

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
«15» марта 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

шифр 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

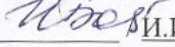
Энергетики и автоматизированных систем
Информатики и информационной безопасности
4,5
8,9

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)

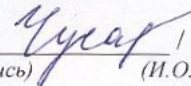
Рабочая программа составлена:

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)

1 Цели освоения дисциплины (модуля)

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 (модуля) в структуре образовательной программы

Дисциплина Управление информационной безопасностью входит в базовую часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организационное и правовое обеспечение информационной безопасности

Основы информационной безопасности

Разработка и эксплуатация защищенных автоматизированных систем

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Производственная-преддипломная практика

Подготовка к защите и защита выпускной квалификационной работы

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

В результате освоения дисциплины (модуля) «Управление информационной безопасностью» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	
Знать	- задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики ИБ организации;
Уметь	- разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.

Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.
ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз.
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - 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.
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации.
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	
Знать	- основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС.
Уметь	- разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследовать инциденты ИБ.
Владеть	- навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом построения СУИБ.
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	

Знать	<ul style="list-style-type: none"> - основы законодательства Российской Федерации; - нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.
Уметь	<ul style="list-style-type: none"> - обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей; - предпринимать необходимые меры по восстановлению нарушенных прав.
Владеть	<ul style="list-style-type: none"> - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов.
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Знать	<ul style="list-style-type: none"> - основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики информационной безопасности организации.
Уметь	<ul style="list-style-type: none"> - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС.
Владеть	<ul style="list-style-type: none"> - навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать	<p>Ключевые процессы менеджмента ИБ</p> <p>Требования нормативно-правовых документов, регламентирующих систему менеджмента</p>
Уметь	<p>Проводить оценку состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации</p> <p>Определять цели применения мер и средств контроля и управления для обработки рисков</p>
Владеть	<p>Навыками выбора необходимых мер и средств контроля и управления ИБ</p> <p>Навыками определения способов измерения результативности выбранных мер управления ИБ</p>

ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на <u>предприятии и в учреждении</u>	
Знать	Этапы построения и использования СМИБ Семейство стандартов ISO/IEC 27000
Уметь	Оценивать уровень знаний сотрудников в области ИБ Разрабатывать программы по обучению и повышению квалификации сотрудников в области ИБ Выявлять возможности улучшения СМИБ
Владеть	Навыками разработки плана обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ

4. Структура, объём и содержание дисциплины (модуля)

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

- контактная работа – 142,8 академических часов;
- аудиторная – 136 академических часов;
- внеаудиторная – 6,8 академических часов
- самостоятельная работа – 109,5 академических часов;
- подготовка к экзамену – 35,7 академических часов

Форма аттестации - зачет, курсовая работа, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в академических часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Создание системы управления информационной безопасностью								
1.1 Основные принципы создания системы управления информационной безопасностью. Структура системы управления информационной безопасностью.	8	8		8/4И	8	Подготовка структуры СУИБ заданного ОИ.	ИДЗ, Отчет на образовательном портале	ПК-11, ПК-12, ОК-4
1.2 Проектирование систем ИБ. Внедрение ISO 27001/17799.		4		4	6	Изучение этапов проектирования	Устный опрос. ИДЗ, Отчет на образовательном портале	ПК-11, ПК-19, ПК-22

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

Итого по разделу	34		34/23И	71,3			
Итого за семестр	34		34/40И	71,3		экзамен,кр	
Итого по дисциплине	68		68/40И	109,5		зачет, курсовая работа, экзамен	ПК-11,ПК-12,ОК-4,ПК-19,ПК-22,ПК-28

5 Образовательные 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	
ОК-4 - способностью использовать основы правовых знаний в различных сферах деятельности		
Знать	<ul style="list-style-type: none"> - основы законодательства Российской Федерации; - нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации; - правовые основы организации защиты государственной тайны и конфиденциальной информации; - меры правовой и дисциплинарной ответственности за разглашение защищаемой информации. 	<p>Теоретические вопросы</p> <ol style="list-style-type: none"> 1. Перечислить стандарты, относящиеся к управлению информационной безопасностью. 2. Основные положения стандарта управления информационной безопасностью BS 7799. 3. Основные положения стандарта управления информационной безопасностью ISO/IEC 17799. 4. Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования.»
Уметь	<ul style="list-style-type: none"> - обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей; - предпринимать необходимые меры по восстановлению нарушенных прав. 	Сформулировать цели внедрения ISO 27001/17799 в организации. Провести сертификацию заданной СУИБ на соответствие ISO 27001.
Владеть	<ul style="list-style-type: none"> - навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов. 	Описать этапы разработки и внедрения системы управления ИБ
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы		
Знать	<ul style="list-style-type: none"> - задачи органов защиты государственной тайны и служб защиты информации на предприятиях; - систему организационных мер, направленных на защиту информации ограниченного доступа - нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; - основные угрозы безопасности информации и модели нарушителя объекта информатизации; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; 	<p>Теоретические вопросы</p> <ol style="list-style-type: none"> 1. Что относится к административному уровню обеспечения информационной безопасности? 2. Что относится к среднему уровню обеспечения информационной безопасности? 3. Что относится к нижнему уровню обеспечения информационной безопасности? 4. Организация режима секретности. 5. Принципы формирования политики информационной безопасности организации.

Структурный элемент компетенции	Планируемые результаты обучения	
	- принципы формирования политики ИБ организации;	
Уметь	- разрабатывать модели угроз и модели нарушителя ОИ; - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; - разрабатывать предложения по совершенствованию системы управления ИБ АС.	1. Разработать частную модель угроз для заданного ОИ. Составить предложения по совершенствованию системы управления информационной безопасностью.
Владеть	- навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней.	1. На основе частной модели угроз разработать заданную политику безопасности.
ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы		
Знать	- особенности решений по ЗИ в информационных процессах и системах; - определения рисков ИБ применительно к ОИ с заданными характеристиками; - методы и подходы к реализации системы управления безопасностью АИС; - методы анализа процессов для определения актуальных угроз.	Теоретические вопросы 1. Основные принципы организации СУИБ. 2. Что понимают под профилем защиты. 3. Содержание профиля защиты. 4. Что включает в себя методика определения защищенности ИС. 5. Что включает в себя активное и пассивное тестирование системы защиты. 6. Методики определения рисков.
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - разрабатывать политики безопасности информации АС; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ.	Провести анализ защищенности заданного ОИ.
Владеть	- навыками управления рисками ИБ, навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	Подготовить отчет по проведенному анализу защищенности: 1. Общие описание объекта обследования 2. Структура и состав комплекса программно-технических средств
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы		
Знать	- нормативные методические документы ФСТЭК России в области ИБ; - основные угрозы безопасности	1. Назовите основные угрозы безопасности информации 2. Дайте описание внешнего нарушителя 3. Кто относится к внутренним

Структурный элемент компетенции	Планируемые результаты обучения	
	информации и модели нарушителя в ИС; - стратегии обеспечения ИБ, способы их организации и оптимизации.	нарушителям 4. Цели тестирования системы защиты
Уметь	- оценивать различные инструменты в области проектирования и управления ИБ; - обосновывать решения по обеспечению ИБ объектов в профессиональной сфере деятельности; - расследовать инциденты ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	1. Провести анализ защищенности внешнего периметра корпоративной сети. 2. Провести анализ защищенности внутренней организации сетевой корпоративной инфраструктуры.
Владеть	- навыками расчета и управления рисками ИБ; - навыками разработки положения о применимости механизмов контроля в контексте управления рисками ИБ.	По проведенному анализу защищенности подготовить: 1. Рекомендации по устранению уязвимостей внешнего периметра сети. 2. Рекомендации по устранению уязвимостей внутренней организации сетевой корпоративной инфраструктуры.
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации		
Знать	- основные угрозы безопасности информации и модели нарушителя ОИ; - правовые основы организации защиты ПДн и охраны результатов интеллектуальной деятельности; - принципы формирования политики информационной безопасности организации.	1. Комплект типовых документов по информационной безопасности. 2. Типовые документы для внедрения СУИБ организации. 3. Комплект типовых документов для операторов ПДн: а. Проектная документация; б. Положения и политики; в. Планы; г. Инструкции и регламенты; д. Приказы; е. Акты; ж. Журналы; з. Перечни; и. Обязательства и уведомления; к. Согласия субъекта. 4. Комплект типовых документов для управления рисками информационной безопасности. 5. Методика анализа защищенности ИС. 6. Последовательность мероприятий по анализу защищенности. 7. Структура отчета по результатам анализа защищенности. 8. Тестирование системы защиты

Структурный элемент компетенции	Планируемые результаты обучения	
		<p>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>
Уметь	<ul style="list-style-type: none"> - разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих ЗИ ограниченного доступа в организации; - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - разрабатывать частные политики ИБ АС; - контролировать эффективность принятых мер по реализации частных политик ИБ АС. 	<ol style="list-style-type: none"> 1. Разработать заданную частную политику информационной безопасности. 2. Составить описание информационной инфраструктуры организации. 3. Выбрать и обосновать меры защиты информационных ресурсов.
Владеть	<ul style="list-style-type: none"> - навыками выявления угроз безопасности информации в АС; - владеть навыками разработки политик безопасности различных уровней. 	Разработать комплекс внутренних организационно-распорядительных документов по ОБИ для образовательного учреждения
ПК-28 способностью управлять информационной безопасностью автоматизированной системы		
Знать	<ul style="list-style-type: none"> - основные угрозы безопасности информации и модели нарушителя в ИС; - основные меры по ЗИ в АС. 	<ol style="list-style-type: none"> 1. Назовите основные угрозы безопасности информации. 2. Дайте описание внешнего нарушителя. 3. Кто относится к внутренним нарушителям. 4. На какие группы разделяют инциденты ИБ. 5. Расследование инцидентов ИБ.
Уметь	<ul style="list-style-type: none"> - разрабатывать нормативно-методические материалы по регламентации системы организационной ЗИ; - расследовать инциденты ИБ. 	<ol style="list-style-type: none"> 1. Описать процесс расследования инцидента 2. Составить заключение по проведенному расследованию. 3. Подготовить типовой комплект документов СУИБ.
Владеть	<ul style="list-style-type: none"> - навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АС; - терминологией и процессным подходом построения СУИБ. 	Разработать Технические политики (Technical Policy) информационной безопасности на предприятии.

Структурный элемент компетенции	Планируемые результаты обучения	
ПСК-7.2 способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах		
Знать	Ключевые процессы менеджмента ИБ Требования нормативно-правовых документов, регламентирующих систему менеджмента информационной безопасности (СМИБ)	<ol style="list-style-type: none"> 1. Основные принципы создания СУИБ. 2. Процедура внедрения СУИБ. 3. Разработка политик ИБ. 4. Разработка профилей защиты и заданий по безопасности. 5. Организация режима секретности. 6. Технические политики ИБ на предприятии. 7. Идентификация рисков 8. Процессный подход для
Уметь	Проводить оценку состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации Определять цели применения мер и средств контроля и управления для обработки рисков	Подготовить отчет по проведенному анализу защищенности выбранного объекта: <ol style="list-style-type: none"> 1. Идентификацию рисков 2. Идентификацию активов и определение их владельцев 3. Идентификация угроз в отношении активов 4. Идентификация уязвимостей 5. Результаты анализа
Владеть	Навыками выбора необходимых мер и средств контроля и управления ИБ Навыками определения способов измерения результативности выбранных мер управления ИБ	По проведенному анализу защищенности подготовить: <ol style="list-style-type: none"> 1. Рекомендации по устранению уязвимостей внутренней ИТ-инфраструктуры. 2. Рекомендации по устранению обнаруженных недостатков и повышению уровня защищенности
ПСК-7.5 способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении		
Знать	Этапы построения и использования СМИБ Семейство стандартов ISO/IEC 27000	<ol style="list-style-type: none"> 1. Способы контроля и оценки эффективности имеющихся средств управления и процедур ИБ 2. Интегральный показатель эффективности СМИБ

Структурный элемент компетенции	Планируемые результаты обучения	
Уметь	Оценивать уровень знаний сотрудников в области ИБ Разрабатывать программы по обучению и повышению квалификации сотрудников в области ИБ Выявлять возможности улучшения СМИБ	Подготовить отчет по проведенному анализу защищенности: 1. Результаты анализа организационных уязвимостей 2. Распределение между ответственными лицами задач систем безопасности 3. Разработать методику оценки знаний сотрудников в области ИБ 4. Разработать инструкции для сотрудников по обеспечению организации защиты информации по
Владеть	Навыками разработки плана обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ	По проведенному анализу защищенности подготовить: 1. Рекомендации по устранению организационных уязвимостей. 2. Разработать указания и требования Политики ИБ с учетом внедрения программно-аппаратных комплексов и

Примерные темы курсовых работ:

1. Разработка комплекса внутренних организационно-распорядительных документов по ОБИ для заданного объекта информатизации (варианты различаются исходными данными на объект).

2. Разработка Задания по безопасности для заданного объекта информатизации (варианты различаются исходными данными на объект).

3. Разработка Профиля защиты для заданного объекта информатизации (варианты различаются исходными данными на объект).

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. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/997108> (дата обращения: 15.02.2020)

2.Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/422772> (дата обращения: 15.02.2020).

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). —

ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/414083> (дата обращения: 15.02.2020).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж: Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/923295> (дата обращения: 15.02.2020)

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

Макрообъект*.

***РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ**

1. Перейти по адресу электронного каталога <https://magtu.informsystema.ru>.
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта.

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты.

в) Методические указания:

1. Методические указания по выполнению практических работ (Приложение 1).
2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
7Zip	свободно	бессрочно
LibreOffice	свободно	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021

MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Yandex	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Федеральная служба по техническому и экспортному контролю России (ФСТЭК)	URL: www.fstec.ru
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Федеральное агентство по техническому регулированию и метрологии (Росстандарт)	URL: https://www.rst.gov.ru/portal/gost/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

- Мультимедийные средства хранения, передачи и представления информации.

Компьютерные классы:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Лаборатория сетей и систем передачи данных. Лаборатория безопасности сетей ЭВМ:

- Стенд коммуникационного оборудования сервером для моделирования облачного сервиса.

Лаборатория программно-аппаратных средств обеспечения защиты информации:

- DLP «SecureTower» (Лицензионный ключ - 9752920000005A48, бессрочная в рамках договора)

Помещения для самостоятельной работы обучающихся: - Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Рекомендации направлены на оказание методической помощи студентам при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности студентов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы ИТ, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы студент демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ
САМОСТОЯТЕЛЬНЫХ РАБОТ**

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

- 1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
 - а) предоставляемыми преподавателем на лекционных занятиях;
 - б) предоставляемыми преподавателем в рамках электронных образовательных курсов;
 - с) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
- 2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
- 3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
- 4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами

группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.6) «Оценочные средства для проведения промежуточной аттестации» данной РПД.