1 ПК-4	3 курс, Шестой семестр	Зачет	Модуль 2: Практические вопросы организации информационной безопасности в компьютерных сетях.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:
Компетенция ПК-1 формируется в процессе изучения дисциплин:
3D моделирование, Алгебра, Вводный курс математики, Внеурочная деятельность учащихся по информатике, Геометрия, Задачи с параметрами и методы их решения, Интернет-

технологии, Информационная безопасность в образовании, Информационные системы, Искусственный интеллект и экспертные системы, Исследовательская и проектная деятельность на уроках математики, Исследовательская и проектная деятельность учащихся по информатике, Исторический подход в обучении математике, Компетентностный подход в обучении математике, Компьютерная алгебра, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Математический анализ, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения математике в профильных классах, Методология обучения математике, Методы аксиоматического построения алгебраических систем, Методы решения задач ГИА по математике, Методы решения задач по информатике, Моделирование в системах динамической математики, Нестандартные методы решения математических задач, Общая теория линейных операторов и ее приложение к решению геометрических задач, Оптимизация и продвижение сайтов, Основные направления развития топологии, Практикум по информационным технологиям, Применение систем динамической математики в образовании, Программирование, Проектирование в системах автоматизированного проектирования, Проектирование информационно-образовательной среды, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Реализация прикладной направленности в обучении математике, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение задач профильного уровня ЕГЭ по математике, Решение олимпиадных задач по информатике, Свободные инструментальные системы, Системы компьютерной математики, Современные проблемы геометрии, Современные средства оценивания результатов обучения, Современные технологии в обучении математике, Теоретические основы информатики, Теория рядов и ее приложения, Технология обучения математическим понятиям в школе, Технология обучения учащихся решению математических задач, Технология разработки элективных курсов по математике, Физика, Формы и методы работы с одаренными детьми, Численные методы, Элементарная математика, Элементы конструктивной геометрии в школьном курсе математики, Элементы функционального анализа.

Компетенция ПК-4 формируется в процессе изучения дисциплин: 3D моделирование, Интернет-технологии, Информационная безопасность в образовании, Информационные системы, Исследовательская и проектная деятельность на уроках математики, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения математике в профильных классах, Методика подготовки учащихся к ГИА по информатике, Методы решения задач по информатике, Моделирование в системах динамической математики, Оптимизация и продвижение сайтов, Практикум по информационным технологиям, Применение систем динамической математики в образовании, Программирование, Проектирование в системах автоматизированного проектирования, Проектирование информационно-образовательной среды, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Реализация прикладной направленности в обучении математике, Решение олимпиадных задач по информатике, Свободные инструментальные системы, Системы компьютерной математики, Теоретические основы информатики, Технология разработки и методика проведения элективных курсов по информатике, Технология разработки элективных курсов по математике, Физика, Формы и методы работы с одаренными детьми, Численные методы.

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач.

Базовый уровень:

знает и понимает теоретическое содержание; в достаточной степени сформированы умения применять на практике и переносить из одной научной области в другую теоретические знания;

умения и навыки демонстрируются в учебной и практической деятельности; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.

Пороговый уровень:

понимает теоретическое содержание; имеет представление о проблемах, процессах, явлениях; знаком с терминологией, сущностью, характеристиками изучаемых явлений; демонстрирует практические умения применения знаний в конкретных ситуациях профессиональной деятельности.

Уровень ниже порогового:

имеются пробелы в знаниях основного учебно-программного материала, студент допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не способен продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%
Пороговый	зачтено	60 – 75%
Ниже порогового	незачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Зачтено	Владеет навыками организации информационной безопасности на компьютере
Незачтено	Не владеет навыками организации информационной безопасности на компьютере

8.3. Вопросы, задания текущего контроля

Модуль 1: Проблемы информационной безопасности в современном обществе

ОК-3 способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

1. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.

2. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.

3. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности на предприятии.

4. Описать процедуру установки на компьютер антивирусного программного средства (из списка)

5. Расскажите о программных средствах, используемых для организации информационной безопасности при работе в компьютерной сети.

Модуль 2: Практические вопросы организации информационной безопасности в компьютерных сетях

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности на предприятии. Охарактеризуйте виды угроз, приведите примеры.

2. Раскройте суть нормативно-правового аспекта защиты информации на предприятии.

3. Раскройте административные вопросы, регламентирующие деятельность предприятия по организации информационной безопасности.

4. Охарактеризуйте организационные меры защиты информации на предприятии. Обоснуйте основные мероприятия по обеспечению информационной безопасности.

5. Раскройте понятие «сетевой атаки». Приведите примеры сетевых атак на корпоративную сеть. Укажите пути противодействия сетевым атакам.

ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов

1. Охарактеризуйте технологические меры информационной безопасности на предприятии. Обоснуйте классификацию средств технологической защиты информации.

2. Опишите технологию функционирования брандмауэров. Раскройте технологию настройки брандмауэра на примере конкретного приложения.

3. Расскажите о проактивных системах защиты компьютера. Приведите примеры программ данного класса.

4. Приведите способы несанкционированного проникновения на сетевой компьютер предприятия и расскажите о путях противодействия проникновению.

5. Раскройте суть нормативно-правового аспекта защиты информации на предприятии.

8.4. Вопросы промежуточной аттестации

Шестой семестр (Зачет, ОК-3, ПК-1, ПК-4)

1. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.

2. Охарактеризуйте структуру законодательства РФ в области защиты информации.

3. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности в России. Охарактеризуйте материалы, представленные в этих документах.

4. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне.

5. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.

6. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.

7. Перечислите нормативно-правовые акты, регламентирующие обращение с персональными данными. Приведите примеры внутренних нормативных актов на предприятии о персональных данных.

8. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности на предприятии.

9. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности на предприятии.

10. Расскажите о программных средствах, используемых для организации информационной безопасности при работе на компьютере.

11. Расскажите о программных средствах, используемых для организации информационной безопасности при работе в компьютерной сети.

12. Охарактеризуйте аппаратные средства защиты информации. Дайте их классификации. Приведите примеры аппаратных средств защиты информации в компьютерной сети предприятия.

13. Раскройте основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на компьютере для сотрудников предприятия.

14. Раскройте основные направления организации информационной безопасности в компьютерной сети предприятия. Сформулируйте рекомендации для организации информационной безопасности при работе на сетевом компьютере для сотрудников предприятия.

15. Приведите способы несанкционированного проникновения на сетевой компьютер редприятия и расскажите о путях противодействия проникновению.

16. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения нформационной безопасности на предприятии. Охарактеризуйте виды угроз, приведите примеры.

17. Раскройте суть нормативно-правового аспекта защиты информации на предприятии.

18. Раскройте административные вопросы, регламентирующие деятельность предприятия

о организации информационной безопасности.

19. Раскройте правовые вопросы, регламентирующие деятельность предприятия по рганизации информационной безопасности.

20. Охарактеризуйте организационные меры защиты информации на предприятии. Обоснуйте основные мероприятия по обеспечению информационной безопасности.

21. Охарактеризуйте технологические меры информационной безопасности на редприятии. Обоснуйте классификацию средств технологической защиты информации.

22. Опишите технологию функционирования брандмауэров. Раскройте технологию астройки брандмауэра на примере конкретного приложения.

23. Расскажите о проактивных системах защиты компьютера. Приведите примеры рограмм данного класса.

24. Раскройте понятие «сетевой атаки». Приведите примеры сетевых атак на орпоративную сеть. Укажите пути противодействия сетевым атакам.

25. Расскажите о системах отражения сетевых атак. Опишите их виды, принципы ункционирования.

26. Опишите принципы организации DoS- и DoSS-атак. Расскажите о способах борьбы с анным видом информационной угрозы.

27. Опишите принципы организации DoS- и DoSS-атак. Расскажите об облачных ехнологиях как способе борьбы с данным видом информационной угрозы.

8.5. Методические материалы, определяющие процедуры оценивания знаний, умений, авыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация проводится в форме зачета.

Зачет позволяет оценить сформированность компетенций, теоретическую подготовку гудента, его способность к творческому мышлению, готовность к практической деятельности, риобретенные навыки самостоятельной работы, умение синтезировать полученные знания и рименять их при решении практических задач.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом абранной суммы баллов.

Собеседование (устный ответ) на зачете

Для оценки сформированности компетенции посредством собеседования (устного ответа) гуденту предварительно предлагается перечень вопросов или комплексных заданий, редполагающих умение ориентироваться в проблеме, знание теоретического материала, умения рименять его в практической профессиональной деятельности, владение навыками и приемами ыполнения практических заданий. При оценке достижений студентов необходимо обращать собое внимание на:– усвоение программного материала;– умение излагать программный атериал научным языком;– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

– владение навыками поиска, систематизации необходимых источников литературы по зучаемой проблеме;

умение обосновывать принятые решения;– владение навыками и приемами выполнения рактических заданий;

– умение подкреплять ответ иллюстративным материалом.

Контекстная учебная задача, проблемная ситуация, ситуационная задача, кейсовое задание. При определении уровня достижений студентов при решении учебных практических задач еобходимо обращать особое внимание на следующее:

– способность определять и принимать цели учебной задачи, самостоятельно и творчески ланировать ее решение как в типичной, так и в нестандартной ситуации;

– систематизированные, глубокие и полные знания по всем разделам программы;

– точное использование научной терминологии, стилистически грамотное, логически равильное изложение ответа на вопросы и задания;

– владение инструментарием учебной дисциплины, умение его эффективно использовать в остановке и решении учебных задач;

– грамотное использование основной и дополнительной литературы;

– умение использовать современные информационные технологии для решения учебных

адач, использовать научные достижения других дисциплин;

– творческая самостоятельная работа на практических, лабораторных занятиях, активное частие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Тестирование

При определении уровня достижений студентов с помощью тестового контроля ответ читается правильным, если:

– в тестовом задании закрытой формы с выбором ответа выбран правильный ответ;

– по вопросам, предусматривающим множественный выбор правильных ответов, ыбраны все или некоторые правильные ответы;

– в тестовом задании открытой формы дан правильный ответ;

– в тестовом задании на установление правильной последовательности установлена равильная последовательность;

– в тестовом задании на установление соответствия сопоставление произведено верно для сех пар.

При оценивании учитывается вес вопроса (максимальное количество баллов за правильный твет устанавливается преподавателем в зависимости от сложности вопроса). Количество баллов а тест устанавливается посредством определения процентного соотношения набранного оличества баллов к максимальному количеству баллов.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.

Индивидуальные результаты освоения дисциплины студентами фиксируются в электронной информационно-образовательной среде университета.

12.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

1. Microsoft Windows 7 Pro
2. Microsoft Office Professional Plus 2010
3. 1С: Университет ПРОФ

12.2 Перечень информационно-справочных систем
(обновление выполняется еженедельно)

1. Гарант Эксперт (сетевая)
2. Справочная правовая система «КонсультантПлюс»

12.3 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/opendata/)
2. Профессиональная база данных «Портал открытых данных Министерства культуры Российской Федерации» (http://opendata.mkrf.ru/)
3. Электронная библиотечная система Znanium.com(http://znanium.com/)
4. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)

13. Материально-техническое обеспечение дисциплины(модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

Индивидуальные результаты освоения дисциплины фиксируются в электронной

информационно-образовательной среде университета.

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Оснащение аудиторий

Лаборатория вычислительной техники.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, коврик), проектор, экран, интерактивная доска, магнитно-маркерная доска, колонки SVEN, наушники.

Учебно-наглядные пособия:

Презентации.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 13 шт.).

Учебно-наглядные пособия:

Презентации.

Помещения для самостоятельной работы.

Лаборатория вычислительной техники.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт.).

Учебно-наглядные пособия:

Презентации.

Читальный зал.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети .«Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

Учебники и учебно-методические пособия, периодические издания, справочная литература.

Стенды с тематическими выставками..