МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2019 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____У.В. Михайлова

Рецензент:
Начальник отдела информационной безопасности АО "КУБ",

_____М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» являются: обучить обучающихся практическим навыкам работы с нормативно-правовой базой деятельности в области обеспечения безопасности информации. Знания и практические навыки, полученные в курсе «Организационное и правовое обеспечение информационной безопасности» используются обучаемыми при разработке курсовых и дипломных работ.

Задачи дисциплины:

• дать представление о законодательстве РФ в области информации;

• ознакомить с системой защиты государственной тайны;

• ознакомить с правилами лицензирования и сертификации в области защиты информации;

• ознакомить с организационными методами защиты информации;

• ознакомить с методами обеспечения информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Организационное и правовое обеспечение информационной безопасности входит в базовую часть учебного плана образовательной программы.

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

Введение в специальность

Основы информационной безопасности

Информационная безопасность распределенных информационных систем

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

Методы выявления нарушений информационной безопасности, аттестация АИС

Моделирование угроз информационной безопасности

Методы мониторинга информационной безопасности АС

Защита электронного документооборота

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Управление информационной безопасностью

Анализ рисков информационной безопасности

Защита программного обеспечения

Информационная безопасность систем организационного управления

Методы проектирования защищенных распределенных информационных систем

Моделирование систем и процессов защиты информации

Научно-исследовательская работа

Подготовка к защите и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

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

В результате освоения дисциплины (модуля) «Организационное и правовое обеспечение информационной безопасности» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	
Знать	-основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; -правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности - владения юридической терминологией; -навыками работы с правовыми актами; навыками реализации правовых норм; навыками принятия необходимых мер правового регулирования и (или) защиты интересов субъектов правовых отношений
Владеть	-навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	
Знать	-виды тайн, закрепленные в российском законодательстве -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях -основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях

Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Владеть	-навыками работы с нормативными правовыми актами -навыками подготовки деловой корреспонденции
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	
Знать	-нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов
Уметь	-разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Владеть	-способностью разрабатывать научно-техническую документацию
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	
Знать	основные меры по защите информации в автоматизированных системах (организационные, правовые); автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности
Уметь	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия разрабатывать предложения по совершенствованию системы управления ИБ
Владеть	методами организации и управления деятельностью служб защиты информации на предприятии
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	
Знать	-организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации -организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
Уметь	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров

Владеть	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований, -методами организации и управления деятельностью служб защиты информации на предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 51,95 акад. часов:

– аудиторная – 51 акад. часов;

– внеаудиторная – 0,95 акад. часов

– самостоятельная работа – 56,05 акад. часов;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Правовое обеспечение информационной								
1.1 Законодательство РФ в области информационной безопасности: Основы законодательства Российской федерации в области информационной безопасности. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты	7	1		2	4	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала и ЭБС. Самостоятельная работа с интернет-источниками	Устный опрос, тестирование	ОК-4
1.2 Правовой режим защиты государственной тайны: Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Система нормативных правовых актов, регламентиру-ющих обеспечение сохранности сведений, составляющих государственную тайну в РФ.		2		4/1И	8	Самостоятельное изучение учебной литературы и конспектов лекций, публикаций в периодических изданиях. Работа с Интернет-ресурсами. Изучение нормативной документации. Подготовка к аудиторным контрольным работам.	Аудиторная контрольная работа	ОК-4, ОПК-6

1.3 Лицензирование в области защиты информации: Понятие лицензирования. Нормативные правовые акты РФ, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации.		3		4/1И	8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Индивидуальное домашнее задание	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
1.4 Сертификация в области защиты информации: Понятие сертификации. Нормативные правовые акты РФ и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации.		2		4/2И	6	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала. Подготовка и выполнение ИДЗ	Индивидуальное домашнее задание	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
1.5 Законодательство РФ в области конфиденциальной информации и коммерческой тайны. Ответственность.		1		2/2И	1,5	Самостоятельное изучение учебной и научной литературы, работа с материалами образовательного портала.	Устный опрос	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
Итого по разделу		9		16/6И	27,5			
2. Организационное обеспечение информационной безопасности								
2.1 Понятие организационной защиты информации. Сущность организационных методов защиты информации.	7	2		4/2И	8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Устный опрос	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
2.2 Анализ и оценка угроз информационной безопасности объекта. Методы и способы анализа угроз безопасности информации. Порядок проведения оценки опасности угрозы.		2		4/2И	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Устный опрос	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18

2.3 Оценка ущерба: Понятие ущерба. Методы и способы оценки ущерба.		1		2/1И	3	Поиск дополнительной информации по заданной теме.	Индивидуальное домашнее задание	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
2.4 Служба безопасности объекта: Место службы безопасности объекта в общей структуре системы защиты государственной тайны и государственной системы защиты информации. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности.		1		2/1И	1,5	Подготовка к компьютерному тестированию. Самостоятельная работа с интернет-источниками.	Компьютерное тестирование	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
2.5 Средства и методы физической защиты объекта: Объекты обеспечения физической без-опасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового		1		4/1И	4,05	Поиск дополнительной информации по заданной теме.	Индивидуальное домашнее задание	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
2.6 Организация и обеспечение режима секретности: Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. Требования к помещениям и хранилищам, в которых ведут-ся закрытые работы. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. Защита информации в		1		2/1И	6	Самостоятельное изучение учебной и научной литературы, работа с материаламиобразова-тельного портала и ЭБС. Самостоятельная работа с интернет-источниками	Тестирование	ОК-4, ОПК-6, ПК-7, ПК-21, ПК-18
Итого по разделу		8		18/8И	28,55			
Итого за семестр		17		34/14И	56,05		зачёт	
Итого по дисциплине		17		34/14И	56,05		зачет	ОК-4,ОПК-6,ПК-7,ПК-21,ПК-18

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Организационное и правовое обеспечение информационной безопасности» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного 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, обществен-ной 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.

выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», ре-конструкцией 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 IT

— 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 пор-тале.

• 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.

— 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 «Организационное и правовое обеспечение информационной безопасности» 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 обучающегося.

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):

Тема 1.1. Задание 1. Выбрать, вид и область деятельности, название фирмы. Составить план мероприятий по защите коммерческой тайны (в соответствии с законом РФ «О коммерческой тайне»). Указать перечень внутрифирменных документов, которые будут использоваться в целях правовой защиты секретов фирмы. Составить перечень сведений, составляющих коммерческую тайну фирмы. Описать методы конкурентной разведки, которые будут использоваться информационно-аналитической службой.

Тема 1.4. Задание 2. Обосновать необходимость проведения лицензирования выбранного вида деятельности. Указать порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности. Указать перечень сертификационных документов, необходимых для выбранной деятельности фирмы. Составить для фирмы документы, необходимые для осуществления заданного вида деятельности.

7. Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
ОК 4 - способностью использовать основы правовых знаний в различных сферах деятельности		
Знать	-основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты	Теоретические вопросы Основы законодательства Российской федерации в области информационной безопасности. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты информации. Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Понятие лицензирования. Нормативные

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
	государственной тайны и служб защиты информации на предприятиях;	правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. Нормативные правовые акты Российской Федерации, определяющие требования к защите авторских и смежных прав Сущность организационных методов защиты информации. . Понятие угрозы безопасности информации. . Методы и способы анализа угроз безопасности информации. Порядок проведения оценки опасности угрозы . Понятие ущерба. Методы и способы оценки ущерба.
Уметь:	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности - владения юридической терминологией; -навыками работы с правовыми актами; навыками реализации правовых норм; навыками принятия необходимых мер правового регулирования и (или) защиты интересов субъектов правовых отношений	Указать перечень сертификационных документов, необходимых для выбранной деятельности фирмы. Составить для фирмы документы, необходимые для осуществления заданного вида деятельности
Владеть:	-навыками работы с нормативными правовыми актами, нормотворческой деятельности, работы с законами и иными нормативными правовыми актами и применения их на практике	Задание. Обосновать необходимость проведения лицензирования выбранного вида деятельности. Указать порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности.

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности		
Знать	-виды тайн, закрепленные в российском законодательстве -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях -основы организационного и правового обеспечения информационной безопасности, -основные нормативные правовые акты в области обеспечения информационной безопасности - нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; -правовые основы организации защиты государственной тайны и конфиденциальной информации, -задачи органов защиты государственной тайны и служб защиты информации на предприятиях	Теоретические вопросы 1. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 2. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. 3. Требования к помещениям и хранилищам, в которых ведутся закрытые работы. 4. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. 5. Защита информации в экстремальных ситуациях. 6. Виды информации, подлежащие защите в соответствии с законодательством Российской Федерации. 7. Государственная тайна. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 8. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. 9. Лицензионные требования ФСТЭК России на деятельность по технической защите конфиденциальной информации. 10. Лицензионные требования ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. 11. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		информации
Уметь:	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	Задача. Определение способы реализации угроз безопасности информации для типового предприятия согласно заданию. Определить контролируемую зону, «ОТСС», «ВТСС», «зону 2», «зону 1», «контролируемая зона (КЗ)».
Владеть:	-навыками работы с нормативными правовыми актами -навыками подготовки деловой корреспонденции	Задача. Используя методы и способы анализа угроз безопасности информации, определить соотношения «зоны 2» и «зоны 1» по отношению к размеру «контролируемой зона (КЗ)» для решения задач технической защиты информации.
ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ		
Знать	нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности, структуру научно-технических отчетов	Теоретические вопросы 1. Виды информации, подлежащие защите в соответствии с законодательством Российской Федерации. 2. Государственная тайна. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 3. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. 4. Лицензионные требования ФСТЭК России на деятельность по технической защите конфиденциальной информации. 5. Лицензионные требования ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. 6. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		7. Определение понятия «угроза безопасности информации». Способы реализации угроз безопасности информации.. Определение понятий «контролируемая зона», «ОТСС», «ВТСС», «зона 2», «зона 1», «контролируемая зона (КЗ)». 8. Методы и способы анализа угроз безопасности информации. Соотношения «зоны 2» и «зоны 1» по отношению к размеру «контролируемой зона (КЗ)». при решении задач технической защиты информации. 9. Порядок проведения оценки опасности угрозы. 10. Понятие ущерба. Методы и способы оценки ущерба. 11. Структура системы защиты государственной тайны и государственной системы защиты информации. Место службы безопасности объекта 12. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. 13. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности. 14. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 15. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. 16. Требования к помещениям и хранилищам, в которых ведутся закрытые работы. 17. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей.
Уметь:	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;	Задача. Оценить угрозы информационным ресурсам выбранного предприятия (укажите наиболее вероятные виды компьютерных преступлений). Указать мероприятия, проводимые при создании системы защиты информации в вашей

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	компьютерной сети. Укажите перечень РД ФСТЭК, учитываемых при разработке «Политики безопасности» на вашем предприятии. Определите и обоснуйте требования по защите вашей конфиденциальной информации - группу и класс защищенности СВТ от НСД.
Владеть:	способностью разрабатывать научно-техническую документацию	Задача. Указать цель обеспечения информационной безопасности предприятия. Задать величину степени защищенности создаваемой на объекте системы защиты информации и стоимость используемых активов АС. Выбрать и обосновать стратегические принципы безопасности АС. Оценить величину ущерба активам АС при реализации угроз. Рассчитать ожидаемые потери после создания системы информационной безопасности.
ПК-18 **способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности**		
Знать	организацию деятельности службы безопасности объекта по основным направлениям работ по защите информации организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	Теоретические вопросы 18. Задачи, решаемые службой безопасности объекта. Структура и состав службы безопасности объекта. 19. Роль и место подразделения (штатного специалиста) по технической защите информации, решаемые задачи, права и обязанности. 20. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 21. Допуск должностных лиц к государственной тайне и к информации ограниченного доступа, не отнесенной к государственной тайне. 22. Требования к помещениям и хранилищам, в которых ведутся закрытые работы. 23. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. 24. Защита информации в экстремальных ситуациях.

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
Уметь:	-применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности -анализировать и обобщения информации на стадии принятия и реализации управленческого решения, -пользоваться конструктивной критикой, учитывать мнения коллег и подчиненных, осуществлять подбор и расстановки кадров	Задача. Описать выбранный объект обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима.
Владеть:	-навыками ведения деловых переговоров, публичного выступления, взаимодействия с другими ведомствами, государственными органами, представителями субъектов Российской Федерации, муниципальных образований, -методами организации и управления деятельностью служб защиты информации на предприятии -навыками организации и обеспечения режима секретности -навыками планирования работы, контроля, анализа и прогнозирования последствий принимаемых решений, стимулирования достижения результатов,	Задача: Описать требования к помещениям и хранилищам, в которых ведутся закрытые работы. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. Защита информации в экстремальных ситуациях.
ПК- 21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем		
Знать	основные меры по защите информации в автоматизированных системах (организационные, правовые); автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и	Теоретические вопросы 1. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. 2. Лицензируемые виды деятельности в области защиты информации. 3. Порядок получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
	методы обеспечения ее информационной безопасности	информации. Существующие лицензионные требования. 4. Порядок получения лицензии ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации. 5. Существующие лицензионные требования. 6. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации
Уметь:	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; оценивать автоматизированную систему как объект информационного воздействия разрабатывать предложения по совершенствованию системы управления ИБ	Задача. Разработать проект документа «Допуск должностных лиц к информации ограниченного доступа, не отнесенной к государственной тайне».
Владеть:	методами организации и управления деятельностью служб защиты информации на предприятии	Задача. Разработать проект документа «Оценка соответствия помещения требованиям к помещениям и хранилищам, в которых ведутся закрытые работы.

Критерии оценки

– 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.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. 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: 24.02.2020).

2. Баранкова, И.И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности: учебное пособие / И. И. Баранкова, О. В. Пермякова; МГТУ. - Магнитогорск: МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true (дата обращения: 04.10.2019). - Макрообъект. - Текст: электронный. - ISBN 978-5-9967-1031-7. - Сведения доступны также на CD-ROM.

б) Дополнительная литература:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

3. Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне».

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

7. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 09.09.2000 № Пр-1895)

8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.

9. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

10. ГОСТ Р 50922-2006 «Национальный стандарт российской федерации. Защита информации. Основные термины и определения».

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 классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
FAR Manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Сетевой ресурс (Сайт ФСТЭК)	URL: www.fstec.ru
Сетевой ресурс (Сайт РОССТАНДАРТ)	URL: https://www.rst.gov.ru/portal/gost
Банк данных угроз безопасности информации ФСТЭК России	URL: https://bdu.fstec.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1. Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.

2. Компьютерные классы с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

3. Мультимедийные поточные аудитории университета с мультимедийными средствами хранения, передачи и представления информации

ПРИЛОЖЕНИЕ 1

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 или учебной специализированной лаборатории 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 IT, 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.

ПРИЛОЖЕНИЕ 2

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):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) 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.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.