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**

УТВЕРЖДЕНО
директором Павловского филиала ННГУ
к.э.н. Н.А. Ягуновой
(распоряжение от 11.03.2020 г. № 19ф)

**Рабочая программа дисциплины**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

*(наименование дисциплины (модуля))*

Уровень высшего образования

**БАКАЛАВРИАТ**

Направление подготовки / специальность

**38.03.02 МЕНЕДЖМЕНТ**

Направленность образовательной программы

**ПРОИЗВОДСТВЕННЫЙ МЕНЕДЖМЕНТ**

Форма обучения

**ОЧНАЯ, ЗАОЧНАЯ**

Павлово

2020 год

## *Лист актуализации*

**Визирование РПД для исполнения в очередном учебном году**

Председатель ОМК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры

_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

**Визирование РПД для исполнения в очередном учебном году**

Председатель ОМК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры

_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

**Визирование РПД для исполнения в очередном учебном году**

Председатель МК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры

_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

**Визирование РПД для исполнения в очередном учебном году**

Председатель ОМК
__ _____ 20___ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры

_____

Протокол от __ _____ 20___ г. № __
Зав. кафедрой _____

## 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 38.03.02 Менеджмент для очной формы обучения на 1 курсе, для заочной форм обучения на 2 курсе.

Трудоемкость дисциплины составляет 5 зачетных единицы.

**Целями** учебной дисциплины является подготовка студентов-бакалавров к эффективному освоению теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

Для изучения данной дисциплины студент должен обладать входными знаниями, умениями и компетенциями, полученными при изучении дисциплины «Информатика».

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

| **Формируемые компетенции** (код компетенции, уровень освоения – при наличии в карте компетенции) | **Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций** |
|---|---|
| *ОПК-7* способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | **Знать:** требования информационной безопасности и средства ее обеспечения в информационно-коммуникационных технологиях;<br>**Уметь:**<br>Готовить документы, формировать коммуникации информационной и библиографической культуры при соблюдении требований информационной безопасности; формировать информационное обеспечение своей профессиональной деятельности и работ по решению стандартных задач в рамках информационно-коммуникационных технологий при соблюдении правил информационной и библиографической культуры и требований информационной безопасности<br>**Владеть:** навыками информационной и библиографической культуры |

## 3. Структура и содержание дисциплины (модуля).

Объем дисциплины для очной формы обучения составляет ___5____ зачетных единиц, всего ___180____часов, из которых ___66___часов составляет контактная работа обучающегося с преподавателем (__32___часов занятия лекционного типа, __32____часов занятия семинарского типа, 2 часа - КСР),__36____часов контроль,____78____часов составляет самостоятельная работа обучающегося.

Объем дисциплины для заочной формы обучения составляет ___5____ зачетных единиц, всего ___180____часов, из которых ___14___час составляет контактная работа обучающегося с преподавателем (__4___часа занятия лекционного типа, __8____часа занятия семинарского типа, 2 часа- КСР) __9____часов контроль,____157____часов составляет самостоятельная работа обучающегося.

### Структура и содержание дисциплины (модуля)

| **Наименование и краткое содержание разделов и тем дисциплины (модуля),** | **Всего (часы)** | В том числе | |
|---|---|---|---|
| | | **Контактная работа (работа во взаимодействии с преподавателем), часы** из них | **Самостоятельная работа обучающегося, часы** |

| форма промежуточной аттестации по дисциплине (модулю) | | | | Занятия лекционного типа | | | Занятия семинарского типа | | | Занятия лабораторного типа | | | Всего | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная |
| Тема 1. Введение в информационную безопасность | 21 | | 29 | 4 | | 0,5 | 4 | | 1 | | | | 8 | | 1,5 | 13 | | 27,5 |
| Тема 2. Угрозы информационной безопасности | 21 | | 29 | 4 | | 0,5 | 4 | | 1 | | | | 8 | | 1,5 | 13 | | 27,5 |
| Тема 3. Программно-технические методы защиты информации | 25 | | 29 | 6 | | 0,5 | 6 | | 1 | | | | 12 | | 1,5 | 13 | | 27,5 |
| Тема 4. Менеджмент и аудит информационной безопасности на уровне предприятия | 25 | | 28 | 6 | | 0,5 | 6 | | 1 | | | | 12 | | 1,5 | 13 | | 26,5 |
| Тема 5. Управление рисками информационной безопасности | 25 | | 28 | 6 | | 1 | 6 | | 2 | | | | 12 | | 3 | 13 | | 25 |
| Тема 6. Управление информационной безопасностью на государственном уровне | 25 | | 26 | 6 | | 1 | 6 | | 2 | | | | 12 | | 3 | 13 | | 23 |
| КСР | 2 | | 2 | | | | 2 | | 2 | | | | | | | | | |
| Контроль | 36 | | 9 | | | | | | | | | | | | | | | |
| Промежуточная аттестация - **Экзамен** | | | | | | | | | | | | | | | | | | |

**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 информации 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 гражданами 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 «Информационная безопасность» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр по актуальным статистическим проблемам, разбор конкретных ситуаций) 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.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

Практические занятия проводятся в компьютерных классах с применением специализированных информационных систем, комплексов и технологий бизнес-индустрии.

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 информационной безопасности (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 экзамену учитывать общие требования и рекомендации.

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

**Методические указания по выполнению научно-исследовательской работы**

**Целью** выполнения работы является:

- закрепление знаний, полученных студентами в процессе теоретического обучения;
- проведение исследования проблемы;
- активное использование пакетов прикладных программ; анализ библиографических материалов.
- отработка приемов и способов аналитических расчетов на практическом материале.

**Выбор темы** производится студентом и утверждается преподавателем. Рекомендуемый объем работы 35-40 страниц машинописного текста.

В каждой работе, кроме основных разделов, независимо от темы, предусматривается «Введение», «Заключение», «Список используемой литературы», «Приложения».

**Список литературы** должен быть составлен в соответствии с библиографическими требованиями.

Выполнять научно-исследовательскую работу необходимо с использованием текстового редактора MS Word, электронных таблиц Excel, а также можно использовать пакеты прикладных программ (ППП).

К оформлению научно-исследовательской работы предъявляются общие типовые требования.

**Рекомендуемые направления научно-исследовательских работ**

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
7. Информационная безопасность (по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
12. Составление инструкции по обработке и хранению конфиденциальных документов.
13. Направления и методы защиты документов на бумажных носителях.
14. Направления и методы защиты машиночитаемых документов.
15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты аудио- и визуальных документов.
17. Порядок подбора персонала для работы с конфиденциальной информацией.
18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
28. Назначение, виды, структура и технология функционирования системы защиты информации.
29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.
30. Аналитическая работа по выявлению каналов утечки информации фирмы.
31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
32. Направления и методы защиты профессиональной тайны.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.
37. Защита секретов в дореволюционной России.
38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

**Перечень вопросов к экзамену**

1. Прогресс информационных технологий и необходимость обеспечения безопасности.
2. Основные понятия информатизации общества и информационной безопасности.
3. Структура понятия « Информационная безопасность»
4. Объекты информационной безопасности в компании.
5. Системный подход к защите информации.
6. Обеспечивающие компоненты системы защиты информации.
7. Экономическая информация как товар и объект безопасности.
8. Перечень сведений, относящихся к коммерческой тайне. Объекты банковской тайны.
9. Информационные угрозы и их классификация.
10. Действия и события, нарушающие информационную безопасность.
11. Основные виды каналов утечки информации.
12. Пути несанкционированного доступа к информации.
13. Личностно – профессиональные характеристики сотрудников, способствующие реализации информационных угроз.
14. Способы воздействия угроз на информационные объекты.
15. Вредоносные программы, их виды.
16. Признаки воздействия вирусов на компьютерную систему.
17. Компьютерные преступления и их классификация.
18. Субъекты компьютерных преступлений.
19. Объективная сторона компьютерных преступлений.
20. Уголовно - правовой контроль над компьютерной преступностью в России.
21. Государственное регулирование информационной безопасности.
22. Типы международных организаций в сфере ИБ.
23. Направление работы крупных альянсов в сфере ИБ.
24. Доктрина информационной безопасности РФ.
25. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
26. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».
27. Методы и средства обеспечения ИБ.
28. Фрагментный и системный подход к защите информации.
29. Уголовно – правовая характеристика компьютерных преступлений.
30. Статьи 272, 273, 274 УК о компьютерных преступлениях.
31. Меры предупреждения преступлений в сфере компьютерной информации.

32. Исторические аспекты компьютерных преступлений.
33. Перечень сведений, которые не могут составлять коммерческую тайну.
34. Стратегия и тактика злоумышленника при несанкционированном доступе.
35. Организация конфиденциального делопроизводства.
36. Защита от компьютерных преступлений.
37. Структура службы безопасности компании.
38. Принципы построения системы информационной безопасности.
39. Электронная цифровая подпись и особенности ее применения.
40. Защита информации в Интернете.
41. Организация системы защиты информации экономических систем.
42. Этапы построения системы защиты информации.
43. Политика безопасности.
44. Оценка эффективности инвестиций в информационную безопасность.
45. Информационная безопасность электронной коммерции (ЭК)
46. Сущность криптографических методов.
47. Организационно – административные мероприятия обеспечения компьютерной безопасности.
48. Принципы обеспечения информационной безопасности на основе инженерно – технического обеспечения.
49. Информационная безопасность предпринимательской деятельности.
50. Методика защиты электронной почты.
51. Обеспечение безопасности должностных лиц и представителей деловых кругов.

## 6. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю).

### 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-7*** способностью 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** | **Критерии оценивания (дескрипторы)** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **«плохо»** | **«неудовлетворительно»** | **«удовлетворительно»** | **«хорошо»** | **«очень хорошо»** | **«отлично»** | **«превосходно»** |
| **Знания** требования информационной безопасности и средства ее обеспечения в информационно-коммуникационных технологиях | отсутствие знаний материала | наличие грубых ошибок в основном материале | знание основного материала с рядом негрубых ошибок | знание основного материалом с рядом заметных погрешностей | знание основного материала с незначительными погрешностями | знание основного материала без ошибок и погрешностей | знание основного и дополнительного материала без ошибок и погрешностей |
| **Умения** формировать информационное обеспечение своей профессиональной деятельности и работ по решению стандартных задач в рамках информационно- | отсутствует способность решения стандартных задач | наличие грубых ошибок при решении стандартных задач | способность решения основных стандартных задач с негрубым и ошибками | способность решения всех стандартных задач с незначительными погрешностями | способность решения всех стандартных задач без ошибок и погрешностей | Способность решения стандартных и некоторых нестандартных задач | способность решения стандартных задач и широкого круга нестандартных задач |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| коммуникационных технологий при соблюдении правил информационной и библиографической культуры и требований информационной безопасности | | | | | | | |
| **Владения** навыками информационной и библиографической культуры | полное отсутствие навыков, предусмотренных компетенцией | отсутствие ряда важнейших навыков, предусмотренных данной компетенцией | наличие минимально необходимого множества навыков | наличие большинства основных навыков, продемонстрированное в стандартных ситуациях | наличие всех основных навыков, продемонстрированных в стандартных ситуациях | наличие всех навыков, продемонстрированное в стандартных ситуациях | Наличие всех навыков, продемонстрированное в стандартных и нестандартных ситуациях |
| Шкала оценок по проценту правильно выполненных контрольных заданий | 0 – 20 % | 20 – 50 % | 50 – 70 % | 70-80 % | 80 – 90 % | 90 – 99 % | 100% |

### 6.2. Описание шкал оценивания результатов обучения по дисциплине

Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде экзамена, на котором определяется:

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

Экзамен проводится в устной форме. Устная часть экзамена 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.

| Оценка | Уровень подготовки |
|---|---|
| Превосходно | Высокий уровень подготовки, безупречное владение теоретическим материалом, студент демонстрирует творческий поход к решению нестандартных ситуаций. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждая теоретический материал практическими примерами из практики. Студент активно работал на практических занятиях. |
| Отлично | Высокий уровень подготовки с незначительными ошибками. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждает теоретический материал практическими примерами из практики. Студент активно работал на практических занятиях. |
| Очень хорошо | Хорошая подготовка. Студент дает ответ на все теоретические вопросы билета, но имеются неточности в определениях понятий, процессов и т.п. Студент активно работал на практических занятиях. |
| Хорошо | В целом хорошая подготовка с заметными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы билета, но имеются |

| | |
|---|---|
| | неточности в определениях понятий, процессов и т.п. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы экзаменатора. Студент работал на практических занятиях. |
| Удовлетворительно | Минимально достаточный уровень подготовки. Студент показывает минимальный уровень теоретических знаний, делает существенные ошибки, но при ответах на наводящие вопросы может правильно сориентироваться и в общих чертах дать правильный ответ. Студент посещал практические занятия. |
| Неудовлетворительно | Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на наводящие и дополнительные вопросы экзаменатора. Студент пропустил большую часть практических занятий. |

### 6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, 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.

По итогам изучения дисциплины предусмотрен экзамен с комплексной проверкой теоретических знаний, практических навыков и умений по применению информационных средств и технологий ИБ.

Теоретические знания оцениваются путем тестирования или на основании письменных или устных ответов студентов на поставленные теоретические вопросы из разных разделов и тем дисциплины.

Практические навыки определяются путем построения студентами на компьютере системы безопасности с использованием инструментальных средств IT-индустрии. При оценке задач учитываются полнота и правильность решения, выбор инструментария и соблюдение технологии решения, качество и время решения.

Итоговые результаты экзамена оцениваются в соответствии с общепринятой в ННГУ методикой и критериями. Кроме знаний, навыков и умений, показанных студентами непосредственно на зачете, учитывается их текущая успеваемость - аттестация и работа в семестре.

<u>Критерии оценки тестов</u>

| | |
|---|---|
| «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. |

<u>Описание шкалы оценивания для выполненных практических заданий</u>

| Оценка | Критерии оценивания |
|---|---|
| Превосходно | Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, студент отвечает четко и последовательно, показывает глубокое знание основного и дополнительного материала. |
| Отлично | Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, студент отвечает четко и |

| | |
|---|---|
| | последовательно, показывает глубокое знание основного материала |
| Очень хорошо | Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, студент отвечает четко и последовательно, показывает глубокое знание материала, допущено не более 2 неточностей непринципиального характера |
| Хорошо | Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, допущены неточности непринципиального характера, но студент показывает систему знаний по теме своими ответами на поставленные вопросы |
| Удовлетворительно | Задание выполнено не в полном объеме (решено более 50% поставленных задач), но студент допускает ошибки, нарушена последовательность ответа, но в целом раскрывает содержание основного материала |
| Неудовлетворительно | Задание выполнено не в полном объеме (решено менее 50% поставленных задач), студент дает неверную информацию при ответе на поставленные задачи, допускает грубые ошибки при толковании материала, демонстрирует незнание основных терминов и понятий. |
| Плохо | Задание не выполнено, студент демонстрирует полное незнание материала |

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 (ОПК-7)**

*На каждый вопрос предложено три варианта ответа. Выберите один правильный и отметьте его* √ .

1. Третьим этапом построения системы защиты является:

- планирование;
- реализация;
- анализ.

2. «Люком» называется..?

- использование после окончания работы части данных, оставшиеся в памяти;
- передача сообщений в сети от имени другого пользователя;
- неописанная в документации на программный продукт возможность работы с ним.

3. Правовое обеспечение информационной безопасности - это..?

- нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
- документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
- широкое использование технических средств защиты информации.

4. К активным угрозам относятся:

- попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
- разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы;
- копирование информации.

5. Какого подхода к обеспечению безопасности информации не существует?

- комплексный;
- фрагментарный;

– теоретический.

6. Типовыми путями несанкционированного доступа к информации, являются:

– дистанционное фотографирование;
– выход из строя ПЭВМ;
– ураганы.

7. Первым этапом построения системы защиты является:

– анализ;
– планирование;
– сопровождение.

8. «Троянский конь»- это …?

– способ, состоящий в тайном введении в чужую программу вредоносных команд;
– встраивание в программу набора команд, срабатываемых при определенных условиях;
– проникновение в компьютерную систему злоумышленников, выдающих себя за законного пользователя.

9. В политике безопасности основным принципом является усиление самого слабого звена?

– нет;
– да;
– отчасти.

10. Криптографические средства - это..?

– регламентация правил использования, обработки и передачи информации ограниченного доступа;
– средства защиты с помощью преобразования информации (шифрование);
– средства, в которых программные и аппаратные части полностью взаимосвязаны.

11. Шифрование с симметричным ключом предполагает, что..?

– используются два разных ключа;
– оба ключа одинаковы;
– невозможно отказаться от авторства.

12. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети предусмотрено в ..?

– ст. 272 УК РФ;
– ст. 273 УК РФ;
– ст. 274 УК РФ.

### 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. Исключение 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. На первом этапе изучения дисциплины идет накопление знаний обучающихся, на проверку которых направлены такие оценочные средства как

подготовка докладов, дискуссии, устный опрос, коллоквиум. Затем проводится контрольная работа, позволяющая оценить не только знания, но и умения студентов по их применению. На следующем этапе изучения дисциплины делается акцент на компонентах «уметь» и «владеть» посредством выполнения типовых заданий с возрастающим уровнем сложности. Затем предусматриваются устные опросы с практикоориентированными вопросами и заданиями. На заключительном практическом занятии проводится тестирование по дисциплине.

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 (рецензирования студентами работ друг друга, взаимное оппонирование студентами проектов, исследовательских работ, экспертные оценки группами из студентов, преподавателей, работодателей и др.);
- анализ достижений по итогам оценивания с выявлением положительных и отрицательных индивидуальных и групповых результатов и направлений развития.

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Условиями оценивания результатов освоения дисциплины являются:

- валидность (объекты оценки должны соответствовать поставленным целям обучения);
- полнота и адекватность отображения требований образовательного стандарта и ООП;
- 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 обеспечение дисциплины

### Основная литература

1. Баранова Е. К Информационная 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 Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-16-106532-7. - Текст : электронный. - URL: (Доступно в ЭБС «Знаниум», режим доступа: https://znanium.com/catalog/product/1114032 )

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2020. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-16-101207-9. - Текст : электронный. - URL: (Доступно в ЭБС «Знаниум», режим доступа: https://znanium.com/catalog/product/1093657 )

3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-16-101302-1. - Текст : электронный. - URL: (Доступно в ЭБС «Знаниум», режим доступа: https://znanium.com/catalog/product/1081318 )

4. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2019. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа http://znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571. - ISBN 978-5-16-102993-0. - Текст : электронный. - URL: (Доступно в ЭБС «Знаниум», режим доступа:https://znanium.com/catalog/product/991792 )

5. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-16-106532-7. - Текст : электронный. - URL: (Доступно в ЭБС «Знаниум», режим доступа: https://znanium.com/catalog/product/1114032 )

**Программное обеспечение и интернет-ресурсы**

1. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.
2. www.itsec.ru Интернет-журнал «Информационная безопасность».
3. www.inside-zi.ru Информационно-методический журнал «Защита информации. Инсайд»
4. www.kaspersky.ru Лаборатория Касперского.
5. Операционная система Microsoft Windows
6. Пакет прикладных программ Microsoft Office
7. Правовая система «Консультант плюс»
8. Правовая система «Гарант».

## 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 Microsoft Windows, пакет прикладных программ Microsoft Office) и свободно распространяемого программного обеспечения.

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

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

## 9. Особенности организации обучения по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

**9.1. Обучение обучающихся с ограниченными возможностями здоровья** при необходимости осуществляется филиалом с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

Профессорско-педагогический 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 Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

**9.2. В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями** здоровья филиал обеспечивает:

1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

- размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;
- выпуск альтернативных форматов методических материалов (крупный шрифт).

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающего обучающемуся необходимую помощь.

3) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

- возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения, а также пребывание в указанных помещениях;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь.

**9.3. Образование обучающихся с ограниченными возможностями здоровья** может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

**9.4. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.**

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

| № п/п | Критерии студентов | Формы |
|---|---|---|
| 1 | С нарушением слуха | – в печатной форме<br>– в форме электронного документа |
| 2 | С нарушением зрения | – в печатной форме увеличенным шрифтом<br>– в форме электронного документа |

| | | |
|---|---|---|
| 3 | С нарушением опорно-двигательного аппарата | – в печатной форме<br>– в форме электронного документа |

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

**9.5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.**

9.5.1 *Перечень фондов оценочных средств, соотнесённых с планируемыми результатами освоения образовательной программы*.

Для студентов с ограниченными возможностями здоровья предусмотрены следующие оценочные средства:

| № п/п | Критерии студентов | Виды оценочных средств | Формы контроля и оценки результатов обучения |
|---|---|---|---|
| 1 | С нарушением слуха | тест | преимущественно письменная проверка |
| 2 | С нарушением зрения | собеседование по вопросам | преимущественно устная проверка (индивидуально) |
| 3 | С нарушением опорно-двигательного аппарата | решение письменных тестов, контрольные вопросы | письменная проверка |

Студентам с ограниченными возможностями здоровья увеличивается время на подготовку ответов к экзамену.

*9.5.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций*

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме;
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);

2. доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом);

3. доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине (модулю) может проводиться в несколько этапов.

**9.6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья предоставляются основная и дополнительная учебная литература в виде электронного документа в фонде библиотеки и/ или в электронно-библиотечных системах.

**9.7. Методические указания для обучающихся по освоению дисциплины**

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

**9.8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения:

- лекционная аудитория – мультимедийное оборудование, источники питания для индивидуальных технических средств;
- учебная аудитория для практических занятий (семинаров) - мультимедийное оборудование, источники питания для индивидуальных технических средств;
- учебная аудитория для самостоятельной работы – стандартные рабочие места с персональными компьютерами; рабочее место с персональным компьютером, с программой экранного доступа, программой экранного увеличения «экранная лупа» для студентов с нарушением зрения.

В аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусмотрены места для обучающихся с учётом ограничений их здоровья.

Программа составлена в соответствии с требованиями ОС ВО ННГУ и ОПОП ВО по направлению 38.03.02 «Менеджмент», направленность образовательной программы «Производственный менеджмент».

**Автор**: _____

**Рецензент:** к.э.н., генеральный директор
ООО НЗСМИ «Парацельс» _____ Ягунов А.Е.

**Заведующий кафедрой** экономики и права к.э.н., доцент _____ Ягунова Н.А.

Программа одобрена на заседании объединенной методической комиссии ИОО и филиалов университета, протокол № 11 от 10.03.2020 года