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 (МОДУЛЯ)

Наименование дисциплины (модуля): Информационная безопасность
Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Физическая культура. Безопасность жизнедеятельности
Форма обучения: Очная

Разработчик:
Карабанова О. Н., старший преподаватель

Программа рассмотрена и утверждена на заседании кафедры, протокол № 10 от 26.04.2016 года

Зав. кафедрой Якимова Е. А.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 29.08.2017 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 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; сформировать у бакалавров систему знаний, умений и навыков, необходимых для использования инновационных технологий обучения в предметных областях физическая культура и безопасность жизнедеятельности, раскрыть подходы к пониманию и определению специфики образовательных технологий и проанализировать опыт их применения.

Задачи дисциплины:

- ознакомление студентов с терминологией информационной безопасности;
- развитие мышления студентов;
- обучение определению причин, видов, источников и каналов утечки, искажения информации;
- раскрыть студентам задачи, содержание, принципы, формы, методы и средства инновационных технологий в предметных области безопасность жизнедеятельности;
- ознакомление студентов использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ОД.6 «Информационная безопасность» относится к вариативной части учебного плана.

Дисциплина изучается на 1 курсе, в 2 семестре.

Для изучения дисциплины требуется: обеспечения информационной безопасности

Освоение дисциплины Б1.В.ОД.6 «Информационная безопасность» является необходимой основой для последующего изучения дисциплин (практик):

Б1.В.ДВ.23.2 Основы управления безопасностью жизнедеятельности;

Б1.Б.4 Безопасность жизнедеятельности;

Б1.Б.14 Информационные технологии в образовании.

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) (воспита-

тель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими общекультурными компетенциями (ОК):

ОК-3. способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	
ОК-3 способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	знать: - основные понятия Федерального закона; - Государственную систему правового обеспечения защиты информации в Российской Федерации; - основные направления государственной политики в сфере информатизации; уметь: - определять виды угроз информационным системам; владеть: - информационными системами;- навыками работы с различными источниками информации, информационными ресурсами и технологиями, применения основных методов, способов и средств получения, хранения, поиска, систематизации, обработки и передачи информации, применения в профессиональной.
ОК-9. способность использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций	
ОК-9 способность использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций	знать: - идентификацию травмирующих, вредных и поражающих факторов чрезвычайных ситуаций; уметь: - планировать мероприятия по защите производственного персонала и населения в чрезвычайных ситуациях и при необходимости принимать участие в проведении спа-сательных работ и других неотложных работ при ликвида-ции последствий чрезвычайных ситуаций; владеть: - методами обеспечения безопасности жизнедеятельности населения в повседневной жизни и чрезвычайных ситуациях.

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

ПК-2. способность использовать современные методы и технологии обучения и диагностики

педагогическая деятельность

ПК-2 способность использовать современные методы и технологии обучения и диагностики	знать: - современные методы и технологии обучения и диагностики; уметь: - использовать различные формы, методы воспитания и обучения в профессиональной деятельности; владеть: - словесными, практическими, наглядными и игровыми методами обучения и различными методами диагностики в ходе организованной практической деятельности.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Второй семестр
Контактная работа (всего)	**54**	**54**

Лекции	18	18
Практические	36	36
Самостоятельная работа (всего)	**14**	**14**
Виды промежуточной аттестации	**40**	**40**
Экзамен	40	40
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Основные понятия информационной безопасности:

Основные составляющие. Важность проблемы Понятие информационной безопасности. Основные составляющие информационной безопасности . Важность и сложность проблемы информационной безопасности. Составляющие национальных интересов РФ в информационной безопасности.

Модуль 2. Технологии защиты информации:

Основные понятия объектно-ориентированного подхода. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.

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

5.2. Содержание дисциплины: Лекции (18 ч.)

Модуль 1. Основные понятия информационной безопасности (8 ч.)

Тема 1. Понятие информационной безопасности. (2 ч.)

Основные составляющие. Важность проблемы Понятие информационной безопасности. Основные составляющие информационной безопасности

Тема 2. Наиболее распространенные угрозы (2 ч.)

Основные определения и критерии классификации угроз. Некоторые примеры угроз доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.

Тема 3. Наиболее распространенные угрозы (2 ч.)

Основные определения и критерии классификации угроз. Некоторые примеры угроз доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.

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

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

Модуль 2. Технологии защиты информации (10 ч.)

Тема 5. Законодательный уровень информационной безопасности (2 ч.)

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

Тема 6. Стандарты и спецификации в области информационной безопасности (2 ч.)

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Администрирование средств безопасности. Функциональные требования. Требования доверия безопасности. Гармонизированные критерии Европейских стран. Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России. «СЗИ НСД» система защиты информации от несанкционированного доступа.

Тема 7. Стандарты и спецификации в области информационной безопасности (2 ч.)

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Администрирование средств безопасности. Функциональные требования. Требования доверия безопасности. Гармонизированные критерии Европейских стран. Интерпретация "Оранжевой книги" для сетевых конфигураций. Руководящие документы Гостехкомиссии России. «СЗИ НСД» система защиты информации от несанкционированного доступа.

Тема 8. Стандарты и спецификации в области информационной безопасности (2 ч.)

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Администрирование средств безопасности. Функциональные требования. Требования доверия безопасности. Гармонизированные критерии Европейских стран. Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России. «СЗИ НСД» система защиты информации от несанкционированного доступа.

Тема 9. Стандарты и спецификации в области информационной безопасности (2 ч.)

5.3. Содержание дисциплины: Практические (36 ч.)

Модуль 1. Основные понятия информационной безопасности (18 ч.)

Тема 1. Понятие информационной безопасности (2 ч.)

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

Тема 2. Понятие информационной безопасности (2 ч.)

1. Основные составляющие.

2. Важность проблемы.

3. Понятие информационной безопасности.

4. Основные составляющие информационной безопасности

Тема 3. Распространение объектно-ориентированного подхода на информационную безопасность (2 ч.)

1. О необходимости объектно-ориентированного подхода к информационной безопасности.

2. Основные понятия объектно-ориентированного подхода.

3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.

Тема 4. Распространение объектно-ориентированного подхода на информационную безопасность (2 ч.)

1. О необходимости объектно-ориентированного подхода к информационной безопасности.

2. Основные понятия объектно-ориентированного подхода.

3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.

Тема 5. 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 6. 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 7. 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 8. 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 9. . Стандарты и спецификации в области информационной безопасности (2 ч.)

1. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.

2. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем.

3. Сетевые сервисы безопасности.

4. Администрирование средств безопасности. Функциональные требования. Требования доверия безопасности.

Модуль 2. Технологии защиты информации (18 ч.)

Тема 10. . Стандарты и спецификации в области информационной безопасности (2 ч.)

1. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.

2. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем.

3. Сетевые сервисы безопасности.

4. Администрирование средств безопасности. Функциональные требования. Требования доверия безопасности.

Тема 11. Административный уровень информационной безопасности (2 ч.)

1. Политика безопасности.
2. Программа безопасности.
3. Синхронизация программы безопасности с жизненным циклом систем.

Тема 12. Административный уровень информационной безопасности (2 ч.)

1. Политика безопасности.
2. Программа безопасности.
3. Синхронизация программы безопасности с жизненным циклом систем.

Тема 13. Идентификация и аутентификация, управление доступом (2 ч.)

1. Идентификация и аутентификация.
2. Парольная аутентификация.
3. Сервер аутентификации Kerberos.
4. Идентификация/аутентификация с помощью биометрических данных.

Тема 14. Идентификация и аутентификация, управление доступом (2 ч.)

1. Идентификация и аутентификация.
2. Парольная аутентификация.
3. Сервер аутентификации Kerberos.
4. Идентификация/аутентификация с помощью биометрических данных.

Тема 15. Идентификация и аутентификация, управление доступом (2 ч.)

1. Идентификация и аутентификация.
2. Парольная аутентификация.
3. Сервер аутентификации Kerberos.
4. Идентификация/аутентификация с помощью биометрических данных.

Тема 16. Процедурный уровень информационной безопасности (2 ч.)

1. Физическая защита.
2. Поддержание работоспособности.
3. Реагирование на нарушения режима безопасности.
4. Планирование восстановительных работ.

Тема 17. Процедурный уровень информационной безопасности (2 ч.)

1. Физическая защита.
2. Поддержание работоспособности.
3. Реагирование на нарушения режима безопасности.
4. Планирование восстановительных работ.

Тема 18. Процедурный уровень информационной безопасности (2 ч.)

1. Физическая защита.
2. Поддержание работоспособности.
3. Реагирование на нарушения режима безопасности.
4. Планирование восстановительных работ.

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

6.1 Вопросы и задания для самостоятельной работы

Второй семестр (56 ч.)

Модуль 1. Основные понятия информационной безопасности (28 ч.)

Вид СРС: Выполнение компетентностно-ориентированных заданий

1. Составление синквейна.
2. Составление кластера по темам: «Безопасность», «Чрезвычайная ситуация», «Опасность».

Вид СРС: Выполнение индивидуальных заданий

Опорные схемы по темам:

1. Классификация чрезвычайных ситуаций.
2. Структура Единой российской государственной системы предупреждения и ликвидации стихийных бедствий и чрезвычайных ситуаций (РСЧС).
3. Классификация чрезвычайных ситуаций природного характера.
4. Классификация чрезвычайных ситуаций техногенного характера.
5. Классификация чрезвычайных ситуаций природного характера.
6. Источники формирования, признаки и классификация опасностей.

Модуль 2. Технологии защиты информации (28 ч.)

Вид СРС: Выполнение индивидуальных заданий

Темы опорных схем:

1. «Правила оказания доврачебной помощи в условиях автономии».
2. Средства индивидуальной и коллективной защиты населения в условиях чрезвычайной ситуации.
3. Классификация опасностей в быту и защита от них.
4. Системы жизнеобеспечения и источники опасностей в них.

Вид СРС: Подготовка публикаций (научных статей, тезисов, других научных работ)

Темы презентаций:

1. Эвакуация. Организация и порядок проведения эвакуационных мероприятий.
2. Устойчивость функционирования производственных объектов.
3. Принципы и способы защиты населения от чрезвычайных ситуаций.
4. Меры предупреждения чрезвычайных ситуаций в быту и на производственных объектах.
5. Составление синквейна.
6. Заполнение бортового журнала по темам: «Электрический ток и его воздействие на организм. Первая доврачебная помощь при поражении электрическим током»; «Системы газоснабжения и правила их эксплуатации. Первая доврачебная помощь при отравлении газом»; «Опасные и вредные факторы, возникающие при эксплуатации компьютера».
7. Разработать памятку «Правила поведения в ситуациях бытовых и промышленных пожаров».
8. Составить план эвакуации.

7. Тематика курсовых работ

Не предусмотрены

8. Оценочные средства по дисциплине

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ОК-3, ОК-9	1 курс, Второй семестр	Экзамен	Модуль 1: Основные понятия информационной безопасности.
ПК-2	1 курс, Второй семестр	Экзамен	Модуль 2: Технологии защиты информации.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:

Компетенция ОК-3 формируется в процессе изучения дисциплин:

Естественнонаучная картина мира, Информационная безопасность, Информационные технологии в образовании, Научно-исследовательская работа, Основы математической обработки информации, Подготовка к защите и защита выпускной квалификационной работы, Преддипломная практика, Технические средства обучения.

Компетенция ОК-9 формируется в процессе изучения дисциплин:

Автономное выживание человека в природной среде, Безопасность городской среды обитания, Безопасность жизнедеятельности, Безопасность на дороге и в общественном транспорте, Безопасный отдых и туризм, Гражданская оборона, Девиантное поведение как угроза безопасности личности, Здоровый образ жизни и его составляющие, Здоровье и безопасность человека, Информационная безопасность, Летняя педагогическая практика, Медико-биологические основы выживания в экстремальных ситуациях, Медико-биологические особенности воздействия на организм человека негативных факторов среды, Основы медицинских знаний, Охрана труда на производстве и в учебном процессе, Подготовка к сдаче и сдача государственного экзамена, Формирование готовности населения к действиям в экстремальных ситуациях,

Чрезвычайные ситуации природного, социального, техногенного характера и защита от них, Экологические аспекты физической культуры и спорта, Экология и безопасность жизнедеятельности, Эргономические основы безопасности жизнедеятельности.

Компетенция ПК-2 формируется в процессе изучения дисциплин:

Адаптивное физическое воспитание в дошкольных образовательных организациях, Гимнастика, Гражданская оборона, Единоборства, Информационная безопасность, Информационные технологии в образовании, Легкая атлетика, Лыжный спорт, Медико-биологические основы выживания в экстремальных ситуациях, Медико-биологические основы спортивной подготовки детей школьного возраста, Методика антропологических исследований при спортивном отборе, Олимпийское образование детей и молодежи, Основы ВНД и психического здоровья детей, Основы физической реабилитации при заболеваниях нервной системы у детей, Особенности физического воспитания и физического развития ребенка в дошкольных образовательных организациях, Педагогическая практика, Педагогические технологии в волонтерской деятельности физической культуры и спорта, Плавание, Подготовка к сдаче и сдача государственного экзамена, Практика по получению профессиональных умений и опыта профессиональной деятельности, Преддипломная практика, Психологические основы безопасности, Рекреация детей и молодежи средствами физической культуры, Система работы классного руководителя с родителями учащихся по физическому воспитанию и ЗОЖ, Современные направления оздоровительных видов физической культуры, Спортивные и подвижные игры, Теоретико-методические особенности применения здоровьесберегающих технологий в образовательном процессе, Теория и методика обучения безопасности жизнедеятельности, Теория и методика физической культуры, Технологии спортивной подготовки легкоатлетов, Технологии физкультурно-спортивной деятельности, Технология начальной подготовки прыгунов в длину, Туризм, Физическое воспитание в сельских школах, Экологические аспекты физической культуры и спорта, Эксплуатация и управление спортивными объектами.

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 «Информационная безопасность» ; 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:

демонстрирует студент, обнаруживший пробелы в знаниях основного учебно-программного материала, допускающий принципиальные ошибки в выполнении предусмотренных программой заданий, не способный продолжить обучение или приступить к

профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Уровни сформированности компетенций

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)	незачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Студент знает: фундаментальные понятия информационной безопасности; аспекты информационной безопасности; основные подходы к разработке политики информационной безопасности; нормативно-правовые документы на всех государственных уровнях, регламентирующих организацию защиты информации в РФ; функционал аппаратно-программного обеспечения и сервисы Интернет с целью организации защиты компьютерной информации в процессе профес-сиональной деятельности; правила предостережения от интернет-мошенничества; основные способы защиты компьютерной информации; способы шифрования данных Владеет средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях; криптографическими методами защиты информации; методами организации комплексной защиты информации (компьютерной, конфиденциальной)
Хорошо	Студент владеет средствами обеспечения информационной безопасности ,методами защиты информации, знает понятия информационной безопасности, аспекты информационной безопасности.
Удовлетворительно	Студент демонстрирует название основных понятий содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала.
Неудовлетворительно	Студент затрудняется отвечать.

8.3. Типовые задания для текущего контроля успеваемости

Модуль 1: Основные понятия информационной безопасности

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

1. Основные угрозы конфиденциальности
2. Основные определения и критерии классификации угроз
3. Основные угрозы целостности
4. Правовые акты общего назначения, затрагивающие вопросы информационной без-опасности

5. Перечислите уровни формирования режима ИБ

ОК-9 способность использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций

1. Назовите вредные и опасные факторы, действующие на работающего на ЭВМ
2. Дайте характеристику преднамеренным угрозам
3. Перечислите классы угроз ИБ
4. Дайте определение политики безопасности
5. Биологическое воздействие ЭМП на человека

Модуль 2: Технологии защиты информации

ПК-2 способность использовать современные методы и технологии обучения и диагностики

1. Охарактеризуйте угрозы доступности информации
2. Назовите классификационные признаки и характерные черты компьютерных вирусов
3. Перечислите деструктивные возможности компьютерных вирусов
4. Что включает в себя административный уровень
5. Приведите примеры стандартов, их роль при проектировании и разработке информационных систем

8.4. Вопросы для промежуточной аттестации

Второй семестр (Экзамен, ОК-3, ОК-9, ПК-2)

1. Дайте определение понятия «информационная безопасность». В чем заключается проблема информационной безопасности.
2. Перечислите составляющие информационной безопасности.
3. Назовите взаимосвязь между составляющими информационной безопасности. Приведите собственные примеры
4. Перечислите уровни формирования режима ИБ.
5. Какие определения информационной безопасности приводятся в «Концепции информационной безопасности сетей связи общего пользования Российской Федерации».
6. Каким образом взаимосвязаны между собой составляющие информационной безопасности. Приведите собственные примеры.
7. Что понимается под «компьютерной безопасностью». Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
8. Перечислите основные механизмы безопасности.
9. Назовите, что понимается под администрированием средств безопасности.
10. Перечислите задачи информационной безопасности общества.
11. Дайте определение политики безопасности.
12. Перечислите классы угроз ИБ.
13. Назовите причины и источники случайных воздействий на информационные системы.
14. Дайте характеристику преднамеренным угрозам.
15. Перечислите каналы несанкционированного доступа.
16. Что понимается под техническим каналом утечки информации.
17. Охарактеризуйте угрозы доступности информации.
18. Перечислите основополагающие документы по информационной безопасности.
19. Назовите классификационные признаки и характерные черты компьютерных вирусов.
20. Назовите вид вирусов, который наиболее распространен в распределенных вычислительных сетях. Почему?

21. Перечислите деструктивные возможности компьютерных вирусов.

22. Перечислите виды «вирусоподобных» программ.

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

24. Перечислите виды антивирусных программ.

25. Охарактеризуйте антивирусные сканеры.

26. Назовите факторы, которые определяют качество антивирусных программ.

27. Перечислите наиболее распространенные пути заражения компьютеров вирусами.

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

29. Что понимается под средствами защиты государственной тайны. Какие категории государственных информационных ресурсов определены в Законе «Об информации, информатизации и защите информации».

30. Раскройте цели и задачи административного уровня обеспечения информационной безопасности. Что включает в себя административный уровень.

31. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика. Перечислите основные механизмы безопасности.

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

33. Перечислите основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.

34. Дайте определения понятия политики безопасности информационных систем. Назначение политики безопасности.

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

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

37. Дайте характеристику Законодательного уровня обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.

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

39. Перечислите классы угроз информационной безопасности. Дайте характеристику преднамеренным угрозам.

40. Дайте определение программного вируса. Какие трудности возникают при определении компьютерного вируса

41. Какие виды избыточности могут использоваться в вычислительных сетях. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?

42. Перечислите классификационные признаки компьютерных вирусов. Охарактеризуйте файловый и загрузочный вирусы.

43. Перечислите субъекты информационных отношений и их роли при обеспечении информационной безопасности.

44. Дайте определение понятию «доступности информации». Перечислите каналы несанкционированного доступа.

45. Назовите причины и источники случайных воздействий на информационные системы. В чем особенность «упреждающей» защиты в информационных системах.

46. Что понимается под администрированием средств безопасности. Раскройте содержание административного уровня.

47. Перечислите основные этапы разработки защищенной системы: определение

политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

48. Назовите основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики, их содержание.

49. Перечислите функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.

50. Дайте определения понятия атаки на систему информационной безопасности. Особенности локальных атак.

51. Раскройте основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

52. Перечислите основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

53. Раскройте основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

54. Что понимается под администрированием средств безопасности. Раскройте содержание административного уровня.

55. Раскройте основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

56. Раскройте основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

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

58. Что понимается под «компьютерной безопасностью». Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.

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

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

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

Процедура промежуточной аттестации в институте регулируется «Положением о зачетно-экзаменационной сессии в ФГБОУ ВПО «Мордовский государственный педагогический институт имени М. Е. Евсевьева» (утверждено на заседании Ученого совета 29.05.2014 г., протокол №14); «Положением о независимом мониторинге качества образования студентов в ФГБОУ ВПО «Мордовский государственный педагогический институт имени М. Е. Евсевьева» (утверждено на заседании Ученого совета 29.05.2014 г., протокол №14), «Положением о фонде оценочных средств дисциплины в ФГБОУ ВПО «Мордовский государственный педагогический институт имени М. Е. Евсевьева» (утверждено на заседании Ученого совета 29.05.2014 г., протокол №14), «Положением о курсовой работе студентов в ФГБОУ ВПО «Мордовский государственный педаго-

гический институт имени М. Е. Евсевьева» (утверждено на заседании Ученого совета 20.10.2014 г., протокол №4).

Промежуточная аттестация проводится в форме (выбрать форму в соответствии с учебным планом) экзамена и (или) зачета, (защиты курсовых работ, отчетов по практике).

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.

Собеседование (устный ответ) на зачете

Для оценки сформированности компетенции посредством собеседования (устного ответа) студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

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

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом.

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. Башлы, П. Н. Информационная безопасность : учеб.-практ. пособие / П. Н. Башлы, Е. К. Баранова, А. В. Бабаш. – М. : Евразийский открытый институт, 2012. – 375 с. [Электронный ресурс, Университетская библиотека online, доступ с сайта : http://www.biblioclub.ru]

2. Безопасность жизнедеятельности : учеб. пособие / под ред. Л. А. Муравья. – М. : Юнити-Дана, 2015. – 431 с. [Электронный ресурс, Университетская библиотека online, доступ с сайта : http://www.biblioclub.ru]

3. Гаврилов, М. В. Информатика и информационные технологии : учеб. для бакалавров / М. В. Гаврилов, В. А. Климов. – 3-е изд., перераб. и доп. – М. : Юрайт, 2013. – 378 с. – (Бакалавр. Базовый курс).

4. Загинайлов, Ю. Н. Основы инфор-мационной безопасности : учеб. по-собие / Ю. Н. Загинайлов. – М., Бер-лин : Директ-Медиа, 2015. – 105 с. [Электронный ресурс, Университет-ская библиотека online, доступ с сайта : http://www.biblioclub.ru]

5. Загинайлов, Ю. Н. Основы инфор-мационной безопасности : учеб. по-собие / Ю. Н. Загинайлов. – М., Бер-лин : Директ-Медиа, 2015. – 105 с. [Электронный ресурс, Университет-ская библиотека online, доступ с сайта : http://www.biblioclub.ru]

6. Захарова, И. Г. Информационные технологии в образовании : учеб. для студентов учреждений высш. проф. образования / И. Г. Захарова. – 8-е изд., перераб. и доп. – М. : Академия, 2013. – 203 с. – (Бакалавриат).

7. Канивец, Е.К. Информационные технологии в профессиональной деятельности. Курс лекций [Электронный ресурс] : учебное пособие / Е.К. Канивец. - Оренбург : ОГУ, 2015. - 108 с. - URL: //biblioclub.ru/index.php?page=book&id=439012

8. Каракеян, В. И. Безопасность жизнедеятельности : учеб. для бакалавров / В. И. Каракеян, И. М. Никулина. – М. : Юрайт, 2013. – 455 с.

9. Карпенков, С.Х. Технические средства информационных технологий [Электронный ресурс] : учебное пособие / С.Х. Карпенков. – 3-е изд., испр. и доп. – М. ; Берлин : Директ-Медиа, 2015. – 376 с. – Режим доступа: //biblioclub.ru/index.php?page=book&id=275367

10. Красильникова, В.А. Информационные и коммуникационные технологии в образовании [Электронный ресурс] : учебное пособие / В.А. Красильникова. – М. : Директ-Медиа, 2013. – 231 с. – Режим доступа: //biblioclub.ru/index.php?page=book&id=209292

11. Красильникова, В.А. Использование информационных и коммуникационных технологий в образовании [Электронный ресурс] : учебное пособие / В.А. Красильникова. – М. : Директ-Медиа, 2013. – 292 с. – Режим доступа: //biblioclub.ru/index.php?page=book&id=209293

12. Лемешко, Т. Б. Информационные технологии в образовании [Электронный ресурс] : учебное пособие / Т. Б. Лемешко. М. : Издательство РГАУ-МСХА, 2012. – 132 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=144926

13. Лыткина, Е.А. Применение информационных технологий [Электронный ресурс] : учебное пособие / Е.А. Лыткина. – Архангельск : САФУ, 2015. – 91 с. – Режим доступа: //biblioclub.ru/index.php?page=book&id=436329

14. Нестеров, С. А. Основы информа-ционной безопасности : учеб. пособие / С. А. Нестеров. – СПб. : Изд-во Политехнического университета, 2014. – 322 с. [Электронный ресурс, Универ-ситетская библиотека online, доступ с сайта : http://www.biblioclub.ru]

15. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. нестеров. – СПб. : Изд-во Политехнического ун-та, 2014. – 322 с. [Электронный ресурс, Университетская библиотека online, доступ с сайта : http://www.biblioclub.ru]

16. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. – самара : СГАСУ, 2014. – 113 с. [Электронный ресурс, Университетская библиотека online, доступ с сайта : http://www.biblioclub.ru]

17. Рабинович, П. Д. Практикум по интерактивным технологиям : метод. пособие / П. Д. Рабинович, Э. Р. Баграмян. – 3-е изд. – М. : БИНОМ. Лаборатория знаний, 2013. – 96 с. – (ИКТ в работе учителя).

18. Современные компьютерные технологии [Электронный ресурс] : учебное пособие/ Р.Г. Хисматов, Р.Г. Сафин, Д.В. Тунцев, Н.Ф. Тимербаев. – Казань : Издательство КНИТУ, 2014. – 83 с. – Режим доступа: //biblioclub.ru/index.php?page=book

Дополнительная литература

1. Казанцев, С. Я. Правовое обеспечение информационной безопасности : учебное пособие для вузов / С. Я. Казанцев и др. ; под ред. С. Я. Казанцева. – М. : Академия, 2005. – 240 с.

2. Куприянов, А. И. Основы защиты информации : учебное пособие для вузов / А. И. Куприянов и др. – М. : Академия, 2006. – 256 с.

3. . Мельников, В. П. Информационная безопасность и защита информации : учебное пособие для вузов / В. П. Мельников и др. ; под ред. С. А. Клейменова. – М. : Академия, 2006. – 336 с.

4. Информационное общество : Информационные войны. Информационное управление. Информационная безопасность / С. М. Виноградова и др. ; под ред. М. А. Вуса. – СПб. : Издательство СПбГУ, 1999. – 212 с.

5. Ярочкин, В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. – М. : Академический Проект, 2003. – 638 с.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

1. http://0bj.ru/ - Сайт Безопасность жизнедеятельности

2. <Объект не найден> (9080:a8ac00505683152e11e6dfb8b13ff07d) - Безопасность жизнедеятельности: учебное пособие. / Осетров Г.В. – М.: Книжный мир, 2011. – 232 с.

3. http://bzhde.ru/ - Энциклопедия безопасности жизнедеятельности

4. http://window.edu.ru/resource/483/70483 - Единое окно доступа к образовательным ресурсам / Федеральный портал / Федеральный центр ЭОР / Единая коллекция ЦОР

5. http://www.koob.ru/ilyin_a/shkola_vizhivaniya_v_prirodnih_usloviyah - Школа выживания в природных условиях. Ильин А.А

6. http://www.school-obz.org - Основы безопасности жизнедеятельности. Электронное научно-методическое издание для учителей ОБЖ .

7. http://www.mchs.gov.ru/ - Портал МЧС России

8. https://yadi.sk/d/MSnKOolvR4wAv - Оказание первой помощи пострадавшим – практическое пособие

9. http://www.scrf.gov.ru/ - Сайт Совета безопасности Российской Федерации

11. Методические указания обучающимся по освоению дисциплины

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;

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 информационно-справочных систем

1. Microsoft Windows 7 Pro
2. Microsoft Office Professional Plus 2010

12.2 Перечень современных профессиональных баз данных

1. Информационно-правовая система «ГАРАНТ» (http://www.garant.ru)
2. Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)

12.3 Электронные библиотечные системы

1. Профессиональная база данных «Портал открытых данных Министерства культуры Российской Федерации» (http://opendata.mkrf.ru/);
2. Единое окно доступа к образовательным ресурсам (http://window.edu.ru).

13. Материально-техническое обеспечение дисциплины

- Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
- Помещение укомплектовано специализированной мебелью и техническими средствами обучения.
- Основное оборудование:
- Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (УМК трибуна, проектор, интерактивный экран, компьютер, документ-камера, гарнитура, лазерная указка), доска маркерная.
- Учебно-наглядные пособия:
- Презентации.
- Лицензионное программное обеспечение:
- Microsoft Windows 7 Pro – Лицензия № 60948555 от 30.08.2012 г.
- Microsoft Office Professional Plus 2010 – Акт на передачу прав № 51 от12.07.2012 г.
- 1С: Университет ПРОФ – Лицензионное соглашение № 10920137 от 23.03.2016 г.