МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы и средства защиты информации

Направление подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность программы
Информатика и экономика

Уровень высшего образования – бакалавриат

Программа подготовки – академический бакалавриат

Форма обучения
Очная

Институт	Энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	4
Семестр	7

Магнитогорск
2016 г.

Рабочая программа составлена на основе ФГОС ВО по направлению 44.03.05 «Педагогическое образование», утвержденного 09.02.2016 г. №91 для профиля «Информатика и экономика».

Рабочая программа рассмотрена и одобрена на заседании кафедры Бизнес-информатики и информационных технологий 28.09.16 г., протокол № 2.

Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа одобрена методической комиссией института энергетики и автоматизированных систем 28.09.16 г., протокол № 1.

Председатель _____ С.И. Лукьянов

Рабочая программа составлена: доцентом кафедры БИ и ИТ, кандидатом педагогических наук, доцентом

_____ Е.В. Черновой

Рецензент: директор МОУ СОШ № 33, к.п.н. _____ И.В. Шмынева

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата. № протокола заседания кафедры	Подпись зав. кафедрой
1	8,9	Актуализация информационно-методического и информационного обеспечения дисциплины. Актуализация материально-технического обеспечения дисциплины	21.09.17, протокол № 2	
2	3,4,7,8,9	Корректировка РПД в соответствии с новым макетом (распоряжение № 10-39/75 от 21.09.2018 «О формировании и актуализации образовательных программ). Актуализация информационно-методического и информационного обеспечения дисциплины. Актуализация материально-технического обеспечения дисциплины	25.09.18, протокол № 2	
3	8,9	О формировании и актуализации образовательных программ. Актуализация информационно-методического и информационного обеспечения дисциплины. Актуализация материально-технического обеспечения дисциплины	02.09.19, протокол № 1	
4	8	Актуализация учебно-методического и информационного обеспечения дисциплины	31.08.20, протокол №1	

1 Цели освоения дисциплины

Сформировать у бакалавров теоретические знания по основам обеспечения охраны здоровья и жизни обучающихся при обращении с компьютерной техникой и программным обеспечением и, в особенности, в области применения различных сетевых технологий, а также практических навыков обеспечения защиты информации в системах обработки информации. Получить базовые знания, умения и навыки в области методов защиты информации для поддержки деятельности обучающихся в учебно-воспитательном процессе и внеурочной работе; для создания, формирования и администрирования электронных образовательных ресурсов с требуемым уровнем безопасности.

2 Место дисциплины в структуре образовательной программы подготовки бакалавра

Дисциплина «Методы и средства защиты информации» входит в вариативную часть блока 1 образовательной программы по направлению 44.03.05 «Педагогическое образование».

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения, полученных студентами в процессе изучения дисциплин «Теоретические основы информатики», «Программное обеспечение ЭВМ», «Компьютерные сети и интернет-технологии», «Информационные технологии в образовании», «Безопасность жизнедеятельности», «Основы медицинских знаний и здорового образа жизни».

Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для «Основы искусственного интеллекта», «Администрирование компьютерных сетей», «Предметно-ориентированные экономические информационные системы». «Информационная безопасность в системе открытого образования», «Документирование управленческой деятельности в сфере образования».

3 Компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения

В результате освоения дисциплины «Информационная безопасность в системе открытого образования» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
***ОК-7* – способностью использовать базовые правовые знания в различных сферах деятельности**	
Знать	– принципы работы с информацией на различных ресурсах, с учетом требований информационной безопасности*;*
Уметь	– соблюдать права интеллектуальной собственности на информацию;
Владеть	– навыками обеспечения защиты информации согласно существующему законодательству;
***ОПК-4* – готовностью к профессиональной деятельности в соответствии с нормативно-правовыми актами сферы образования**	
Знать	– содержание основных нормативно-правовых актов сферы образования в области соблюдения информационной безопасности;
Уметь	– применять на практике требования к обеспечению информационной безопасности и защиты информации из нормативно-правовых актов сферы образования;
Владеть	– профессиональным языком предметной области знания;

Структурный элемент компетенции	Планируемые результаты обучения
***ОПК-6* – готовностью к обеспечению охраны жизни и здоровья обучающихся**	
Знать	– сущность и общую характеристику информационных процессов информационного общества в аспекте обеспечения охраны жизни и здоровья обучающихся;
Уметь	– настраивать операционную систему и программные средства общего назначения с позиции требований обеспечения охраны жизни и здоровья обучающихся;
Владеть	– навыком применения средств и методов обеспечения охраны жизни и здоровья обучающихся в процессе работы с информационными технологиями;
ДПК-2 – способен использовать современные информационные и коммуникационные технологии для поддержки деятельности обучающихся в учебно-воспитательном процессе и внеурочной работе; для создания, формирования и администрирования электронных образовательных ресурсов	
Знать	– основные понятия и определения в области обеспечения информационной безопасности и защиты информации;
Уметь	– использовать методы и средства защиты информации от несанкционированного доступа;
Владеть	– навыками использования программных средств защиты информации от несанкционированного доступа;
***ПК-1* – готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов**	
Знать	– сущность и структуру образовательных программ по учебному предмету в соответствии с требованиями образовательных стандартов, с учетом требований защиты информации;
Уметь	– осуществлять анализ образовательных программ по учебному предмету на соответствие с требованиями нормативно-правовых актов по обеспечению защиты информации;
Владеть	– отдельными методами, приемами обучения при реализации образовательных программ по учебному предмету в соответствии с общими принципами соблюдения требований защиты информации;

4 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:
- контактная работа – 57,2 акад. часов:
  - аудиторная – 54 акад. часов;
  - внеаудиторная – 3,2 акад. часов
- самостоятельная работа – 51,1 акад. часов;
- подготовка к экзамену – 35,7 акад. часа

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
Раздел 1. Основы информационной безопасности и защиты информации								
1.1. Сущность и понятие информационной безопасности и защиты информации Основные понятия. Значение информационной безопасности для субъектов информационных отношений. Понятие и сущность защиты информации. Цели и концептуальные основы защиты информации. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой информации.	7	2	2		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 1 «Надежность и достоверность информации»	ОПК-4 – з ОПК-6 – зув
1.2. Правовое обеспечение информационной безопасности и защиты информации Назначение и структура правового обеспечения	7	2	4		10	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Тестирование Выступление на семинаре по ЛР2 «Законодательная и нормативно-правовая база	ОПК-4 – зув ОК-7 – зув

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
защиты информации. Методы правовой защиты информации. Правовая основа допуска и доступа персонала к защищаемым сведениям. Правовые основы защиты информации в организации. Понятие интеллектуальной собственности, ее виды и основные объекты образования. Международные и национальные стандарты и спецификации в области ИБ. Федеральные критерии безопасности информационных технологий. Профиль защиты. Назначение, структура и этапы разработки профиля защиты. Ядро безопасности. Современные стандарты в области управления рисками информационной безопасности.						Подготовка к семинарскому занятию по ЛР 2: проработка научно-методической литературы, доклад и презентация Подготовка к семинарскому занятию по ЛР 3: проработка научно-методической литературы, доклад и презентация	обеспечение информационной безопасности» Выступление на семинаре по ЛР3 «Стандарты и спецификации в области информационной безопасности»	
1.3. Виды и источники угроз информационной безопасности Угрозы информационной безопасности и защиты информации. Дестабилизирующее воздействие на защищаемую информацию. Классификация видов угроз информационной безопасности по различным признакам. Несанкционированный доступ к информации	7	2	4		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 4 «Классификация угроз предметной области»	ОПК-4 – зув ОПК-6 – зув ПК-1 – зув ДПК-2 – зув ОК-7 – зув
1.4. Классификация и характеристика основных методов и средств защиты Методы защиты информации. Способы защиты информации. Средства защиты	7	2	-		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Тестирование Эссе «Методы защиты информации предметной области»	ОПК-4 – з ОПК-6 –з ПК-1 – з

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
информации.								
Итого по разделу		**8**	**10**		**16**			
Раздел 2. Обеспечение информационной безопасности и защиты информации								
2.1. Административный уровень обеспечения ИБ Политика безопасности. Программа безопасности. Оценка рисков и базовый уровень защиты. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.	7	2	10		12	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 5: проработка научно-методической литературы, доклад и презентация Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование Выступление на семинаре по ЛР 5 «Политика информационной безопасности» ЛР 6 «Аудит защищенности сетей» ЛР 7 «Парольная защита и менеджеры паролей» ЛР 8 «Массовая рассылка писем»	ОПК-4 – зув ОПК-6 – зув ПК-1 – зув ДПК-2 – зув ОК-7 – зув
2.2. Программные средства защиты информации Защита программного обеспечения от несанкционированного доступа. Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации	7	2	8		10	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 9 «Защита от несанкционированного доступа к информации» ЛР 10 «Защита информации в документах» ЛР 11 «Удаление информации» ЛР 12 «Восстановление данных»	ОПК-4 – з ОПК-6 –з ПК-1 – з ДПК-2 – зув

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
2.3. Вирусы и антивирусные средства Определение компьютерных вирусов. Классификация компьютерных вирусов. Признаки заражения. Профилактика заражения. Программные антивирусные средства. Структура антивирусной программы. Принципы выбора сигнатуры компьютерного вируса.	7	2	4		3	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 13: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР 13 «Современные вредоносные программы для ПК и мобильных устройств»	ОПК-4 – зув ОПК-6 – зув ПК-1 – зув ОК-7 – зув
2.4. Криптографические методы защиты Методы криптографии. Средства криптографической защиты информации. Криптографические преобразования. Шифрование и дешифрование информации. Цифровая подпись.	7	2	4/2И		8,1	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию Выполнение заданий лабораторной работы	Тестирование ЛР 14 «Защита информации с помощью криптографии» ЛР 15 «Защита информации с помощью стеганографии»	ОПК-6 –з ПК-1 – з ОК-7 – зув
2.5. Технические средства защиты информации Инженерная защита объектов, защита информации от утечки по техническим каналам.	7	2	-		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Тестирование	ОПК-4 – з ОПК-6 –з ПК-1 – з
Итого по разделу		**10**	**26/2И**		**35,1**			
Итого за семестр		**18**	**36/2И**		**51,1**			

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
Итого по дисциплине		**18**	**36/2И**		**51,1**		**экзамен**	

5 Образовательные и информационные технологии

При проведении занятий и организации самостоятельной работы студентов используются:

Традиционные технологии обучения, предполагающие передачу информации в готовом виде, формирование учебных умений по образцу: лекция-изложение, лекция-объяснение, лабораторные работы, контрольная работа и др.

Использование традиционных технологий обеспечивает ориентирование студента в потоке информации, связанной с различными подходами к определению сущности, содержания, методов, форм развития и саморазвития личности; самоопределение в выборе оптимального пути и способов личностно-профессионального развития; систематизацию знаний, полученных студентами в процессе аудиторной и самостоятельной работы. Лабораторные занятия обеспечивают развитие и закрепление умений и навыков определения целей и задач саморазвития, а также принятия наиболее эффективных решений по их реализации.

Интерактивные формы обучения, предполагающие организацию обучения как продуктивной творческой деятельности в режиме взаимодействия студентов друг с другом и с преподавателем

Использование интерактивных образовательных технологий способствует повышению интереса и мотивации учащихся, активизации мыслительной деятельности и творческого потенциала студентов, делает более эффективным усвоение материала, позволяет индивидуализировать обучение и ввести экстренную коррекцию знаний.

При проведении лабораторных занятий используются групповая работа, технология коллективной творческой деятельности, технология сотрудничества, обсуждение проблемы в форме дискуссии. Данные технологии обеспечивают высокий уровень усвоения студентами знаний, эффективное и успешное овладение умениями и навыками в предметной области, формируют познавательную потребность и необходимость дальнейшего самообразования, позволяют активизировать исследовательскую деятельность, обеспечивают эффективный контроль усвоения знаний.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы и средства защиты информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа бакалавров включает в себя выполнение заданий лабораторных работ, представление результатов и оформление их в соответствии с. требованиями к оформлению СМК-О-СМГТУ-42-09 Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления.

Внеаудиторная самостоятельная работа студентов осуществляется в виде изучения учебной и научной литературы по соответствующему разделу с проработкой материала, участие в дистанционном курсе или изучении МООК, предложенном преподавателем и выполнения домашних заданий (подготовка к лабораторным работам) с консультациями преподавателя.

Лабораторная работа 1. Надежность и достоверность информации

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 2. Законодательная и нормативно-правовая база обеспечение информационной безопасности

1. Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Подготовьте доклад и презентацию по выбранной теме.

2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»

3. Презентация и доклад представляются на занятии.

Лабораторная работа 3. Стандарты и спецификации в области информационной безопасности

1. Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Подготовьте доклад и презентацию по выбранной теме.

2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»

3. Презентация и доклад представляются на занятии

Лабораторная работа 4. Классификация угроз предметной области

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Разработайте модель нарушителя и модель угроз ИБ для организации, предложенной преподавателем. Оформите отчет по лабораторной работе в соответствии с требованиями

Лабораторная работа 5. Политика информационной безопасности

1. Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Подготовьте доклад и презентацию по выбранной теме.

2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»

3. Презентация и доклад представляются на занятии.

Лабораторная работа 6. Аудит защищенности сетей

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 7. Парольная защита и менеджеры паролей

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 8. Массовая рассылка писем

Познакомьтесь с рекомендуемым программным средством. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 9. Защита от несанкционированного доступа к информации

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 10. Защита информации в документах

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 11. Удаление информации

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 12. Восстановление данных

Познакомьтесь с рекомендуемыми программными средствами. Выполните задания лабораторной работы в рекомендованных программных средствах или найденных самостоятельно, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 13. Современные вредоносные программы для ПК и мобильных устройств

1. Подготовить доклад и презентацию по выбранной теме.

2. Презентация загружается на портал, доклад сдается преподавателю в распечатанном виде, оформление в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления»

3. Презентация и доклад представляются на занятии.

Лабораторная работа 14. Защита информации с помощью криптографии

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Лабораторная работа 15. Защита информации с помощью стеганографии

Изучите рекомендуемую и дополнительную учебную и научную литературу, используйте источники, найденные самостоятельно. Выполните задания лабораторной работы, оформите отчет по лабораторной работе в соответствии с требованиями.

Эссе «Методы защиты информации предметной области»

Опишите методы защиты информации, которые необходимо применить на вашей предметной области из лабораторной работы 4.

7 Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОК-7 – способностью использовать базовые правовые знания в различных сферах деятельности		
Знать	– принципы работы с информацией на различных ресурсах, с учетом требований информационной безопасности*;*	**Примерные варианты тестовых заданий.** 1. Что такое безопасность данных? a. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение b. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное искажение c. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их преднамеренное получение, изменение или уничтожение d. состояние защищенности национальных интересов РФ во всех сферах человеческой деятельности 2. Что является целью защиты информации? a. защита информации от утечки b. желаемый результат защиты информации c. защита информации от утраты d. предотвращение утраты и утечки конфиденциальной информации **Перечень вопросов для подготовки к экзамену** 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности 3. Важность и сложность проблемы информационной безопасности 4. Законодательный уровень информационной безопасности 5. Обзор российского законодательства в области информационной безопасности 6. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности 7. Закон «Об информации, ИТ и защите информации» 8. Закон «О лицензировании отдельных видов деятельности» 9. Закон «Об электронной цифровой подписи»
Уметь	– соблюдать права интеллектуальной собственности на информацию;	**Практическое задание** 1. Студент 4-го курса технического ВУЗа Иванов И.И. написал в рамках курсовой работы компьютерную программу «TEST», позволяющую проводить тестирование остаточных знаний по ряду математических

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		дисциплин. Назовите объекты и субъекты авторского права. Кому принадлежат личные неимущественные и исключительные права на данное программное обеспечение (ПО)? Сотрудники фирмы «Аргус», специализирующейся в области создания компьютерных игр, разработали новую игру «BIBL», пользующуюся большим спросом. В разработке участвовали сотрудник Иванчук, разработавший алгоритм игры, и программисты Алюторцев и Чванов. Назовите объекты и субъекты авторского права по данной разработке? Кто является автором данной разработки? Кому принадлежат личные неимущественные и исключительные права? Какие права принадлежат фирме «Аргус»?
Владеть	– навыками обеспечения защиты информации согласно существующему законодательству;	**Комплексное задание** 1. Студенты 4-го курса университете Р. и Т. занимались распространением компакт-дисков с программами, предназначенными для снятия защиты с программных продуктов, а также “взломанных” версий программ. Чьи права в данном случае нарушены? Какие права нарушены? Какая ответственность и за какие нарушения возникает?
ОПК-4 – готовностью к профессиональной деятельности в соответствии с нормативно-правовыми актами сферы образования		
Знать	– содержание основных нормативно-правовых актов сферы образования в области соблюдения информационной безопасности;	**Примерные варианты тестовых заданий.** 1. Согласно рекомендациям X.800, целостность с восстановлением может быть реализована на: a. Сетевом уровне b. Транспортном уровне c. Прикладном уровне d. Логическом уровне 2. Требования «Общих критериев» группируются в: a. Классы b. Подклассы c. Группы d. Подгруппы **Перечень вопросов для подготовки к экзамену** 1. Обзор зарубежного законодательства в области информационной безопасности 2. Оценочные стандарты и технические спецификации. 3. Синхронизация программы безопасности с жизненным циклом систем
Уметь	– применять на практике требования к обеспечению информационной безопасности и защиты информации из нормативно-правовых актов сферы образования;	**Практическое задание** Разработать модель нарушителя для заданной организации

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Владеть	– профессиональным языком предметной области знания.	**Комплексное задание** На основе анализа ФЗ «Об образовании в РФ» (4 глава) подготовить свод ваших прав как обучающегося в высшем учебном заведении. Изучить Федеральный закон «Об образовании в РФ» (глава 5, статьи 47, 48) и внести в таблицу положения, касающиеся прав, обязанностей педагогических работников. Охарактеризовать профессиональный стандарт педагога как документ, характеризующий требования к квалификации.
ОПК-6 – готовностью к обеспечению охраны жизни и здоровья обучающихся		
Знать	– сущность и общую характеристику информационных процессов информационного общества в аспекте информационной безопасности;	**Примерные варианты тестовых заданий.** 1. Укажите некорректное определение нарушителя ИБ: a. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами b. физическое или юридическое лицо, случайно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами c. это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства 2. Что такое защищаемая информация? a. любая информация, которая появляется в СМИ b. информация, которая подлежит защите в соответствии с требованиями правовых документов и обязательно относится к государственной тайне c. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации **Перечень вопросов для подготовки к экзамену** 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности 3. Важность и сложность проблемы информационной безопасности 4. Основные определения и критерии классификации угроз 5. Наиболее распространенные угрозы доступности 6. Вредоносное программное обеспечение 7. Основные угрозы целостности 8. Основные угрозы конфиденциальности 9. Идентификация и аутентификация 10. Управление доступом

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		11. Ролевое управление доступом 12. Протоколирование и аудит 13. Шифрование 14. Экранирование 15. Классификация межсетевых экранов 16. Анализ защищенности 17. Доступность 18. Отказоустойчивость и зона риска 19. Криптография 20. Вредоносные программы и способы защиты от них 21. Подразделения технической защиты информации. 22. Место и роль аппаратно-программных средств защиты. 23. Требования руководящих документов к средствам защиты информации от несанкционированного доступа. 24. Обнаружение сетевой атаки. 25. Способы обеспечения безопасной работы в Интернет. 26. Принципы функционирования брандмауэров. 27. Перечень информационных ресурсов, подлежащих защите. 28. Основы безопасности web-ресурсов. 29. Способы защиты файлов от постороннего доступа. 30. Эргономические и нормативные требования к организации рабочего места пользователя 31. Вредоносное программное обеспечение. 32. Пути проникновения вредоносного программного обеспечения. *33.* Способы защиты от вредоносного программного обеспечения
Уметь	– настраивать операционную систему и программные средства общего назначения с позиции требований обеспечения охраны жизни и здоровья обучающихся;	**Практическое задание** Восстановить удаленную информацию Удалить информацию с заданными параметрами Защитить информацию: пароль, криптография, стеганография
Владеть	– навыком применения средств и методов обеспечения охраны жизни и здоровья обучающихся в процессе работы с информационными технологиями.	**Комплексное задание** Применять специализированное программное обеспечение для сохранения конфиденциальности информации: хранение паролей, удаление информации, сокрытие информации
ДПК-2 – способен использовать современные информационные и коммуникационные технологии для поддержки деятельности обучающихся в учебно-		

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
воспитательном процессе и внеурочной работе; для создания, формирования и администрирования электронных образовательных ресурсов		
Знать	– основные понятия и определения в области обеспечения информационной безопасности и защиты информации;	**Примерные варианты тестовых заданий.** 1. Главная цель мер, предпринимаемых на административном уровне: a. Сформировать программу безопасности и обеспечить ее выполнение b. Выполнить положения действующего законодательства c. Отчитаться перед вышестоящими инстанциями d. Выявление критически важных функций организации 2. В число принципов управления персоналом входят: a. Минимизация привилегий b. Минимизация зарплаты c. Максимизация привилегий **Перечень вопросов для подготовки к экзамену** 1. Управление рисками 2. Основные классы мер процедурного уровня 3. Управление персоналом 4. Физическая защита 5. Поддержание работоспособности 6. Реагирование на нарушения режима безопасности 7. Основные понятия программно-технического уровня информационной безопасности 8. Особенности современных информационных систем, существенные с точки зрения безопасности 9. Понятие и сущность защиты информации. 10. Объекты защиты информации. 11. Средства защиты информации. 12. Методы защиты информации.
Уметь	– использовать методы и средства защиты информации от несанкционированного доступа;	**Практическое задание** Сформировать пароль с заданными критериями устойчивости Рассчитать устойчивость пароля
Владеть	– навыками использования программных средств защиты информации от несанкционированного доступа;	**Комплексное задание** Обеспечить защиту информации документов различного типа
ПК-1 – готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов		
Знать	– сущность и структуру образовательных программ по учебному предмету в соответ-	**Перечень вопросов для подготовки к экзамену** 1. Вопросы защиты информации в образовательных программах по информатике для школы

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	ствии с требованиями образовательных стандартов, с учетом требований защиты информации;	2. Вопросы защиты информации в образовательных программах по информатике для внеурочной деятельности
Уметь	– осуществлять анализ образовательных программ по учебному предмету на соответствие с требованиями нормативно-правовых актов по обеспечению защиты информации;	**Практическое задание** Охарактеризовать учебные пособия по информатике для школьников с точки зрения соответствия требований нормативно-правовых актов по обеспечению защиты информации
Владеть	– отдельными методами, приемами обучения при реализации образовательных программ по учебному предмету в соответствии с общими принципами соблюдения требований защиты информации;	**Комплексное задание** Подобрать дидактические инструменты для обучения школьников методам и средствам защиты информации, согласно ООП для школы, внеурочной деятельности и дополнительного образования

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Методы и средства защиты информации» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Экзамен по данной дисциплине проводится в устной форме по экзаменационным билетам, каждый из которых включает один теоретический вопрос и одно практическое задание.

Показатели и критерии оценивания экзамена:

«Отлично» – оценка знаний бакалавра, который свободно владеет:

1) понятийно-терминологической базой дисциплины и знает значение наиболее часто используемых аббревиатур;

2) четко увязывает теоретическое познание дисциплины с реальной практикой;

3) знаком с широким кругом литературных источников, знает, где их достать, хорошо разбирается в истории становления дисциплины, в оценке ее текущего состояния и перспектив ее развития;

4) полностью владеет материалом практического задания, четко и аргументировано защищает его положительные результаты, обосновано комментирует и объясняет допущенные недочеты.

«Хорошо» – оценка знаний бакалавра, который владеет понятийно-терминологической базой дисциплины, может увязать теоретическое познание дисциплины с реальной практикой. Владеет материалом практического задания, показал способность к объяснению смысла основных положений;

«Удовлетворительно» – оценка знаний бакалавра, который в большей части владеет, с небольшими изъянами, понятийно-терминологической базой дисциплины, имеет представление о внутренней логике дисциплины, представленной в виде учебной программы, Владеет, но неуверенно, материалом практического задания.

«Неудовлетворительно» – оценка знаний бакалавра, который не владеет понятийно-терминологической базой дисциплины и материалом практического задания.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-450371

2. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2019.– 223 с. – (Высшее образование: Бакалавриат). – www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. – Текст : электронный. – URL: https://znanium.com/read?id=342244

б) Дополнительная литература:

1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-cheloveka-449350

2. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР: ИНФРА-М, 2019. – 400 с. – (Высшее образование). – DOI: https://doi.org/10.12737/1759-3 – Текст : электронный. – URL: https://znanium.com/read?id=339378

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/prestupleniya-v-sfere-informacionnoy-bezopasnosti-448295

в) Методические указания:

1. Методические указания по выполнению лабораторной работы «Надежность и достоверность информации» для бакалавров направления 38.03.05 Бизнес-информатика, 09.03.03 «Прикладная информатика», 44.03.05 «Педагогическое образование (Информатика и экономика)». – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – 12 с.

2. Методические указания по выполнению лабораторных работ по дисциплине «Методы и средства защиты информации» для бакалавров направления 44.03.05 «Педагогическое образование (Информатика и экономика)». – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – 30 с.

г) Программное обеспечение и Интернет-ресурсы:

Лицензионное программное обеспечение:

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 (подписка Imagine Premium)	Д-1227 от 8.10.2018	11.10.2021
MS Windows 10 (подписка Imagine Premium)	Д-1227 от 8.10.2018	11.10.2021
MS Office 2007	№ 135 от 17.09.2007	бессрочная
FAR Manager	свободно распространяемое ПО	бессрочная

7Zip	свободно распространяемое	бессрочная
Lpro	GNU GPL v3	бессрочная
GlassWire	free (бесплатная)	бессрочная
Генератор паролей 1.5	FreeWare	бессрочная
KeePass Password Safe	GNU General Public License	бессрочная
Thunderbird	MPL v1.1/GPL v3/LGPL v3	бессрочная
Recuva	бесплатно	бессрочная
Alternate File Shredder	FreeWare	бессрочная
HDD Low Level Format Tool	FreeWare	бессрочная
Шифратор «Решетка Кардано»	бесплатно	бессрочная
S-Tools	Freeware	бессрочная
Mozilla Firefox для Windows	Mozilla Public License, version 2.0, GNU GPL и GNU LGPL	бессрочная

Интернет-ресурсы:

1. Портал научной электронной библиотеки – URL: http://elibrary.ru/defaultx.asp
2. Электронный фонд правовой и нормативной документации. – URL: http://docs.cntd.ru
3. Справочная правовая система «Консультант плюс» – URL: http://www.consultant.ru/
4. Справочная правовая система «Гарант» – URL: http://www.garant.ru/
5. Positive Hack Days – URL: https://www.phdays.com/ru/
6. Информационная безопасность. Защита данных – URL: https://habr.com/ru/hub/infosecurity/
7. Сервис генерации паролей с заданными требованиями – URL: https://genpas.peter23.com/
8. Сервис проверки пароля на устойчивость ко взлому – URL: https://exploit.in/passcheck/
9. Сервис проверки логина и пароля по базе взломанных паролей – URL: https://haveibeenpwned.com/Passwords
10. Онлайн менеджер паролей – URL: https://passgenerator.ru/menedzher-paroley
11. Сервис генерации токенов – URL: https://www.stationx.net/canary/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Учебные аудитории для проведения занятий лекционного типа	Персональный компьютер (или ноутбук) с пакетом MS Office с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета. Мультимедийный проектор, экран. Мультимедийные презентации к лекциям, учебно-наглядные пособия
Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Персональные компьютеры с пакетом MSOffice, операционной системой MS Windows и выходом в Интернет Требуемое ПО, приведенное в таблице «Лицензионное программное обеспечение»
Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки	Персональные компьютеры с пакетом MS Office, операционной системой MS Windows, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета
Аудитория для хранения и профилактического обслуживания учебного оборудования	Мебель для хранения и обслуживания оборудования (шкафы, столы), учебно-методические материалы, стеллажи для хранения учебно-наглядных пособий и учебно-методической документации.