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

Факультет физической культуры

Кафедра теории и методики физической культуры
и безопасности жизнедеятельности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность

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

Профиль подготовки: Физическая культура. Безопасность жизнедеятельности

Форма обучения: Очная

Разработчики:
Мамаев А. Р., канд. пед. наук, старший преподаватель

Программа рассмотрена и утверждена на заседании кафедры, протокол № 10 от 19.04.2019 года

Зав. кафедрой  Якимова Е. А.

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

Зав. кафедрой  Якимова Е. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – заложить терминологический фундамент, научить правильно, проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности, способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Задачи дисциплины:

– изучение основных направлений организации информационной безопасности (правового, технического, аппаратного);

– изучение основ правового регулирования информационной безопасности в России;

– формирование знаний о технических способах и средствах обеспечения защиты информации;

– изучение программных средств обеспечения информационной безопасности при работе на ПК и в сети Интернет;

– формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения по защите данных на ПК;

– формирование умений по организации защиты файлов и отдельных данных в документах Microsoft;

– формирование умений разрабатывать и реализовывать политику информационной безопасности на предприятии, в частности в образовательном учреждении;

- особенности поиска, анализа и синтеза информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.22 «Информационная безопасность» изучается на 1 курсе, в 1 семестре.

Для изучения дисциплины требуется: для освоения дисциплины студенты используют знания, умения, навыки, сформированные при изучении дисциплин общепрофессиональной и профессиональной подготовки.

Область профессиональной деятельности, на которую ориентирует дисциплина «Информационная безопасность», включает: образование, социальную сферу, культуру.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

– обучение;

– воспитание;

– развитие;

– просвещение;

– образовательные системы.

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 дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты № 544н от 18.10.2013).

Выпускник должен обладать следующими общекультурными компетенциями (ОК):

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
УК-1.1 Демонстрирует знание особенностей системного и критического мышления и готовность к нему.	**знать:** – особенности системного и критического мышления; **уметь:** – разделять системное мышление от критического; **владеть:** – навыками организованного обучения различным видам мышления.
УК-1.2 Применяет логические формы и процедуры, способен к рефлексии по поводу собственной и чужой мыслительной деятельности.	**знать:** – логические формы и процедуры собственной и чужой мыслительной деятельности; **уметь:** – выбирать логические формы обучения мыслительной деятельности; **владеть:** – навыками выбора форм обучения.
УК-1.3 Анализирует источник информации с точки зрения временных и пространственных условий его возникновения.	**знать:** – точки зрения временных и пространственных условий его возникновения информации; уметь: – анализировать информационную среду; владеть: – навыками анализирования информационной среды.
УК-1.4 Анализирует ранее сложившиеся в науке оценки информации.	**знать:** – ранее сложившиеся в науке оценки информации; **уметь:** – анализировать и производить оценку информации в науке; **владеть:** – навыками анализирования и оценки информаций.
УК-1.5 Сопоставляет разные источники информации с целью выявления их противоречий и поиска достоверных суждений.	знать: – основные виды источников информации; уметь: – сопоставлять разные виды источников информации; владеть: – навыками сопоставления информации.
УК-1.6 Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение.	**знать:** – основы формирования собственного суждения и оценку информации; **уметь:** – принимать обоснованное решение; **владеть:** – навыками применения обоснованных решений в области информации.
УК-1.7 Определяет практические последствия предложенного решения задачи.	**знать:** – практические последствия предложенного решения; **уметь:** – применять на практике решение задач;

	владеть: – навыками определения практических задач.
ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этик	
ОПК-1.1 Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно-правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего профессионального образования, профессионального обучения, законодательства о правах ребенка, трудового законодательства.	**знать:** – приоритетные направления развития образовательной системы ; **уметь:** – подбирать приоритетные направления в образовательной системе; **владеть:** – навыками подбора приоритетных направлений в образовательной системе.
ОПК-1.2 Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности.	**знать:** – нормативно-правовые акты в сфере образования; **уметь:** – подбирать нормативно-правовые акты в сфере образования; **владеть:** – навыками подбора нормативно-правовых актов в образовательное среде.
ПК-3. Способен реализовывать образовательные программы различных уровней в соответствии с современными методиками и технологиями, в том числе информационными, для обеспечения качества учебно-воспитательного процесса.	
ПК-3.1 Проектирует результаты обучения в соответствии с нормативными документами в сфере образования, возрастными особенностями обучающихся, дидактическими задачами урока.	**знать:** – основные нормативные документы в сфере образования; **уметь:** – подбирать нормативно-правовые документы в сфере образования; **владеть:** – навыками подбора нормативно-правовых документов.

ПК-3.2 Осуществляет отбор предметного содержания, методов, приемов и технологий, в том числе информационных, обучения истории и обществознанию, организационных форм учебных занятий, средств диагностики в соответствии с планируемыми результатами обучения.	**знать:** – содержание методов, приемов и технологий, в том числе информационных, обучения истории и обществознанию, организационных форм учебных занятий, средств диагностики в соответствии с планируемыми результатами обучения; **уметь:** – выбирать методы, приемы и технологии при обучении; **владеть:** – навыками преобразования методов, приемов и технологии при обучении.
ПК-3.3 Проектирует план-конспект / технологическую карту урока физической культуры и основ безопасности жизнедеятельности.	**знать:** – технологическую карту урока; **уметь:** – проектировать урок; **владеть:** – навыками проектирования уроков.
ПК-3.4 Формирует познавательную мотивацию обучающихся к физической культуре и безопасности жизнедеятельности в рамках урочной и внеурочной деятельности.	**знать:** – познавательную мотивацию обучающихся; **уметь:** – строить занятия с акцентом на познавательную деятельность обучающихся; **владеть:** – навыками построения занятий.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Первый семестр
Контактная работа (всего)	**36**	**36**
Лекции	18	18
Практические	18	18
Самостоятельная работа (всего)	**36**	**36**
Виды промежуточной аттестации	**36**	**36**
Экзамен	36	36
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Место информационной безопасности в системе национальной безопасности РФ:

Общие вопросы информационной безопасности. Теория информационной безопасности и ее основные направления. Виды возможных нарушений информационной безопасности. Причины возникновения информационных угроз и меры защиты от них.

Модуль 2. Законодательство в области информационной безопасности:

Назначение и задачи обеспечения информационной безопасности на уровне государства. Понятие о видах вирусов. Антивирусная защита компьютера. Технология построения защищенных информационных систем. Криптография как наука. Методы психологического воздействия на пользователя сети Интернет.

5.2. Содержание дисциплины: Лекции (18 ч.)

Модуль 1. Место информационной безопасности в системе национальной безопасности РФ (8 ч.)

Тема 1. Понятие информационной безопасности (2 ч.)

1. Основные составляющие.
2. Важность проблемы. Понятие информационной безопасности.
3. Основные составляющие информационной безопасности

Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность (2 ч.)

1. Объектно-ориентированный подход к информационной безопасности
2. Основные понятия объектно-ориентированного подхода
3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Тема 3. Наиболее распространенные угрозы (2 ч.)

1. Основные определения и критерии классификации угроз
2. Некоторые примеры угроз доступности
3. Вредоносное программное обеспечение
4. Основные угрозы целостности
5. Основные угрозы конфиденциальности

Тема 4. Законодательный уровень информационной безопасности (2 ч.)

1. Обзор российского законодательства в области информационной безопасности.
2. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
3. Обзор зарубежного законодательства в области информационной безопасности.
4. О текущем состоянии российского законодательства в области информационной безопасности

Модуль 2. Законодательство в области информационной безопасности (10 ч.)

Тема 5. Стандарты и спецификации в области информационной безопасности (2 ч.)

1. Оценочные стандарты и технические спецификации.
2. «Оранжевая книга» как оценочный стандарт.
3. Основные понятия. Механизмы безопасности.
4. Классы безопасности.
5. Информационная безопасность распределенных систем.
6. Рекомендации X.800. Сетевые сервисы безопасности.
7. Администрирование средств безопасности.

Тема 6. Основы государственной политики в области информационной безопасности (2 ч.)

1. Стратегия национальной безопасности Российской Федерации
2. Доктрина информационной безопасности Российской Федерации
3. Закон «О государственной тайне»
4. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию
5. Уголовно-правовая защита информации, составляющей государственную тайну

Тема 7. Закон «О коммерческой тайне» (2 ч.)

1. Порядок отнесения информации к коммерческой тайне и способы ее получения
2. Права обладателя информации, составляющей коммерческую тайну.
3. Ответственность за нарушение требований Федерального закона «О коммерческой тайне»

Тема 8. Основные угрозы информационной безопасности (2 ч.)

1. Основные непреднамеренные искусственные угрозы
2. Классификация угроз безопасности
3. Описание модели гипотетического нарушителя

Тема 9. Классификация мер обеспечения безопасности компьютерных систем

(2 ч.)

1.Нормативно-правовые меры

2.Морально-этические меры

3.Административные меры

4.Технические (программно-аппаратные) меры

5.3. Содержание дисциплины: Практические (36 ч.)

Модуль 1. Место информационной безопасности в системе национальной безопасности РФ (18 ч.)

Тема 1. Понятие информационной безопасности (2 ч.)

1. Основные составляющие.

2. Важность проблемы. Понятие информационной безопасности.

3.Основные составляющие информационной безопасности

Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность (2 ч.)

1. Объектно-ориентированный подход к информационной безопасности

2. Основные понятия объектно-ориентированного подхода

3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Тема 3. Наиболее распространенные угрозы (2 ч.)

1. Основные определения и критерии классификации угроз.

2. Некоторые примеры угроз доступности.

3. Вредоносное программное обеспечение.

4. Основные угрозы целостности.

5. Основные угрозы конфиденциальности.

Тема 4. Законодательный уровень информационной безопасности (2 ч.)

1. Обзор российского законодательства в области информационной безопасности.

2. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.

3. Обзор зарубежного законодательства в области информационной безопасности.

4. О текущем состоянии российского законодательства в области информационной безопасности

Тема 5. Стандарты и спецификации в области информационной безопасности (2 ч.)

1. Оценочные стандарты и технические спецификации.

2. «Оранжевая книга» как оценочный стандарт.

3. Основные понятия. Механизмы безопасности.

4. Классы безопасности.

5. Информационная безопасность распределенных систем.

6. Рекомендации X.800. Сетевые сервисы безопасности.

7. Администрирование средств безопасности.

Тема 6. Основы государственной политики в области информационной безопасности (2 ч.)

1. Стратегия национальной безопасности Российской Федерации

2. Доктрина информационной безопасности Российской Федерации

3. Закон «О государственной тайне»

4. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

5. Уголовно-правовая защита информации, составляющей государственную тайну

Тема 7. Закон «О коммерческой тайне» (2 ч.)

1. Порядок отнесения информации к коммерческой тайне
и способы ее получения
2. Права обладателя информации, составляющей
коммерческую тайну
3. Ответственность за нарушение требований Федерального
закона «О коммерческой тайне»

Тема 8. Основные угрозы информационной безопасности (2 ч.)

1.Основные непреднамеренные искусственные угрозы
2.Классификация угроз безопасности
3.Описание модели гипотетического нарушителя

Тема 9. Классификация мер обеспечения безопасности компьютерных систем (2 ч.)

1.Нормативно-правовые меры
2.Морально-этические меры
3.Административные меры
4.Технические (программно-аппаратные) меры

Модуль 2. Законодательство в области информационной безопасности (18 ч.)
Тема 10. Критерии оценки надежных компьютерных систем (2 ч.)

1. Основные элементы политики безопасности
2. Механизмы безопасности
3. Классы безопасности

Тема 11. Правовое обеспечение информационной безопасности (2 ч.)

1. Основные нормативно-правовые акты в области информационной безопасности
2. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны

Тема 12. Организационное обеспечение информационной безопасности (2 ч.)

1. Основные стандарты в области обеспечения информационной безопасности
2. Политика безопасности.
3. Экономическая безопасность предприятия

Тема 13. Криптографические методы защиты информации (2 ч.)

1. Симметричные и ассиметричные системы шифрования
2. Цифровые подписи (Электронные подписи)
3. Инфраструктура открытых ключей
4. Криптографические протоколы

Тема 14. Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности (2 ч.)

1. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
2. Формы и методы проведения занятий по теме, применяемые образовательные технологии

Тема 15. Использование криптографических средств защиты информации (2 ч.)

1. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование
2. Формы и методы проведения занятий по теме, применяемые образовательные технологии

Тема 16. Средства стеганографии для защиты информации (2 ч.)

1. Использование средств стеганографии для защиты файлов
2. Формы и методы проведения занятий по теме, применяемые образовательные технологии

Тема 17. Настройка безопасного сетевого соединения (2 ч.)

1. Создание защищенного канала связи средствами виртуальной частной сети
2. Формы и методы проведения занятий по теме, применяемые образовательные технологии

Тема 18. Антивирусные средства защиты информации (2 ч.)

1. Изучение настроек средств антивирусной защиты информации

2. Формы и методы проведения занятий по теме, применяемые образовательные технологии

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

6.1 Вопросы и задания для самостоятельной работы

Первый семестр (28,8 ч.)

Модуль 1. Место информационной безопасности в системе национальной безопасности РФ (7 ч.)

Вид СРС: Выполнение индивидуальных заданий

Подготовить реферат по заданной теме.

Темы рефератов

1. Политика ИБ в образовательном учреждении (отразить концепцию ИБ образовательного учреждения и перечень мероприятий).

2. Организация защиты электронной почты.

3. Организация защиты ПК в образовательном учреждении.

4. Нормативно-правовой аспект защиты информации в образовательном учреждении.

5. Организация защиты баз данных.

6. Ответственность за нарушения в сфере информационного права.

7. Конфиденциальная информация, ее виды и способы защиты.

8. Программные средства защиты (ПК, сети).

9. Угрозы ИБ, виды угроз, способы защиты.

10. Вирусная атака, ее механизм реализации.

Вид СРС: *Подготовка к коллоквиуму

Вопросы к коллоквиуму:

1. Раскройте различные подходы к определению понятия «информационная безопасность». Привести примеры нарушения информационной безопасности в быту и на предприятии.

2. Обоснуйте основные задачи системы информационной безопасности.

3. Обоснуйте этапы развития информационной безопасности.

4. Раскройте понятие «защита информации» и обоснуйте основные аспекты защиты информации.

5. Охарактеризуйте программные средства организации информационной безопасности при работе на компьютере. На примере одного приложения раскройте его функциональные возможности по защите информации.

6. Охарактеризуйте программные средства организации информационной безопасности в компьютерной сети. На примере одного приложения раскройте его функциональные возможности по защите информации.

7. Охарактеризуйте аппаратные средства организации информационной безопасности при работе на компьютере. Приведите примеры аппаратных средств защиты информации.

8. Охарактеризуйте аппаратные средства организации информационной безопасности в компьютерной сети. Приведите примеры аппаратных средств защиты информации.

9. Укажите основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на ПК для сотрудников образовательного учреждения.

10. Раскройте понятие «сетевые атаки». Приведите примеры сетевых атак. Укажите способы несанкционированного проникновения на сетевой компьютер и охарактеризуйте пути противодействия им.

11. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности. Охарактеризуйте виды угроз. Приведите примеры угроз различных видов.

12. Раскройте суть нормативно-правового аспекта защиты информации. Охарактеризуйте структуру законодательства России в области защиты информации.

13. Дайте определение государственной тайне. Перечислите основные статьи в Законе о государственной тайне.

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

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

16. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.

17. Охарактеризуйте организационные меры защиты информации. Обоснуйте основные организационные мероприятия информационной безопасности.

18. Охарактеризуйте технологические меры информационной безопасности. Обоснуйте классификацию средств технологической защиты информации.

19. Охарактеризуйте аппаратные средства защиты информации, укажите основания для их классификации. Приведите примеры аппаратных средств защиты информации.

20. Опишите суть программной защиты информации. Перечислите основные средства программной защиты информации, обоснуйте их классификацию. На примере одного приложения раскройте его функциональные возможности по защите информации.

21. Перечислите антивирусные программные средства. На примере конкретного приложения продемонстрируйте настройку безопасности.

22. Раскройте понятие «компьютерный вирус». Перечислите виды компьютерных вирусов. Приведите примеры, опишите способы их проникновения и особенности разрушительных действий.

23. Перечислите способы проникновения компьютерных вирусов на компьютер. Приведите примеры, опишите особенности их разрушительных действий.

24. Раскройте суть технология антивирусной защиты сетевого компьютера. Приведите примеры антивирусных приложений и укажите особенности их функционала.

25. Охарактеризуйте вредоносные программы и их виды. Перечислите способы борьбы с ними.

26. Охарактеризуйте программные средства ограничения доступа в Интернет, фильтрации информационных ресурсов. На примере одного приложения раскройте его функциональные возможности по ограничению доступа в Интернет.

27. Укажите виды мошенничества в сети Интернет. Перечислите способы противодействия Интернет-мошенникам. Охарактеризуйте поведение при возникновении угрозы Интернет-мошенников.

Вид СРС: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн курса:

«Основы информационной безопасности при работе на компьютере» http://www.intuit.ru/studies/courses/680/536/info

Вид СРС: *Подготовка к промежуточной аттестации

Прохождение онлайн курса:

«Основы информационной безопасности при работе на компьютере» http://www.intuit.ru/studies/courses/680/536/info

Вид СРС: *Подготовка к промежуточной аттестации

Изучение основной и дополнительной литературы по данному модулю.

Модуль 2. Законодательство в области информационной безопасности (7 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Подготовить реферат по заданной теме.

Темы рефератов

1. Электронная цифровая подпись.
2. Киберпреступность в России и в других странах.
3. Криптографические системы защиты данных.
4. Исторические шифры.
5. Современный шифры.

Вид СРС: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн курса:

«Технологии и продукты Microsoft в обеспечении информационной безопасности» http://www.intuit.ru/studies/courses/600/456/info.

Вид СРС: *Подготовка к промежуточной аттестации

Изучение основной и дополнительной литературы по данному модулю.

Вид СРС: Наименование вида СРС

Прохождение тестирование в системе Инфо-вуз

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1. Компетенции и этапы формирования

№ п/п	Оценочные средства	Компетенции, этапы их формирования
1	Учебно-исследовательский модуль	УК-1.
2	Предметно-методический модуль	УК-1, ОПК-1, ПК-3.
3	Психолого-педагогический модуль	ПК-3, ОПК-1.
4	Социально-гуманитарный модуль	УК-1, ОПК-1.
5	Коммуникативный модуль	УК-1.
6	Предметно-технологический модуль	ПК-3.

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
	Экзамен (дифференцированный зачет)	Зачет	
Повышенный	5 (отлично)	зачтено	90 – 100%
Базовый	4 (хорошо)	зачтено	76 – 89%
Пороговый	3 (удовлетворительно)	зачтено	60 – 75%
Ниже порогового	2 (неудовлетворительно)	Не зачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Хорошо	Студент знает и понимает теоретическое содержание; в достаточной степени демонстрирует умения применять на практике и переносить из одной научной области в другую теоретические знания; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.
Неудовлетворительно	Студент демонстрирует незнание основного содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении предлагаемых заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.
Удовлетворительно	Студент 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. Допускается несколько ошибок в содержании ответа при этом ответ отличается недостаточной глубиной и полнотой раскрытия темы.
Отлично	Студент знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач. Ответ студента характеризуется глубиной раскрытия темы, дополнен примерами, использованы межпредметные связи.

8.3. Вопросы, задания текущего контроля

Первый семестр (Экзамен, ОПК-1.1, ОПК-1.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4, УК-1.1, УК-1.2, УК-1.3, УК-1.4, УК-1.5, УК-1.6, УК-1.7)

1. Перечислите основные угрозы информационной безопасности
2. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
3. Опишите правовой режим государственной тайны
4. Перечислите основные виды технических каналов утечки информации
5. Перечислите методы защиты информации от утечки по вибрационному каналу

6. Оказание первой медицинской помощи при поражении электрическим током

2. Оказание первой медицинской помощи при обмороке за рабочим местом (компьютером)

7. Виды ответственности работодателя за не соблюдение рабочего времени

9. Перечислите средства и методы защиты информации от утечки в телефонных линиях

10. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам

11. Назовите основные цели государства в области обеспечения информационной безопасности

12. Назовите основные нормативные акты РФ, связанные с правовой защитой информации

13. Назовите способы и механизмы совершения информационных компьютерных преступлений

14. Перечислите основные угрозы информационной безопасности

15. Перечислите виды защищаемой информации

16. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности

17. Охарактеризуйте биометрические данные как персональные данные

18. Опишите правовой режим государственной тайны

19. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014

20. Перечислите основные виды технических каналов утечки информации

21. Перечислите методы защиты информации от утечки по воздушному каналу

22. Перечислите методы защиты информации от утечки по вибрационному каналу

23. Перечислите методы защиты информации от утечки по индукционному каналу

24. Перечислите средства и методы защиты информации от утечки в телефонных линиях

25. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам

26. Назовите основные цели государства в области обеспечения информационной безопасности

27. Назовите основные нормативные акты РФ, связанные с правовой защитой информации

28. Перечислите виды компьютерных преступлений

29. Назовите способы и механизмы совершения информационных компьютерных преступлений

30. Перечислите основные параметры и черты информационной компьютерной преступности в России

31. Дайте определение: компьютерный вирус. Перечислите основные виды компьютерных вирусов

32. Назовите основные методы защиты от компьютерных вирусов

33. Перечислите основные типы антивирусных программ

34. Назовите основные меры защиты от несанкционированного доступа. Идентификация и аутентификация пользователя

35. Перечислите основные угрозы компьютерной безопасности при работе в сети Интернет

36. Назовите виды защищаемой информации

37. Перечислите составляющие информационной безопасности и их определение

38. Назовите взаимосвязь между составляющими информационной безопасности. Приведите собственные примеры

39. Перечислите уровни формирования режима ИБ

40. Перечислите основные механизмы информационной безопасности

41. Назовите, что понимается под администрированием средств безопасности

42. Дайте определение политика безопасности

43. Перечислите классы угроз ИБ

44. Назовите причины и источники случайных воздействий на информационные системы

45. Дайте характеристику преднамеренным угрозам

46. Перечислите каналы несанкционированного доступа

47. Охарактеризуйте угрозы доступности информации

48. Назовите классификационные признаки и характерные черты компьютерных вирусов

49. Назовите вид вирусов, который наиболее распространен в распределенных вычислительных сетях

50. Перечислите деструктивные возможности компьютерных вирусов

51. Перечислите виды «вирусоподобных» программ

52. Поясните понятия «сканирование на лету» и «сканирование по запросу»

53. Перечислите виды антивирусных программ

54. Охарактеризуйте антивирусные сканеры

55. Назовите факторы, которые определяют качество антивирусных программ

56. Перечислите наиболее распространенные пути заражения компьютеров вирусами

57. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей

58. Перечислите основополагающие документы по информационной безопасности

59. Раскройте понятие «средства защиты государственной тайны». Какие категории государственных информационных ресурсов определены в Законе «Об информации, информатизации и защите информации»

60. Перечислите механизмы безопасности для обеспечения конфиденциальности трафика. Назовите основные механизмы безопасности

61. Дайте определение понятия политики безопасности. Раскройте основные направления разработки политики безопасности

62. Перечислите основные задачи информационной безопасности в соответствии с концепцией национальной безопасности РФ

63. Дайте определение понятия политика безопасности информационных систем. Назначение политики безопасности

64. Перечислите функции и назначение стандартов информационной безопасности. Приведите примеры стандартов, их роль при проектировании и разработке информационных систем

65. Охарактеризуйте единые критерии безопасности информационных технологий. Раскройте понятие профиля защиты. Структура профиля защиты

66. Дайте характеристику Законодательного уровня обеспечения информационной безопасности. Перечислите основные законодательные акты РФ в области защиты информации

67. Перечислите уровни формирования режима информационной безопасности. Дайте краткую характеристику законодательно-правового уровня

68. Назовите основные классы угроз информационной безопасности. Дайте характеристику преднамеренным угрозам

69. Дайте определение программного вируса. Перечислите основные трудности, возникающие при определении компьютерного вируса

70. Назовите виды избыточности, которые могут использоваться в вычислительных сетях. Расскажите о видах вирусов наиболее распространенных и распределенных вычислительных сетях

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

Промежуточная аттестация проводится в форме экзамена.

Экзамен по дисциплине или ее части имеет цель оценить сформированность общекультурных, профессиональных и специальных компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

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

Устный ответ на экзамене

При определении уровня достижений студентов на экзамене необходимо обращать особое внимание на следующее:

– дан полный, развернутый ответ на поставленный вопрос;

– показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи;

– знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей;

– ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

– теоретические постулаты подтверждаются примерами из практики.

Тесты

При определении уровня достижений студентов с помощью тестового контроля необходимо обращать особое внимание на следующее:

– оценивается полностью правильный ответ;

– преподавателем должна быть определена максимальная оценка за тест, включающий определенное количество вопросов;

– преподавателем может быть определена максимальная оценка за один вопрос теста;

– по вопросам, предусматривающим множественный выбор правильных ответов, оценка определяется исходя из максимальной оценки за один вопрос теста.

Письменная контрольная работа

Виды контрольных работ: аудиторные, домашние, текущие, экзаменационные, письменные, графические, практические, фронтальные, индивидуальные.

Система заданий письменных контрольных работ должна:

– выявлять знания студентов по определенной дисциплине (разделу дисциплины);

– выявлять понимание сущности изучаемых предметов и явлений, их закономерностей;

– выявлять умение самостоятельно делать выводы и обобщения;

– творчески использовать знания и навыки.

Требования к контрольной работе по тематическому содержанию соответствуют устному ответу.

Также контрольные работы могут включать перечень практических заданий.

Контекстная учебная задача, проблемная ситуация, ситуационная задача, кейсовое задание.

При определении уровня достижений студентов при решении учебных практических задач необходимо обращать особое внимание на следующее:

– способность определять и принимать цели учебной задачи, самостоятельно и творчески планировать 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 правильное изложение ответа на вопросы и задания;

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

– грамотное использование основной и дополнительной литературы;

– умение использовать современные информационные технологии для решения учебных задач, использовать научные достижения других дисциплин;

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

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А. В. Артемов ; Межрегиональная Академия безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. – Режим доступа ://biblioclub.ru/index.php?page=book&id=428605

2. Бабаш, А. В. Информационная безопасность. Лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – М. : КНОРУС, 2012. – 131 с. + CD

3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа : /biblioclub.ru/index.php?page=book&id=276557

4. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. – 2-е изд., испр. – М. : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. – Режим доступа : //biblioclub.ru/index.php?page=book&id=429035

5. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – СПб. : Издательство Политехнического университета, 2014. – 322 с. – Режим доступа : //biblioclub.ru/index.php?page=book&id=363040

6. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа ://biblioclub.ru/index.php?page=book&id=438331

7. Спицын, В.Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. Режим доступа : //biblioclub.ru/index.php?page=book&id=208694

Дополнительная литература

1. Конституция Российской Федерации.

2. Доктрина информационной безопасности.

3. Закон РФ «Об информации, информатизации и защите информации».

4. Закон РФ «О государственной тайне»

5. Закон РФ «Об электронной цифровой подписи»

6. Закон РФ «О национальной платежной системе» (от 27 июня 2011 г. №161-ФЗ г. Москва).

7. Информационная безопасность. Защита информации [Электронный ресурс]. – Режим доступа: http://all-ib.ru.

8. «Гарант – информационно-правовой портал» [Электронный ресурс]. Адрес доступа: http://www.garant.ru/?gclid=CLX24o_Bsr0CFcoLcwodR7sA2w

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://edu-top.ru/katalog – Университетская библиотека онлайн [Электронный ресурс]. – М. : Издательство «Директ-Медиа». – Режим доступа: http://biblioclub.ru/

2. http://www.intuit.ru – Интернет-Университет Информационных Технологий [Электронный ресурс] / Бесплатные учебные курсы по информационным технологиям. – М. : НОУ «ИНТУИТ»,

3. http://www.informika.ru – Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций» [Электронный ресурс] / М.: Informika.ru, 2002 – 2016. – Режим доступа: http://www.informika.ru/

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;

– конкретизировать для себя план изучения материала;

– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:

– проработайте каждую тему по предлагаемому ниже алгоритму действий;

– изучив весь материал, выполните итоговый тест, который продемонстрирует готовность к сдаче зачета.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

– выпишите в тетрадь основные категории и персоналии по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к зачету;

– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на лабораторном занятии;

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;

– составьте собственные аннотации к другим источникам на карточках, что поможет при подготовке рефератов, текстов речей, при подготовке к зачету;

– выберите те источники, которые наиболее подходят для изучения конкретной темы

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 современных профессиональных баз данных

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

12.3 Перечень современных профессиональных баз данных

13. Материально-техническое обеспечение дисциплины

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.

При изучении дисциплины используется интерактивный комплекс Flipbox для проведения презентаций и видеоконференций, система iSpring в процессе проверки знаний по электронным тест-тренажерам.

Индивидуальные результаты освоения дисциплины студентами фиксируются в информационной системе 1 С:Университет.

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

1. АРМ-19 (в составе: системный блок, сетевой фильтр, клавиатура, мышь, колонки) – 13 шт.