

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

УТВЕРЖДАЮ:  
Директор института  
Энергетики и автоматизированных систем  
 С.И. Лукьянов  
«20» сентября 2017 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**  
*НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ*

Направление подготовки (специальность)

**10.05.03 Информационная безопасность автоматизированных систем**  
инфр наименование направления подготовки (специальности)

Направленность (профиль/ специализация) программы

**Обеспечение информационной безопасности  
распределенных информационных систем**

наименование направленности (профиля) подготовки (специализации)

Уровень высшего образования  
**специалитет**

Форма обучения  
**очная**

Институт  
Кафедра  
Курс  
Семестр

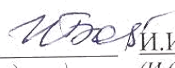
Энергетики и автоматизированных систем  
Информатики и информационной безопасности  
4,5  
8,9

Магнитогорск  
2017 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры  
Информатики и информационной безопасности  
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой  / И.И. Баранкова /  
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией  
института Энергетики и автоматизированных систем  
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель  / С.И. Лукьянов /  
(подпись) (И.О. Фамилия)

Рабочая программа составлена:

зав. кафедрой ИиИБ, д.т.н., профессор  
(должность, ученая степень, ученое звание)

 / И.И. Баранкова /  
(подпись) (И.О. Фамилия)

Рецензент:

зав. кафедрой Бизнес-информатики  
и информационных технологий, к.п.н. профессор  
(должность, ученая степень, ученое звание)

 / Г.Н. Чусавитина /  
(подпись) (И.О. Фамилия)

**Лист регистрации изменений и дополнений**

[illegible]

## 1. Цели освоения дисциплины

Целями изучения дисциплины «Управление информационной безопасностью» являются: формирование знаний принципов политики информационной безопасности в информационных системах; навыков организации и методологии обеспечения информационной безопасности автоматизированных систем, функционирующих на предприятиях и организациях РФ; умений по разработке нормативных материалов, регламентирующих работу по защите информации

## 2. Место дисциплины в структуре образовательной программы подготовки специалиста

Дисциплина «Управление информационной безопасностью» входит базовую часть блока 1 образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем».

Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для прохождения преддипломной практики и выполнения выпускной квалификационной работы.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

Изучение дисциплины направлено на формирование и развитие следующих компетенций: ОК-4; ПК-11; ПК-12; ПК-19; ПК-22; ПК-28

| Структурный элемент компетенции                                                                         | Планируемые результаты обучения                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Знать                                                                                                   | <ul style="list-style-type: none"><li>- основы законодательства Российской Федерации;</li><li>- нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации;</li><li>- правовые основы организации защиты государственной тайны и конфиденциальной информации;</li><li>- меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.</li></ul>                                                                  |
| Уметь                                                                                                   | <ul style="list-style-type: none"><li>- обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей;</li><li>- предпринимать необходимые меры по восстановлению нарушенных прав.</li></ul>                                                                                                                                                                                                                                                    |
| Владеть                                                                                                 | <ul style="list-style-type: none"><li>- навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов.</li></ul>                                                                                                                                                                                                                                                                                                                         |
| <b>ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Знать                                                                                                   | <ul style="list-style-type: none"><li>- задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</li><li>- систему организационных мер, направленных на защиту информации ограниченного доступа</li><li>- нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;</li><li>- основные угрозы безопасности информации и модели нарушителя объекта информатизации;</li></ul> |

| Структурный элемент компетенции                                                                                                                     | Планируемые результаты обучения                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                     | <ul style="list-style-type: none"> <li>- правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;</li> <li>- принципы формирования политики ИБ организации;</li> </ul>                                                                                                                                                                                                                           |
| Уметь                                                                                                                                               | <ul style="list-style-type: none"> <li>- разрабатывать модели угроз и модели нарушителя ОИ;</li> <li>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;</li> <li>- разрабатывать предложения по совершенствованию системы управления ИБАС.</li> </ul>                                                                                  |
| Владеть                                                                                                                                             | <ul style="list-style-type: none"> <li>- навыками выявления угроз безопасности информации вАС;</li> <li>- владеть навыками разработки политик безопасности различных уровней.</li> </ul>                                                                                                                                                                                                                                           |
| <b>ПК-12</b> способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Знать                                                                                                                                               | <ul style="list-style-type: none"> <li>- особенности решений по ЗИ в информационных процессах и системах;</li> <li>- определения рисков ИБ применительно к ОИ с заданными характеристиками;</li> <li>- методы и подходы к реализации системы управления безопасностью АИС;</li> <li>- методы анализа процессов для определения актуальных угроз.</li> </ul>                                                                        |
| Уметь                                                                                                                                               | <ul style="list-style-type: none"> <li>- оценивать различные инструменты в области проектирования и управления ИБ;</li> <li>- разрабатывать политики безопасности информации АС;</li> <li>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.</li> </ul>                                                                                                                                |
| Владеть                                                                                                                                             | <ul style="list-style-type: none"> <li>-навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.</li> </ul>                                                                                                                                                                                                                                             |
| <b>ПК-19</b> способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Знать                                                                                                                                               | <ul style="list-style-type: none"> <li>-нормативные методические документы ФСТЭК России в области ИБ;</li> <li>- основные угрозы безопасности информации и модели нарушителя в ИС;</li> <li>- стратегии обеспечения ИБ, способы их организации и оптимизации.</li> </ul>                                                                                                                                                           |
| Уметь                                                                                                                                               | <ul style="list-style-type: none"> <li>- оценивать различные инструменты в области проектирования и управления ИБ;</li> <li>- обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности;</li> <li>- расследовать инциденты ИБ;</li> <li>- разрабатывать предложения по совершенствованию СУИБ АС.</li> </ul>                                                                                           |
| Владеть                                                                                                                                             | <ul style="list-style-type: none"> <li>- навыками расчета и управления рисками ИБ;</li> <li>- навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.</li> </ul>                                                                                                                                                                                                                       |
| <b>ПК-22</b> способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации  |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Знать                                                                                                                                               | <ul style="list-style-type: none"> <li>- основные угрозы безопасности информации и модели нарушителя ОИ;</li> <li>- правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;</li> <li>- принципы формирования политики информационной безопасности организации.</li> </ul>                                                                                                                       |
| Уметь                                                                                                                                               | <ul style="list-style-type: none"> <li>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации;</li> <li>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;</li> <li>- разрабатывать частные политики ИБАС;</li> <li>- контролировать эффективность принятых мер по реализации частных политик ИБАС.</li> </ul> |
| Владеть                                                                                                                                             | <ul style="list-style-type: none"> <li>- навыками выявления угроз безопасности информации вАС;</li> <li>- владеть навыками разработки политик безопасности различных уровней.</li> </ul>                                                                                                                                                                                                                                           |
| <b>ПК-28</b> способностью управлять информационной безопасностью автоматизированной системы                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Структурный элемент компетенции | Планируемые результаты обучения                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Знать                           | - основные угрозы безопасности информации и модели нарушителя в ИС;<br>- основные меры по ЗИвАС.                                                                                   |
| Уметь                           | - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;<br>- расследовать инциденты ИБ.                                                     |
| Владеть                         | - навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИвАС;<br>- терминологией и процессным подходом построения СУИБ. |

#### 4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 8 зачетных единиц 288 часа, в форме практической подготовки 10 часов, в том числе:

- контактная работа – 142,8 акад. часов:  
аудиторная – 136 акад. часов;  
внеаудиторная – 6,8 кад. часов
- самостоятельная работа – 109,5 акад. часов;
- подготовка к экзамену – 35,7 акад. часа.

Вид промежуточной аттестации –зачет, экзамен, курсовая работа

| Раздел/ тема дисциплины                                                           | Семестр | Аудиторная контактная работа (в акад. часах) |                            | Самостоятельная работа | Вид самост. работы                               | Формы текущего и промежуточного контроля успеваемости | Код и структурный элемент компетенции |
|-----------------------------------------------------------------------------------|---------|----------------------------------------------|----------------------------|------------------------|--------------------------------------------------|-------------------------------------------------------|---------------------------------------|
|                                                                                   |         | Лекции                                       | Практич. занятия / в форме |                        |                                                  |                                                       |                                       |
| 1.Основные принципы создания системы управления информационной безопасностью.     | 8       | 4                                            | 4/2                        | 4                      | Поиск дополнительной информации по заданной теме | Тестирование, Отчет на образовательном портале        | ОК-4-з; ПК-11-з;                      |
| 1.1. Структура системы управления информационной безопасностью.                   |         | 4                                            | 4/2                        | 4                      | Подготовка структуры СУИБ заданного ОИ.          | ИДЗ, Отчет на образовательном портале                 | ОК-4-зув; ПК-11-зу; ПК-12-з;          |
| 1.2. Проектирование систем ИБ. Внедрение ISO 27001/17799.                         |         | 4                                            | 4                          | 6                      | Изучение этапов проектирования                   | Устный опрос. ИДЗ, Отчет на образовательном портале   | ПК-11-зув; ПК-19-зу, ПК-22 зув        |
| 1.3. Административный уровень обеспечения ИБ. Политики среднего и нижнего уровня. |         | 4                                            | 4/2                        | 4                      | Работа материалами образовательного портала.     | Устный опрос, ИДЗ                                     | ПК-11-зув; ПК-12-зув;                 |



|                                                                                                                                                                   |           |                   |             |                                                                |                                                                 |                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------------|-------------|----------------------------------------------------------------|-----------------------------------------------------------------|---------------------------------------|
|                                                                                                                                                                   |           |                   |             | Подготовка основных положений политики одного из уровней       |                                                                 |                                       |
| <b>1.4.</b> Разработка политик ИБ. Профиль защиты. Разработка профилей защиты и заданий по безопасности.                                                          | 4         | 4/2               | 2           | Изучение руководящих материалов по созданию профилей           | ИДЗ, отчет на образовательном портале                           | ПК-12-зுவ<br>ПК-19-з;<br>ПК-22-з;     |
| <b>1.5.</b> Расследование инцидентов ИБ. Администратор безопасности.                                                                                              | 4         | 4/2               | 4           | Работа с материалами образовательного портала.                 | Устный опрос. ИДЗ                                               | ПК-19-зув;<br>ПК-22-зув;              |
| <b>1.6.</b> Комплект типовых документов по ИБ.                                                                                                                    | 5         | 5/2               | 6,2         | Подготовка перечня документов                                  | Аудиторные контрольные работы. Отчет на образовательном портале | ПК-19-зув;<br>ПК-22-зув;              |
| <b>1.7.</b> Технические политики ИБ.                                                                                                                              | 5         | 5/2               | 8           | Подготовка одной из политик                                    | ИДЗ, Отчет на образовательном портале                           | ПК-19-зув;<br>ПК-22-зув;<br>ПК-28-зув |
| <b>Итого по разделу</b>                                                                                                                                           | <b>34</b> | <b>34/<br/>14</b> | <b>38,2</b> |                                                                | <b>Промежуточный контроль (зачет)</b>                           |                                       |
| <b>2.</b> Обеспечение безопасности информации КИИ.                                                                                                                | <b>9</b>  |                   |             |                                                                |                                                                 |                                       |
| <b>2.1.</b> Основные программно-технические подсистемы СОБИ КСИИ.                                                                                                 | 7         | 7/4               | 16          | Подготовка к практическим занятиям. Выполнение ИДЗ.            | Устный опрос. Аудиторные контрольные работы                     | ПК-22-зув;<br>ПК-28-зув               |
| <b>2.2.</b> Управление ОБИ КСИИ документирование и реализация основных процессов.                                                                                 | 7         | 7/4               | 14          | Подготовка к практическим занятиям.                            | Устный опрос. ИДЗ                                               | ПК-22-зув;<br>ПК-28-зув               |
| <b>2.3.</b> Этапы разработки СОБИ КИИ. Аналитическое обоснование необходимости создания СОБИ КИИ. Нормативные методические документы ФСТЭК.                       | 7         | 7/2               | 16          | Изучение документов ФСТЭК. Подготовка к практическим занятиям. | Отчет на образовательном портале ИДЗ                            | ПК-19-зув;<br>ПК-22-зув;<br>ПК-28-зув |
| <b>2.4.</b> Техническое задание на разработку СОБИ КИИ. Основные проектные документы. Разработка комплекса внутренних организационно-распорядительных документов. | 7         | 7/4               | 14          | Разработка технического задания для заданного ОИ.              | ИДЗ                                                             | ПК-19-зув;<br>ПК-22-зув;<br>ПК-28-зув |
| <b>2.5.</b> DLP-системы. Сравнение систем. Принципы                                                                                                               | 6         | 6/4               | 11,3        | Установка DLP-системы                                          | Отчет о порядке установки                                       | ПК-28-зув                             |

|                              |   |           |              |                     |  |                                                          |                                                                 |
|------------------------------|---|-----------|--------------|---------------------|--|----------------------------------------------------------|-----------------------------------------------------------------|
| создания.                    |   |           |              |                     |  |                                                          |                                                                 |
| <b>Итого по разделу</b>      |   | <b>34</b> | <b>34/14</b> | <b>71,3</b>         |  |                                                          |                                                                 |
| <b>Подготовка к экзамену</b> | 9 |           |              | <b>35,7</b>         |  |                                                          |                                                                 |
| <b>Итого по дисциплине</b>   |   | <b>68</b> | <b>68/28</b> | <b>109,5 + 35,7</b> |  | <b>Промежуточный контроль (экзамен, курсовая работа)</b> | ОК-4-зுவ; ПК-11-зுவ; ПК-12-зுவ; ПК-19-зுவ; ПК-22-зுவ; ПК-28-зுவ |

## 5 Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Управление информационной безопасностью» используются традиционная и модульно-компетентностная технологии.

Реализация компетентного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

### Формы учебных занятий с использованием традиционных технологий:

- **обзорные лекции** – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;
- **информационные** – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;
- **лекции-визуализации** – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;
- **Семинар.**
- **Практическое занятие**, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

### Формы учебных занятий с использованием технологий проблемного обучения:

**Проблемная лекция** – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала

- **проблемная** - для развития исследовательских навыков и изучения способов решения задач.
- **лекции с заранее запланированными ошибками** – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.
- **Практическое занятие в форме практикума** – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.
- **Практическое занятие на основе кейс-метода** – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации



#### **Формы учебных занятий с использованием игровых технологий:**

- **Учебная игра** – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.
- **Деловая игра** – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

#### **Технологии проектного обучения**

- **Творческий проект** – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).
- **Информационный проект** – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

#### **Формы учебных занятий с использованием информационно-коммуникационных технологий:**

- **Лекция-визуализация** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
- **Практическое занятие в форме презентации** – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.
- **методы ИТ**
  - Подготовка и проведение лабораторных работ по поиску информации в сетях. Задание критериев поиска информации. Работа с поисковыми системами университета и внешними ресурсами.
  - Подготовка и проведение лабораторных работ по Архивации данных с целью дальнейшего использования в средствах телекоммуникационных технологий: электронной почте, чате, телеконференции т.д.
  - Организация доступа обучающихся к основным и дополнительным лекционным материалам с использованием клиент-серверных технологий.
  - Использование электронных образовательных ресурсов для организации самостоятельной работы обучающихся. Разработка преподавателями кафедры авторских ЭОР, подготовка перечня и ориентация обучающихся на государственные образовательные интернет-ресурсы.
  - Использование в образовательном процессе электронных учебников, компьютерных обучающих систем, интерактивных упражнений.
  - Компьютерный практикум.
- **работа в команде**
  - Работа с элементами «Семинар», «Форум», «Обсуждение» на образовательном портале.
- **case-study**
  - Разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.
- **проблемное обучение**
  - Подготовка тематических рефератов, содержащих разделы, частично или полностью выносимые на самостоятельное изучение.
- **учебная дискуссия**
  - Проведение семинаров, посвященных вопросам информатики, подготовка тематических презентаций по заданным темам, и дальнейший обмен взглядами по конкретной проблеме.
- **использование тренингов**
  - Подготовка и проведение демонстрационных, тематических и итоговых компьютерных тестирований как в качестве локальных, так и внешних контрольных мероприятий.

## 6. Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Управление информационной безопасностью» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

### Примерные индивидуальные домашние задания (ИДЗ):

Задание1: Провести анализ информационной инфраструктуры предприятия. Адаптировать базовую модель угроз для заданного случая.

Задание2: Разработать частную политику безопасности.

Задание3: Составить перечень организационных документов для СУИБ.

## 7. Оценочные средства для проведения промежуточной аттестации

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

| Структурный элемент компетенции                                                                | Планируемые результаты обучения                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Знать                                                                                          | <ul style="list-style-type: none"><li>- основы законодательства Российской Федерации;</li><li>- нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации;</li><li>- правовые основы организации защиты государственной тайны и конфиденциальной информации;</li><li>- меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.</li></ul> | <b>Теоретические вопросы</b><br><b>1.</b> Перечислить стандарты, относящиеся к управлению информационной безопасностью.<br><b>2.</b> Основные положения стандарта управления информационной безопасностью BS 7799.<br><b>3.</b> Основные положения стандарта управления информационной безопасностью ISO/IEC 17799.<br><b>4.</b> Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования.» |
| Уметь                                                                                          | <ul style="list-style-type: none"><li>- обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей;</li><li>- предпринимать необходимые меры по восстановлению нарушенных прав.</li></ul>                                                                                                                                                                                   | <b>1.</b> Сертификация СУИБ на соответствие ISO 27001.<br><b>2.</b> Сформулировать цели внедрения ISO 27001/17799 в организации.                                                                                                                                                                                                                                                                                                         |
| Владеть                                                                                        | <ul style="list-style-type: none"><li>- навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов.</li></ul>                                                                                                                                                                                                                                                        | Провести сертификацию заданной СУИБ на соответствие ISO 27001.<br>Описать этапы разработки и внедрения системы управления ИБ                                                                                                                                                                                                                                                                                                             |

| Структурный элемент компетенции                                                                                                   | Планируемые результаты обучения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ПК-11</b> способностью разрабатывать политику информационной безопасности автоматизированной системы                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Знать                                                                                                                             | <ul style="list-style-type: none"> <li>- задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</li> <li>- систему организационных мер, направленных на защиту информации ограниченного доступа</li> <li>- нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;</li> <li>- основные угрозы безопасности информации и модели нарушителя объекта информатизации;</li> <li>- правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;</li> <li>- принципы формирования политики ИБ организации;</li> </ul> | <b>Теоретические вопросы</b><br><b>1.</b> Что относится к административному уровню обеспечения информационной безопасности?<br><b>2.</b> Что относится к среднему уровню обеспечения информационной безопасности?<br><b>3.</b> Что относится к нижнему уровню обеспечения информационной безопасности?<br><b>4.</b> Организация режима секретности.<br><b>5.</b> Принципы формирования политики информационной безопасности организации. |
| Уметь                                                                                                                             | <ul style="list-style-type: none"> <li>- разрабатывать модели угроз и модели нарушителя ОИ;</li> <li>- разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации;</li> <li>- разрабатывать предложения по совершенствованию системы управления ИБАС.</li> </ul>                                                                                                                                                                                                                                                                                                                           | <b>1.</b> Разработать частную модель угроз для заданного ОИ. Составить предложения по совершенствованию системы управления информационной безопасностью.                                                                                                                                                                                                                                                                                 |
| Владеть                                                                                                                           | <ul style="list-style-type: none"> <li>- навыками выявления угроз безопасности информации вАС;</li> <li>- владеть навыками разработки политик безопасности различных уровней.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>1.</b> На основе частной модели угроз разработать заданную политику безопасности.                                                                                                                                                                                                                                                                                                                                                     |
| <b>ПК-12</b> способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Знать                                                                                                                             | <ul style="list-style-type: none"> <li>- особенности решений по ЗИ в информационных процессах и системах;</li> <li>- определения рисков ИБ применительно к ОИ с заданными характеристиками;</li> <li>- методы и подходы к реализации системы управления безопасностью АИС;</li> <li>- методы анализа процессов для определения актуальных угроз.</li> </ul>                                                                                                                                                                                                                                                                                                                 | <b>Теоретические вопросы</b><br><b>1.</b> Основные принципы организации СУИБ.<br><b>2.</b> Что понимают под профилем защиты.<br><b>3.</b> Содержание профиля защиты.<br><b>4.</b> Что включает в себя методика определения защищенности ИС.<br><b>5.</b> Что включает в себя активное и пассивное тестирование системы защиты.<br><b>6.</b> Методики определения рисков.                                                                 |
| Уметь                                                                                                                             | <ul style="list-style-type: none"> <li>- оценивать различные инструменты в области проектирования и управления ИБ;</li> <li>- разрабатывать политики безопасности информации АС;</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Провести анализ защищенности заданного ОИ.                                                                                                                                                                                                                                                                                                                                                                                               |

| Структурный элемент компетенции                                                                                                                     | Планируемые результаты обучения                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                     | - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Владеть                                                                                                                                             | - навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.                                                                                                                                | <p>Подготовить отчет по проведенному анализу защищенности:</p> <ol style="list-style-type: none"> <li>1. Общие описание объекта обследования</li> <li>2. Структура и состав комплекса программно-технических средств</li> <li>3. Результаты анализа организационных уязвимостей</li> <li>4. Результаты анализа защищенности внешнего периметра сети</li> <li>5. Результаты анализа защищенности внутренней ИТ-инфраструктуры</li> <li>6. Рекомендации по устранению обнаруженных недостатков и повышению уровня защищенности</li> </ol> |
| <b>ПК-19</b> способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы |                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Знать                                                                                                                                               | - нормативные методические документы ФСТЭК России в области ИБ;<br>- основные угрозы безопасности информации и модели нарушителя в ИС;<br>- стратегии обеспечения ИБ, способы их организации и оптимизации.                                                          | <p><b>Теоретические вопросы</b></p> <ol style="list-style-type: none"> <li>1. Назовите основные угрозы безопасности информации</li> <li>2. Дайте описание внешнего нарушителя</li> <li>3. Кто относится к внутренним нарушителям</li> <li>4. Цели тестирования системы защиты</li> </ol>                                                                                                                                                                                                                                                |
| Уметь                                                                                                                                               | - оценивать различные инструменты в области проектирования и управления ИБ;<br>- обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности;<br>- расследовать инциденты ИБ;<br>- разрабатывать предложения по совершенствованию СУИБ АС. | <ol style="list-style-type: none"> <li>1. Провести анализ защищенности внешнего периметра корпоративной сети.</li> <li>2. Провести анализ защищенности внутренней ИТ-инфраструктуры.</li> </ol>                                                                                                                                                                                                                                                                                                                                         |
| Владеть                                                                                                                                             | - навыками расчета и управления рисками ИБ;<br>- навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.                                                                                                                 | <p>По проведенному анализу защищенности подготовить:</p> <ol style="list-style-type: none"> <li>1. Рекомендации по устранению организационных уязвимостей.</li> <li>2. Рекомендации по устранению уязвимостей внешнего периметра сети.</li> <li>3. Рекомендации по устранению</li> </ol>                                                                                                                                                                                                                                                |

| Структурный элемент компетенции                                                                                                                    | Планируемые результаты обучения                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                    |                                                                                                                                                                                                                                                               | уязвимостей внутренней ИТ-инфраструктуры.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>ПК-22</b> способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации |                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Знать                                                                                                                                              | <p>- основные угрозы безопасности информации и модели нарушителя ОИ;</p> <p>- правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности;</p> <p>- принципы формирования политики информационной безопасности организации.</p> | <p><b>Теоретические вопросы</b></p> <p><b>1.</b> Основные разделы ГОСТ Р ИСО/МЭК 15408-2002.</p> <p><b>Вопросы к экзамену:</b></p> <ol style="list-style-type: none"> <li>1. Комплект типовых документов по информационной безопасности.</li> <li>2. Типовые документы для внедрения СУИБ организации.</li> <li>3. Комплект типовых документов для операторов ПДн: <ol style="list-style-type: none"> <li>a. Проектная документация;</li> <li>b. Положения и политики;</li> <li>c. Планы;</li> <li>d. Инструкции и регламенты;</li> <li>e. Приказы;</li> <li>f. Акты;</li> <li>g. Журналы;</li> <li>h. Перечни;</li> <li>i. Обязательства и уведомления;</li> <li>j. Соглашения субъекта.</li> </ol> </li> <li>4. Комплект типовых документов для управления рисками информационной безопасности.</li> <li>5. Методика анализа защищенности ИС.</li> <li>6. Последовательность мероприятий по анализу защищенности.</li> <li>7. Структура отчета по результатам анализа защищенности.</li> <li>8. Тестирование системы защиты по методу «черного» и «белого» ящика.</li> <li>9. Анализ защищенности внешнего периметра корпоративной сети.</li> <li>10. Анализ защищенности внутренней ИТ-инфраструктуры.</li> <li>11. Методы предотвращения сетевых атак на периметр сети.</li> <li>12. Инструментальные средства анализа защищенности.</li> <li>13. Основные принципы создания СУИБ.</li> <li>14. Процедура внедрения СУИБ.</li> <li>15. Разработка политик ИБ.</li> <li>16. Разработка профилей защиты и заданий по безопасности.</li> </ol> |

| Структурный элемент компетенции                                                             | Планируемые результаты обучения                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                | 17. Расследование инцидентов ИБ.<br>18. Организация режима секретности.<br>19. Технические политики ИБ на предприятии.<br>20. Процессный подход для управления ИБ.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Уметь                                                                                       | - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации;<br>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;<br>- разрабатывать частные политики ИБАС;<br>- контролировать эффективность принятых мер по реализации частных политик ИБАС. | 1. Разработать заданную частную политику информационной безопасности.<br>2. Составить описание информационной инфраструктуры организации.<br>3. Выбрать и обосновать меры защиты информационных ресурсов.                                                                                                                                                                                                                                                                                                                                                                       |
| Владеть                                                                                     | - навыками выявления угроз безопасности информации вАС;<br>- владеть навыками разработки политик безопасности различных уровней.                                                                                                                                                                                                                               | <b>Перечень тем курсовых работ:</b><br>1. Разработка комплекса внутренних организационно-распорядительных документов по ОБИ для заданного объекта информатизации (варианты различаются исходными данными на объект).<br>2. Разработка Задания по безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект).<br>3. Разработка Профиля защиты для заданного объекта информатизации (варианты различаются исходными данными на объект).<br>Разработка Технических политик (TechnicalPolicy) информационной безопасности на предприятии. |
| <b>ПК-28</b> способностью управлять информационной безопасностью автоматизированной системы |                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Знать                                                                                       | - основные угрозы безопасности информации и модели нарушителя в ИС;<br>- основные меры по ЗИвАС.                                                                                                                                                                                                                                                               | 1. Назовите основные угрозы безопасности информации.<br>2. Дайте описание внешнего нарушителя.<br>3. Кто относится к внутренним нарушителям.<br>4. На какие группы разделяют инциденты ИБ.<br><b>Вопросы к экзамену:</b><br>1. Комплект типовых документов по информационной безопасности.<br>2. Типовые документы для                                                                                                                                                                                                                                                          |



| Структурный элемент компетенции | Планируемые результаты обучения                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                                                                                                                           | <p>внедрения СУИБ организации.</p> <p>3. Комплект типовых документов для операторов ПДн:</p> <ol style="list-style-type: none"> <li>Проектная документация;</li> <li>Положения и политики;</li> <li>Планы;</li> <li>Инструкции и регламенты;</li> <li>Приказы;</li> <li>Акты;</li> <li>Журналы;</li> <li>Перечни;</li> <li>Обязательства и уведомления;</li> <li>Согласия субъекта.</li> </ol> <p>4. Комплект типовых документов для управления рисками информационной безопасности.</p> <p>5. Методика анализа защищенности ИС.</p> <p>6. Последовательность мероприятий по анализу защищенности.</p> <p>7. Структура отчета по результатам анализа защищенности.</p> <p>8. Тестирование системы защиты по методу «черного» и «белого» ящика.</p> <p>9. Анализ защищенности внешнего периметра корпоративной сети.</p> <p>10. Анализ защищенности внутренней ИТ-инфраструктуры.</p> <p>11. Методы предотвращения сетевых атак на периметр сети.</p> <p>12. Инструментальные средства анализа защищенности.</p> <p>13. Основные принципы создания СУИБ.</p> <p>14. Процедура внедрения СУИБ.</p> <p>15. Разработка политик ИБ.</p> <p>16. Разработка профилей защиты и заданий по безопасности.</p> <p>17. Расследование инцидентов ИБ.</p> <p>18. Организация режима секретности.</p> <p>19. Технические политики ИБ на предприятии.</p> <p>20. Процессный подход для управления ИБ.</p> |
| Уметь                           | <p>- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ;</p> <p>- расследовать инциденты ИБ.</p> | <p>1. Описать процесс расследования инцидента</p> <p>2. Составить заключение по проведенному расследованию.</p> <p>3. Подготовить типовой комплект</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Структурный элемент компетенции | Планируемые результаты обучения                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                                                                                                                                                                                                                            | документов СУИБ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Владеть                         | <ul style="list-style-type: none"> <li>- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИвАС;</li> <li>- терминологией и процессным подходом построения СУИБ.</li> </ul> | <p><b>Перечень тем курсовых работ:</b></p> <ol style="list-style-type: none"> <li>4. Разработка комплекса внутренних организационно-распорядительных документов по ОБИ для заданного объекта информатизации (варианты различаются исходными данными на объект).</li> <li>5. Разработка Задания по безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект).</li> <li>6. Разработка Профиля защиты для заданного объекта информатизации (варианты различаются исходными данными на объект).</li> <li>7. Разработка Технических политик (TechnicalPolicy) информационной безопасности на предприятии.</li> </ol> |

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

**Показатели и критерии оценивания зачета:**

- на оценку «**зачтено**» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;
- на оценку «**не зачтено**» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

**Показатели и критерии оценивания экзамена:**

– на оценку «**отлично**» – обучающийся должен показать высокий уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободно и правильно обосновывать принятые решения;

– на оценку «**хорошо**» – обучающийся должен показать средний уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике;

– на оценку «**удовлетворительно**» – обучающийся должен показать пороговый уровень знаний, умений и навыков в соответствии с формируемыми компетенциями; т.е. владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

– на оценку «**неудовлетворительно**» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не умеет использовать полученные знания при решении типовых практических задач.

Курсовая работа выполняется под руководством преподавателя, в процессе ее написания обучающийся развивает навыки к научной работе, закрепляя и одновременно расширяя знания, полученные при изучении дисциплины. При выполнении курсовой работы обучающийся должен показать свое умение работать с нормативным материалом и другими

литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В процессе написания курсовой работы, обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

#### **Показатели и критерии оценивания курсовой работы:**

– на оценку «**отлично**» (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «**хорошо**» (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку «**удовлетворительно**» (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку «**неудовлетворительно**» (2 балла) – работа выполнена частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи, обучающийся не может воспроизвести и объяснить содержание, не может показать интеллектуальные навыки решения поставленной задачи.

### **8 Учебно-методическое и информационное обеспечение дисциплины (модуля)**

#### **а) Основная литература:**

1) Баранкова И.И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс]: учебное пособие / И. И. Баранкова, О. В. Пермякова; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон.опт. диск (CD-ROM). - Режим доступа: <https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true>. - Макрообъект. - ISBN 978-5-9967-1031-7.

2) Баранкова И.И. Техническая защита информации. Лабораторный практикум [Электронный ресурс]: учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск: МГТУ, 2017. - 1 электрон.опт. диск (CD-ROM). - Режим доступа: <https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true>. - Макрообъект.

3) Золотарев В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб.пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. Режим доступа: <http://znanium.com/bookread.php?book=463037>. – Заглавие с экрана.

4) Жукова М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб.пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. Режим доступа: <http://znanium.com/bookread.php?book=463061> . –Заглавие с экрана.

#### **б) Дополнительная литература:**

1) Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.(Высшее образование). ISBN 978-5-8199-0411-4.–Режим доступа: <http://znanium.com/bookread.php?book=402686> . –Заглавие с экрана. –ISBN 978-5-8199-0411-4.

2) Логунов А.Б. Региональная и национальная безопасность [Электронный ресурс]: Учебное пособие / Логунов А.Б.. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с.: Режим доступа:<http://znanium.com/bookread.php?book=406872> . – Заглавие с экрана. –ISBN 978-5-9558-0310-4.

3) 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. - -Режим доступа: <http://znanium.com/bookread.php?book=405000> .–Заглавие с экрана.– ISBN 978-5-369-01178.

4) Гришина Н.В. Информационная безопасность предприятия [Электронный ресурс]: Учебное пособие / Гришина Н.В. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.- (Высшее образование:Бакалавриат).– Режим доступа: <http://znanium.com/bookread.php?book=491597>. –Заглавие с экрана. –ISBN 978-5-00091-007-8.

5) Гусаров Ю.В. Гусарова Л.Ф. Управление процессом устойчивого и безопасного развития социально-экономической системы [Электронный ресурс] / Информационная безопасность регионов, № 2(11), 2012 <http://znanium.com/bookread.php?book=417537>. – Заглавие с экрана.

6) Управление экономической безопасностью высшего учебного заведения [Электронный ресурс]: Учеб. / Под общ. ред. проф. д.э.н. С.Д.Резника - 2 изд., перераб. и доп. - М.: НИЦ Инфра-М, 2013 - 345с.: - (Менедж. в высшей школе). –Режим доступа: <http://znanium.com/bookread.php?book=363835> . –Заглавие с экрана.– ISBN 978-5-16-005365-3

7) Дубинин Е. А. Оценка относительного ущерба безопасности информационной системы [Электронный ресурс]: Монография / Е.А. Дубинин, Ф.Б. Тебугева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил. –Режим доступа:<http://znanium.com/bookread.php?book=471787>. –Заглавие с экрана. –ISBN 978-5-369-01371-7.

#### **в) Программное обеспечение и Интернет-ресурсы:**

1. Банк данных угроз безопасности информации[Электронный ресурс] / – Режим доступа:<http://www.bdu.fstec.ru/ubi/threat>свободный.– Загл. с экрана. Яз. рус.
2. ФСТЭК России Федеральная служба по техническому и экспортному контролю [Электронный ресурс] / – Режим доступа: <http://fstec.ru>свободный. – Загл. с экрана. Яз.рус.
3. Журнал InformationSecurity. Информационная безопасность: периодич. интернет-изд. [Электронный ресурс] / – Режим доступа: <http://www.itsec.ru/articles2/allpubliks> – Загл. с экрана. Яз.рус.
4. Журнал «Безопасность информационных технологий»: периодич. интернет-изд. [Электронный ресурс] / – Режим доступа: [http://www.pvti.ru/articles\\_14.htm](http://www.pvti.ru/articles_14.htm) – Загл. с экрана. Яз.рус.
5. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. [Электронный ресурс] / – Режим доступа: <http://cyberrus.com/> свободный.– Загл. с экрана. Яз.рус.
6. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: <http://www.osp.ru/lan/> Издательство "Открытые системы. СУБД". [Электронный ресурс] / – Режим доступа: <http://www.osp.ru/os/>свободный.– Загл. с экрана. Яз.рус.
7. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: <http://www.gpntb.ru>, свободный.– Загл. с экрана. Яз. рус.
8. Российская национальная библиотека. [Электронный ресурс] / – Режим доступа:<http://www.nlr.ru>. свободный.– Загл. с экрана. Яз.рус.

9. Компьютерра: все новости про компьютеры, железо, новые технологии, информационные: периодич. интернет-изд. [Электронный ресурс] / – Режим доступа: <http://www.computerra.ru/>свободный.– Загл. с экрана. Яз.рус.

## 9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

| Тип и название аудитории                                                                        | Оснащение аудитории                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)                           | Мультимедийные средства хранения, передачи и представления информации                                                                                                                                                                                                                                                                                                                |
| Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)                    | Персональные компьютеры с ПО:<br>- Операционная система MS Windows 7 - <i>Microsoft Imagine PremiumD-1227-18 от 08.10.2018 до 08.10.2021</i> ;<br>- Пакет MS Office 2007 - <i>Microsoft Open License 42649837, бессрочная</i> ;<br>- Архиватор 7zip - <i>GNU LGPL, бессрочная</i> ;<br>- выход в Интернет и доступ в электронную информационно-образовательную среду университета.   |
| Лаборатория радиомониторинга и контроля утечек информации, ауд. 226                             | Персональные компьютеры с ПО:<br>- Операционная система MS Windows 7 - <i>Microsoft Imagine - PremiumD-1227-18 от 08.10.2018 до 08.10.2021</i> ;<br>- DLP «SecureTower» (Лицензионный ключ - 9752920000005A48, бессрочная в рамках договора).                                                                                                                                        |
| Лаборатория систем передачи информации, ауд. 2124                                               | Стенд коммуникационного оборудования с сервером для моделирования облачного сервиса.                                                                                                                                                                                                                                                                                                 |
| Аудитории для самостоятельной работы (ауд.132а): компьютерные классы; читальные залы библиотеки | Персональные компьютеры с ПО:<br>- Операционная система MS Windows 7 - <i>Microsoft Imagine - PremiumD-1227-18 от 08.10.2018 до 08.10.2021</i> ;<br>- Пакет MS Office 2007 - <i>Microsoft Open License 42649837, бессрочная</i> ;<br>- Архиватор 7zip - <i>GNU LGPL, бессрочная</i> ;<br>- Выход в Интернет и доступ в электронную информационно-образовательную среду университета. |