МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

Павловский филиал ННГУ

УТВЕРЖДАЮ:

Директор Павловского филиала ННГУ

_____Н.А. Ягунова

«31»__08___2018 г.

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

38.03.01 ЭКОНОМИКА

Направленность (профиль) образовательной программы

ЭКОНОМИКА ПРЕДПРИЯТИЙ И ОРГАНИЗАЦИЙ

Квалификация

БАКАЛАВР

Форма обучения

ЗАОЧНАЯ

Павлово

2018

1. Место и цели дисциплины (модуля) в структуре ОПОП

Дисциплина относится к базовой части Блока 1 «Дисциплины, модули» и является обязательной для изучения по направлению подготовки 38.03.01 Экономика.

Трудоемкость дисциплины составляет 2 зачетные единицы.

Целью учебной дисциплины «Информационная безопасность» состоит в эффективном освоении теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников).

Формируемые компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ОПК-1базовый уровень способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** основные методы, способы и средства преобразования информации **Уметь:** работать с компьютером как средством управления информацией **Владеть:** основными способами обнаружения информационных угроз и использования современных антивирусных программ
ПК-8базовыйуровень Способность использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии	**Знать:** современные технические средства и информационные технологии **Уметь:** использовать современные технические средства и информационные технологиидля решения аналитических и исследовательских задач **Владеть:** методами современных технических средств и информационных технологий
ПК-10 начальный уровень Способность использовать для решения коммуникативных задач современные технические средства и информационные технологии	**Знать:** теоретические аспекты информационной безопасности (ИБ) экономических систем типы информационных угроз и их характеристики организацию системы защиты информации экономических систем **Уметь:** формулировать цели и задачи защиты информации экономических объектов принимать обоснованные решения по выбору политики безопасности и оценке эффективности инвестиций в ИБ работать в среде специализированных программных комплексов и систем, применяемых в ИБ **Владеть:** методами развития комплексов и технологий ИБ подходами к организации ИБ экономических систем.

3. Структура и содержание дисциплины (модуля)

Объем дисциплины для заочной формы обучения составляет 2 зачетные единицы, всего 72 часа, из которых 11 часов составляет контактная работа обучающегося с преподавателем (4 часа занятия лекционного типа, 6 часов занятия семинарского, 1 час – КСР), 4 часа – контроль, 57 часов составляет самостоятельная работа обучающегося.

Объем дисциплины для заочной (ускоренной) формы обучения составляет 2 зачетные единицы, всего 72 часа, из которых 9 часов составляет контактная работа обучающегося с преподавателем (2 часа занятия лекционного типа, 6 часов занятия семинарского типа, 1 час – КСР), 4 часа – контроль, 59 часов составляет самостоятельная работа обучающегося.

Структура и содержание дисциплины (модуля)

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)			В том числе											
				Контактная работа (работа во взаимодействии с преподавателем), часы, из них									Самостоятельная работа обучающегося, часы		
				Занятия лекционного типа			Занятия семинарского типа			Всего					
	Очная	Заочная	Заочная (У)	Очная	Заочная	Заочная (У)	Очная	Заочная	Заочная (У)	Очная	Заочная	Заочная (У)	Очная	Заочная	Заочная (У)
Тема 1. Введение в информационную безопасность		8	8		1	1		1	1		2	2		6	6
Тема 2. Угрозы информационной безопасности		11	13			1		1	1		1	2		10	11
Тема 3. Программно-технические методы защиты информации		11	12		1			1	1		2	1		9	11
Тема 4. Менеджмент и аудит информационной безопасности на уровне предприятия		12	12					1	1		1	1		11	11
Тема 5. Управление рисками информационной безопасности		13	11		1			1	1		2	1		11	10
Тема 6. Управление информационной безопасностью на государственном уровне		12	11		1			1	1		2	1		10	10
КСР		1	1								1	1			
Контроль		4	4												
Промежуточная аттестация зачет															

Тема 1. Введение в информационную безопасность

Понятие безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Безопасность в экономической сфере России. Цели экономической безопасности, ее содержание и структура. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. Соперничество в информационной сфере, информационные войны. Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности.

Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. Место, цели и задачи информационной безопасности в бизнесе. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы

защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения. Соотношение понятий информационной безопасности и безопасности информации. Взаимосвязь понятий информационной безопасности и защиты информации. Научные взгляды, теории и дискуссии. Концепция защиты информации. Понятие и цели защиты информации, формирование и эволюция понятия. Обеспечивающий технологический аспект защиты информации.

Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Правовое двуединство документированных информационных ресурсов. Понятие ценной (собственной) предпринимательской информации. Ценность и полезность информации. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации. Понятие уязвимости информации. Типовые классификационные группы ценной предпринимательской информации. Информационные ресурсы государственные и негосударственные. Классификация информационных продуктов и услуг. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования.

Тема 2. Угрозы информационной безопасности

Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкуренции. Промышленный и экономический шпионаж, его сущность, история и сфера распространения. Легальные способы получения ценной и конфиденциальной информации, их состав. Нелегальные (противоправные, незаконные) способы получения ценной и конфиденциальной информации, их состав. Понятия злоумышленника, постороннего и случайного лица.

Понятие и классификация источников конфиденциальной информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Характеристика каждого канала. Уязвимость информации. Интерес к информации как предпосылка возникновения угрозы. Понятие угрозы (опасности) информации, виды угроз. Риск угрозы и механизм реализации угрозы. Понятие несанкционированного канала утраты конфиденциальной информации. Случайные и преднамеренные условия возникновения этого канала. Поиск или формирование такого канала злоумышленником. Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. Характеристика каждого канала. Классификация технических каналов утечки конфиденциальной информации. Характеристика каждого канала. Комплексность использования организационных и технических каналов. Особенности структуры каналов распространения информации в компьютерах, локальных сетях, оргтехнике и средствах связи.

Назначение и классификация технических средств промышленного шпионажа. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений.

Тема 3. Программно-технические методы защиты информации

Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасности. Международные критерии. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ.

Тема 4. Менеджмент и аудит информационной безопасности на уровне предприятия

Понятие, цели и задачи системы защиты конфиденциальной информации. Принципы построения системы, ее технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принцип коллегиальности контроля. Принципы надежности и превентивности. Принцип эволюции структуры системы в условиях реальных угроз информации. Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской информации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях. Комплексность системы защиты. Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Разработка и ведение перечня сведений, составляющих предпринимательскую тайну. Цели и задачи перечня сведений, составляющих предпринимательскую тайну. Состав сведений, которые не могут быть тайной. Место перечня в системе защиты информации. Классификация ценной информации в предпринимательских структурах различного типа. Принципы определения состава ценных сведений, подлежащих защите в конкретной фирме. Перечни инвентарные и матричные. Структура перечней различных типов. Перечни списочные и проблемно-ориентированные. Организационные формы составления и ведения перечней. Содержание процедуры разработки перечня. Существующие методики сбора, анализа и обобщения сведений. Место маркетингового исследования в процедуре разработки перечня. Разграничение уровня конфиденциальности сведений, определение срока конфиденциальности, регламентация места документирования, использования и хранения, состава сотрудников, которым эти сведения необходимы для работы.

Назначение нормативно-методических материалов по регламентации системы защиты информации. Регламентация права предпринимательской структуры на защиту своей тайны. Регламентация структуры и содержания комплексной системы защиты инфор-

мации фирмы. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала фирмы с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны фирмы. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и иных наглядных пособий.

Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая структура службы безопасности. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Задачи и функции аналитического подразделения. Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе. Профессиональные и психологические требования к сотрудникам службы безопасности. Плановая и контрольная работа в службе безопасности. Назначение и взаимосвязь плановой и контрольной работы службы безопасности. Их место в построении и функционировании комплексной системы защиты информации фирмы. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций.

Тема 5. Управление рисками информационной безопасности

Основные принципы управления рисками информационной безопасности:

Шестнадцать методов, используемые для реализации пяти принципов управления рисками. Оценка риска и определение потребности. Признание информационных ресурсов в качестве существенных (неотъемлемых) активов организации. Разработка практических процедур оценки рисков, связывающих безопасность и требования бизнеса. Ответственность менеджеров бизнес-подразделений и менеджеров, участвующих в программе обеспечения безопасности. Непрерывное управление рисками. Централизованное управление. Определение бюджета и персонала. Профессионализм и технические знания сотрудников. Средства контроля. Контроль факторов, влияющих на риски и указывающих на эффективность информационной безопасности. Новые методы и средства контроля.

Тема 6. Управление информационной безопасностью на государственном уровне

Защита информации институтом интеллектуальной собственности. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Объекты интеллектуальной собственности. Промышленная собственность. Промышленные образцы. Информация о происхождения товара. Собственность на результаты творческого труда. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Реализация интеллектуальной собственности на документированную информацию. Характеристика норм патентного права. Характеристика норм авторского права и смежных прав. Торговый знак, знак обслуживания, торговая марка, фирменное наименование, эмблема предприятия. Страхование ценной информации. Законодательные акты,охраняющие вещную собственность на документированную информацию. Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации. Организация деятельности средств массовой информации. Отношения средств массовой информации с гражда-

нами и организациями. Ответственность за нарушение законодательства о средствах массовой информации.

Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Распоряжение сведениями, составляющими государственную тайну. Рассекречивание сведений и их носителей. Защита государственной тайны. Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной предпринимательской информации. Производственная тайна. Служебная тайна. Профессиональная тайна. Банковская тайна. Тайны личная и семейная. Понятия - "фирменные секреты", "технологические секреты (ноу-хау)", "научные секреты (ноу-ноу)". Документированная информация (документы) секретная и несекретная. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Сущность термина, особенности и условия применения, дискуссионность. Правовые и технологические аспекты присвоения информации категории конфиденциальной. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциального документа, его особенности. Общая классификация конфиденциальных документов. Сроки (период) конфиденциальности. Деление документов на документы кратковременного и долговременного периода конфиденциальности. Конфиденциальность информации в вычислительных системах и сетях.

4. Образовательные технологии

Реализация компетентностного подхода при изучении дисциплины предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, государственных и муниципальных органов.

Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Тематика практических заданий ориентирована на рассмотрение аналитических типовых и исследовательских задач финансово-экономического характера.

В ходе самостоятельной работы, при подготовке к плановым занятиям, зачету студенты анализируют поставленные преподавателем задачи и проблемы и с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет, находят пути их разрешения.

5. Учебно- методическое обеспечение самостоятельной работы обучающихся

5.1.Рекомендации преподавателю

В ходе изучения дисциплины уделяется внимание как теоретическому усвоению понятий информационной безопасности, так и приобретению, развитию и закреплению практических навыков и умений по использованию специализированных информационных средств и технологий при организации ИБ экономических систем.

На лекциях раскрываются основные вопросы рассматриваемой темы, делаются акценты на наиболее важные, сложные и проблемные положения изучаемого материала, которые должны быть приняты студентами во внимание.

На практических занятиях, ориентированных на предметную область будущей профессиональной деятельности студентов, выборочно контролируется степень усвоения студентами основных теоретических положений. Рассматривается технология применения аппаратно-программных средств для организации ИБ. При решении практических заданий используются не только инструментальные средства информационных технологий бизнес-индустрии, но и методы и понятия дисциплин финансово-экономического блока.

После изучения каждой темы предусматривается выполнение студентами самостоятельной работы с проверкой как степени усвоения ими теоретических знаний, так и объема и качества приобретенных практических навыков и умений.

5.2. Рекомендации студентам

Для лучшего усвоения положений дисциплины студенты должны:

- постоянно и систематически, с использованием рекомендованной литературы и электронных источников информации, закреплять знания, полученные на лекциях;
- находить решения проблемных вопросов, поставленных преподавателем в ходе лекций и практических заданий;
- регулярно и своевременно изучать материал, выданный преподавателем на самостоятельную проработку;
- с использованием средств информационных систем, комплексов и технологий, электронных учебников и практикумов, справочных правовых и тренинго-тестирующих систем, информационных ресурсов сети Интернет выполнить на компьютере тематические практические задания, предназначенные для самостоятельной работы;
- находить, используя разные источники информации, ответы на теоретические и практические контрольные вопросы по темам дисциплины;
- использовать информацию, найденную на сайтах фирм–разработчиков информационных систем и технологий, применяемых в экономике;
- при подготовке к зачету учитывать общие требования и рекомендации.

При освоении данного курса бакалаврам может быть предложено выполнение инициативной научно-исследовательской работы.

Перечень контрольных вопросов к зачету

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.

10. Описать причины возникновения каналов несанкционированного доступа к информации.

11. Классифицировать виды каналов несанкционированного доступа к информации.

12. Описать характер действия организационных каналов несанкционированного доступа к информации.

13. Охарактеризовать технические каналы несанкционированного доступа к информации.

14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.

15. Проанализировать особенности угроз автоматизированным информационным системам.

16. Дать классификацию удаленных атак.

17. Проанализировать основные направления правовой защиты информации.

18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.

19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.

20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.

21. Определить объекты защиты авторских прав.

22. Назвать основные права автора в отношении его произведения.

23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).

25. Дать определение государственной тайны и назвать грифы секретности.

26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.

28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.

32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

33. Назвать основные положения концепции информационной безопасности предприятия.

34. Изложить содержание регламента обеспечения информационной безопасности предприятия.

35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

37. Проанализировать содержание понятия разрешительнойсистемы доступа персонала к конфиденциальным сведениям фирмы.

38. Обосновать критерии выделения конфиденциальных документов из общего по-

тока поступающих документов.

39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

42. Проанализировать особенности текста конфиденциального документа.

43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.

44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

45. Сформулировать возможности, трудности и направления использованияэлектронной почты для передачи конфиденциальных документов.

46. Составить фрагмент номенклатуры дел, содержащих конфиденциальныедокументы.

47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.

48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.

49. Проанализировать пути поиска документов и дел, не обнаруженных припроверке их наличия, дать рекомендации, повышающие эффективностьпоиска и предотвращающие утрату документов и дел.

50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.

51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. .

52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.

53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

54. Назвать основные элементы физической защиты территории и помещений предприятия.

55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.

56. Дать классификацию компьютерных вирусов.

57. Описать основные антивирусные программы.

58. Охарактеризовать основные способы криптографического преобразования данных.

6. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),включающий:

6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикаторы компетенции	**ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**	
	Не зачтено	**Зачтено**
Знания	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок
Умения	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.
Навыки	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 50 %	51-100 %

ПК-8способность использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии

Индикаторы компетенции	**ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**	
	Не зачтено	**Зачтено**
Знания	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок
Умения	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.
Навыки	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 50 %	51-100 %

ПК-10: Способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Индикаторы компе-	**ОЦЕНКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**

тенции	Не зачтено	Зачтено
Знания	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок
Умения	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.
Навыки	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 50 %	51-100 %

6.2. Описание шкал оценивания

Итоговый контроль качества усвоения студентами содержания курса проводится в виде зачета. На зачете определяется:

- уровень усвоения студентами основного учебного материала по дисциплине;
- уровень понимания студентами изученного материала;
- способности студентов использовать полученные знания для решения конкретных задач.

Зачет проводится в устной форме. Устная часть зачета заключается в ответе студентом на теоретические вопроса курса (с предварительной подготовкой) и последующем собеседовании в рамках тематики курса. Собеседование проводится в форме вопросов, на которые студент должен дать краткий ответ.

Критерии оценки знаний при сдаче зачета

Оценка	Уровень подготовки
Зачет	Хороший уровень подготовки, ответ на все основные пункты вопроса изложен в полном объеме и грамотно, возможны некоторые недочеты (неточности при изложении теоретического материала, нет четкости при формулировке определений, допущены несущественные ошибки в формулировках различного рода понятий и т.д.).
Незачет	Крайне низкий уровень подготовки, не изложены основные положения теории; студент не в состоянии изложить основные положения курсов дисциплин специальности; допущены существенные ошибки в формулировках базовых экономических понятий

6.3. Критерии и процедуры оценивания результатов обучения по дисциплине (модулю), характеризующих этапы формирования компетенций

По дисциплине «Информационная безопасность» предусмотрены разные формы контроля и оценки знаний, навыков и умений студентов. Текущий контроль успеваемости студентов осуществляется в ходе практических занятий, при выполнении и оценке самостоятельных заданий, по результатам тематического тестирования.

Критерии оценки тестов

«превосходно» - 96-100% правильных ответов;
«отлично» – 86-95% правильных ответов;
«очень хорошо» - 81-85% правильных ответов;
«хорошо» – 66-80% правильных ответов;
«удовлетворительно» – 56-65% правильных ответов.
«неудовлетворительно» - 46-55% правильных ответов;
«плохо» - 45% и меньше правильных ответов.

Описание шкалы оценивания для выполненных разноуровневых заданий и задач

Оценка	Критерии оценивания
Превосходно	Студент демонстрирует полные и глубокие знания теоретического материала курса, уверенно применяет полученные знания на практике, приобрёл умение быстро ориентироваться в содержании материала, понимает и умеет логично и последовательно разъяснить смысл своего ответа, доказать необходимость использования тех или иных теоретических положений, аргументированно и корректно отстаивает свою позицию, во всех случаях способен предложить альтернативные варианты решения проблемы.
Отлично	Студент демонстрирует полные и глубокие знания теоретического материала курса, уверенно применяет полученные знания на практике, приобрёл умение быстро ориентироваться в содержании материала, понимает и умеет логично и последовательно разъяснить смысл своего ответа, доказать необходимость использования тех или иных теоретических положений, аргументированно и корректно отстаивает свою позицию, в более чем 50% случаев способен предложить альтернативные варианты решения проблемы.
Очень хорошо	Студент демонстрирует знание теоретического материала, но применение теоретических положений на практике вызывает несущественные затруднения, связанные с аргументацией своей позиции. Обучающийся в полной мере понимает суть проблемы. Основные требования к заданию выполнены. В более чем 50% случаев способен предложить альтернативные варианты решения проблемы.
Хорошо	Студент демонстрирует знание теоретического материала, но применение теоретических положений на практике вызывает некоторые затруднения, связанные с аргументацией своей позиции. Обучающийся в полной мере понимает суть проблемы. Основные требования к заданию выполнены. В принципе способен предложить альтернативные варианты решения проблемы.
Удовлетворительно	Студент обладает знанием необходимого минимума теоретического материала, способен дать ответ не менее, чем на 50% поставленных заданий, но не способен аргументированно излагать свою позицию, не видит альтернативных вариантов разрешения проблемной ситуации, не может последовательно изложить суть решения.
Неудовлетворительно	Студент не обладает знанием требуемым объёмом знаний теоретического материала, способен дать ответ менее, чем на 50% поставленных заданий, не способен аргументированно излагать свою позицию, не видит альтернативных вариантов разрешения проблемной ситуации, не может последовательно изложить суть решения.
Плохо	Студент не обладает требуемым объёмом знаний теоретического материала и не может решить практическое задание.

6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.

Примеры тестовых заданий

Тесты для оценки компетенций (ПК-8,10)

Тест 1

1. Информационная война – это…

А. злословие в адрес другого человека;

Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

В. акт применения информационного оружия.

2. Информационная безопасность – это…

А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:

А. природоохранные мероприятия;

Б. надежность работы компьютера;

В. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:

А. информационные ресурсы;

Б. средства вычислительной и организационной техники;

В. Конституция России.

5. Обеспечение безопасности информации – это…

А. одноразовое мероприятие;

Б. комплексное использование всего арсенала имеющихся средств защиты;

В. разработка каждой службой плановых мер по защите информации.

6. Лингвистическое обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;

В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

7. Эргономическое обеспечение информационной безопасности – это?

А. антивирусные программы;

Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;

В. комплекс математических методов, связанных с оценкой опасности технических средств.

8.Информационное обеспечение информационной безопасности – это?

А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

Б. антивирусные программы;

В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

9. Организационное обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. совокупность средств;

В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:

А. раскрытие конфиденциальной информации;

Б. нарушение принципов экономической безопасности;

В. отказ от обслуживания.

11. Информационное оружие – это?

А. комплекс технических средств, методов и технологий, направленных против управленческих систем;

Б. нормативно-правовая база по информационной безопасности;

В. комплекс индивидуального и общественного сознания.

12. Правовое обеспечение информационной безопасности – это..?

А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;

Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;

В. широкое использование технических средств защиты информации.

Пример разноуровневых задач и заданий:

1.Защита информации от сбоев оборудования и случайной потери

1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»

2. Определите методы защиты

1 периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);

2 автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.

3 периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ. Например: DiskDoctor, ScanDisk . Подобные программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.

4 периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.

Определите методы защиты от случайной потери или искажения информации, хранящейся в компьютере:

1 автоматический запрос на подтверждение команды, приводящей к изменению содержимого какого-либо файла. Если вы хотите удалить файл или разместить новый файл под именем уже существующего, на экране дисплея появится диалоговое окно с требованием подтверждения команды либо её отмены;

2 установка специальных атрибутов документов. Например, многие программы-редакторы позволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;

3 возможность отменить последние действия. Если вы редактируете документ, то можете пользоваться функцией отмены последнего действия или группы действий, имеющейся во всех современных редакторах. Если вы ошибочно удалили нужный файл, то специальные программы позволяют его восстановить, правда, только в том случае, когда вы ничего не успели записать поверх удаленного файла;

4 разграничение доступа пользователей к ресурсам файловой системы, строгому разделению системного и пользовательского режимов работы вычислительной системы.

6.5. Методические материалы, определяющие процедуры оценивания.

С целью определения уровня овладения компетенциями, закрепленными за дисциплиной, в заданные преподавателем сроки проводится текущий и промежуточный контроль знаний, умений и навыков каждого обучающегося. Все виды текущего контроля осуществляются на занятиях семинарского типа, практических занятиях. Исклю-

чение составляет устный опрос, который может проводиться в начале или конце лекционного занятия в течение 15-20 мин. с целью закрепления знаний терминологии по дисциплине.

Процедура оценивания компетенций обучающихся основана на следующих принципах:

1. Периодичность проведения оценки.

2. Многоступенчатость: оценка (как преподавателем, так и студентами группы) и самооценка обучающегося, обсуждение результатов и комплекс мер по устранению недостатков.

3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.

Основное требование к организации системы оценивания и структуры оценочных средств в отношении компетенций как предмета контроля результатов обучения – это требование измеримости.

Достоверность и сопоставимость оценок достигается за счет учета следующих факторов:

- дидактико-диалектической взаимосвязи результатов образования и компетенций;
- формирование и развитие компетенций через усвоение содержания образовательных программ, самой образовательной средой вуза и используемыми образовательными технологиями;
- необходимость оценивания компетенций в квазиреальной деятельности при условии максимального приближения к ситуации будущей практики;
- использование индивидуальных и групповых оценок, взаимооценки;
- анализ достижений по итогам оценивания с выявлением положительных и отрицательных индивидуальных и групповых результатов и направлений развития.

Промежуточная аттестация по дисциплине проводится в форме зачета.

Зачет выставляется по итогам успешного выполнения заданий текущего контроля. Для получения зачета необходимо выполнить все задания текущего контроля в соответствующем семестре на оценку не менее чем «удовлетворительно».

Уровень знаний обучающихся определяется следующими оценками: «зачтено», «не зачтено».

Условиями оценивания результатов освоения дисциплины являются:

- валидность (объекты оценки должны соответствовать поставленным целям обучения);
- полнота и адекватность отображения требований образовательного стандарта и ОПОП;
- надежность (использование единообразных стандартов и критериев оценивания);
- справедливость (разные студенты должны иметь равные возможности добиться успеха);
- эффективность (не отнимать много времени у студентов и преподавателей);
- обеспечение решения оценочной задачи.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература

1. Баранова Е. КИнформационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с

(Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=495249)

2. Глинская Е.В.Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. – Режим доступа: (Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=507334

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2017. - 239 с. – (Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=612572)

Дополнительная литература

1. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.(Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=405000)

2. Вдовенко Л.А.Информационная система предприятия: Учебное пособие/Вдовенко Л. А., 2-е изд., пераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с.(Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=501089)

3. Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с. – (Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=471787)

4. Ерохин В.В Безопасность информационных систем [Электронный ресурс] / Ерохин В.В. - М. : ФЛИНТА, 2015. – 182 с.(Доступно в ЭБС «Консультант студента», режим доступа: (http://www.studentlibrary.ru/book/ISBN9785976519046.html)

5. Шаньгин В.Ф.Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. 702 с. (Доступно в ЭБС «Консультант студента», режим доступа: http://www.studentlibrary.ru/book/ISBN9785940747680.html)

Программное обеспечение и Интернет-ресурсы

1. Операционная система MicrosoftWindows
2. Пакет прикладных программ MicrosoftOffice
3. Правовая система «Консультант плюс»
4. Правовая система «Гарант»
5. Фонд образовательных электронных ресурсов ННГУ [Электронный ресурс]. - Режим доступа: http://www.unn.ru/books/resources — Загл. с экрана. [Дата обращения: 26.08.2017]
6. Электронная библиотека учебников[Электронный ресурс]. - Режим доступа: http://studentam.net— Загл. с экрана.[Дата обращения: 26.08.2017]
7. Российская государственная библиотека [Электронный ресурс]. - Режим доступа: http://www.rsl.ru— Загл. с экрана.[Дата обращения: 26.08.2017]
8. Научная электронная библиотека[Электронный ресурс]. - Режим доступа: http://elibrary.ru/— Загл. с экрана.[Дата обращения: 26.08.2017]

8. Материально- техническое обеспечение дисциплины (модуля)

Реализация программы предполагает наличие:

- аудиторий для лекционных и практических занятий с необходимым оборудованием;

- компьютерного класса, имеющего компьютеры, объединенные сетью с выходом в Интернет;

- лицензионного (операционная система MicrosoftWindows, пакет прикладных программ MicrosoftOffice) и свободно распространяемого программного обеспечения.

В ходе проведения занятий рекомендуется использовать компьютерные иллюстрации для поддержки различных видов занятий, подготовленные с использованием MicrosoftOffice или других средств визуализации материала.

Доступ к электронным информационным ресурсам осуществляется в компьютерном классе и библиотеке филиала.

Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала определяется рабочей учебной программой дисциплины, включенными в нее календарным планом изучения дисциплины и перечнем литературы; рекомендуется при подготовке к занятиям повторить материал предшествующих тем рабочего учебного плана, а также материал предшествующих учебных дисциплин, который служит базой изучаемого раздела данной дисциплины. *При подготовке к практическому занятию* необходимо изучить материалы лекции, рекомендованную литературу. Изученный материал следует проанализировать в соответствии с планом занятия, затем проверить степень усвоения содержания вопросов.

Практические занятия неразрывно связаны с домашними заданиями как основным видом текущей самостоятельной работы, являясь, в сочетании с систематическим изучением теоретического материала основой рейтинговой оценки знаний, фиксируемой в промежуточной аттестации.

Самостоятельная работа проводится с целью углубления знаний по дисциплине и предусматривает:

- повторение пройденного учебного материала, чтение рекомендованной литературы;
- подготовку к практическим занятиям;
- выполнение общих и индивидуальных домашних заданий;
- работу с электронными источниками;
- подготовку к сдаче формы промежуточной аттестации.

Планирование времени на самостоятельную работу важно осуществлять на весь семестр, предусматривая при этом повторение пройденного материала.

Важную роль в изучении дисциплины играет *подготовка контрольной или курсовойработы* (при наличии в учебном плане). Прежде чем приступить к написанию работы, следует внимательно ознакомиться с темой и рекомендованной литературой. Целесообразно также использовать монографии, журнальные и газетные статьи, нормативные правовые документы, электронные ресурсы. Перечень использованных литературных источников свидетельствует о глубине проработки темы. Весь изученный материал систематизируется и излагается в соответствии с планом. Важно, при написании контрольной (курсовой) работы выразить собственную позицию по изучаемой проблеме. Материал следует излагать грамотно, четко, без повторений и сокращений (кроме общепринятых).

При подготовке к промежуточной аттестации по дисциплине следует руководствоваться перечнем вопросов для подготовки к итоговому контролю по курсу. При этом необходимо уяснить суть основных понятий дисциплины.

Самостоятельная работа студентов, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

Предполагается, что, прослушав лекцию, студент должен ознакомиться с рекомендованной литературой из основного списка, затем обратится к источникам, указанным в библиографических списках изученных книг, осуществит поиск и критическую оценку материала на сайтах Интернет, соберет необходимую информацию.

Существует несколько методов работы с литературой.

Один из них – метод повторения: смысл прочитанного текста можно заучить наизусть. Простое повторение воздействует на память механически и поверхностно. Полученные таким путем сведения легко забываются.

Наиболее эффективный метод - метод осознанного запоминания: прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке. Чтобы основательно обработать информацию, важно произвести целый ряд мыслительных операций: прокомментировать новые данные; оценить их значение; поставить вопросы; сопоставить полученные сведения с ранее известными.

Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения. Изучение научной, учебной и иной литературы требует ведения рабочих записей. Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

Специальные условия организации обучения по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

Организация обучения по дисциплине инвалидов и лиц с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья при наличии таких обучающихся путем создания специальных условий для получения образования.

Профессорско-преподавательский состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии).

В соответствии с Методическими рекомендациями по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утв. Минобрнауки РФ 08.04.2014 АК-44/05вн при изучении дисциплины предполагается использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

При освоении дисциплины используются различные сочетания видов учебной работы с методами и формами активизации познавательной деятельности обучающихся для достижения запланированных результатов обучения и формирования компетенций. Форма проведения промежуточной аттестации для обучающихся-инвалидов и лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизиологических особенностей. По личной просьбе обучающегося с ограниченными возможностями здоровья, изложенной в форме письменного заявления, по дисциплине предусматриваются:

- замена устного ответа на письменный ответ при сдаче зачета или экзамена;
- увеличение продолжительности времени на подготовку к ответу на зачете или экзамене;
- при подведении результатов промежуточной аттестации студентов выставляется максимальное количество баллов за посещаемость аудиторных занятий.