МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
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
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2018 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)

«07» сентября 2018 г., протокол № 1.

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

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

«26» сентября 2018 г., протокол № 1.

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

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

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

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

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

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1. Цели освоения дисциплины

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 в структуре образовательной программы подготовки специалиста

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в базовую часть блока 1 образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Для изучения дисциплины необходимы знания (умения, навыки), сформированные в результате изучения дисциплин: «Основы информационной безопасности», «Введение в специальность».

Знания (умения, навыки), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин «Основы управленческой деятельности», «Управление информационной безопасностью».

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: ОК-4; ОПК-6; ПК-7; ПК-18; ПК-21

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

Структурный элемент компетенции	**Планируемые результаты обучения**
	- 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-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

Структурный элемент компетенции	**Планируемые результаты обучения**
	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,
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

4 Структура 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 кад. часов
- самостоятельная работа – 56,05 акад. часов;

Семестр7, зачет

Раздел/ тема дисциплины	Аудиторная контактная работа (в акад. часах))		самост. работа	Вид самост работы	Формы текущего и промежуточного контроля успеваемости	Код и структурный элемент компетенции
	лекции	активпрактич. занятия / в				
Раздел 1. Правовое обеспечение информационной безопасности						
1.1. Законодательство Российской Федерации в области информационной безопасности Основы законодательства Российской федерации в области информационной безопасности. Понятие и виды защищаемой информации. Основы международного законодательства в области защиты информации.	1	2	4	Самостоятельное изучение учебной инаучной литературы, работа с материаламиобразовательного портала и ЭБС. Самостоятельная работа с интернет-источниками	Опрос, тестирование, ИДЗ	ОК-4-зув; ОПК-6-зув
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, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.	2	4/1	8	Самостоятельное изучение учебной литературы и конспектов лекций, публикаций в периодических изданиях . Работа с Интернет-ресурсами. Изучение нормативной документации. Подготовка к аудиторным контрольным работам.	Опрос, тестирование	ОК-4-зув; ОПК-6-зув, ПК-7-зу
1.3. Лицензирование в области защиты информации Понятие лицензирования. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты	3	4/1	8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала.	Проверка ИДЗ, обсуждение промежуточных	ОПК-6-зув, ПК-7 - з

информации.					результатов	
1.4. Сертификация 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.	2	4/1	6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала. Подготовка и выполнение ИДЗ	Опрос, коллоквиум, проверка ИДЗ	ОПК-6-зув, ПК-7 – зув, ПК-21-7-зу
Раздел 2. Организационное обеспечение информационной безопасности						
2.1. Понятие организационной защиты информации Сущность организационных методов защиты информации.	2	4/2	8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к практическим занятиям.	Опрос, тестирование Проверка ИДЗ	ПК-7-зув; ПК-18-з
2.2. Анализ и оценка угроз информационной безопасности объекта Понятие угрозы безопасности информации. Методы и способы анализа угроз безопасности информации. Порядок проведения оценки опасности угрозы	2	4/2	6	Подготовка к практическим занятиям. Выполнение ИДЗ	Опрос, тестирование, Проверка ИДЗ	ПК-7-зув; ПК-18-зув
2.3. Оценка ущерба Понятие ущерба. Методы и способы оценки ущерба.	1	2/2	3	Поиск дополнительной информации по заданной теме.	Опрос, коллоквиум	ОПК-6-зув, ПК-7-ЗУ
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.	2	4/2	3	Подбор, описание, экспертная оценка сайтов Интернет. Подготовка к компьютерному тестированию. Самостоятельная работа с интернет-источниками	Опрос, тестирование	ПК-7-зув; ПК-18-зув
2.5. Средства и методы физической защиты объекта Объекты обеспечения физической	1	4/2	4,05	Поиск дополнительной информации по	Опрос, коллоквиум	ПК-18-зу;

безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима.				заданной теме		ПК-21-зу
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 ведутся закрытые работы. Организация защиты информации при приеме посетителей, командированных лиц и иностранных представителей. Защита информации в экстремальных ситуациях.	1	2/1	6	Самостоятельное изучение учебной инаучной литературы, работа с материаламиобразовательного портала и ЭБС. Самостоятельная работа с интернет-источниками	Опрос, тестирование	ПК-18-зув; ПК-21-зув
Итого по дисциплине	**17**	**34/14**	**56,05**			

5 Образовательные и информационные 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, 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 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 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 «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.

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	Теоретические вопросы 1. Основы законодательства Российской

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
	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;	федерации в области информационной безопасности. 2. Понятие и виды защищаемой информации. 3. Основы международного законодательства в области защиты информации. 4. Понятие государственной тайны. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны. 5. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. 6. Понятие лицензирования. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в област изащиты информации. 7. Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. 8. Нормативные правовые акты Российской Федерации, определяющие требования к защите авторских и смежных прав 9. Сущность организационных методов

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		защиты информации. 10. Понятие угрозы безопасности информации. 11. Методы и способы анализа угроз безопасности информации. Порядок проведения оценки опасности угрозы 12. 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..
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,	Теоретические вопросы 1. Объекты обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима. 2. Допуск должностных лиц

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
	-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	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.

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		11. Сертификация. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты 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

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		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 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

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		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; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	Задача. Оценить угрозы информационным ресурсам выбранного предприятия (укажите наиболее вероятные виды компьютерных преступлений). Указать мероприятия, проводимые при создании системы защиты информации в вашей 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.

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		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.
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,	Задача. Описать выбранный объект обеспечения физической безопасности: сооружения, предметы, люди. Организация охраны, пропускного и внутриобъектового режима.

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
	-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,	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 методы обеспечения ее информационной безопасности	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 информации. Существующие лицензионные требования. 4. Порядок получения лицензии ФСТЭК России на деятельность по

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
		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.

8Учебно-методическое и информационное обеспечениедисциплины (модуля)

а) основная литература:

1) Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н. Н. Куняев. - М.:

Логос, 2010. - 348 с. Режим доступа: http://znanium.com/bookread.php?book=469026.–Заглавие с экрана. - ISBN 978-5-98704-513-8.
2) Логунов, А.Б. Региональная и национальная безопасность [Электронный ресурс]: Учебное пособие / А.Б. Логунов. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с. Режим доступа: http://znanium.com/bookread.php?book=406872.–Заглавие с экрана.–ISBN 978-5-9558-0310-4.
3) Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/bookread.php?book=405000.–Заглавие с экрана.
4) Гришина, Н.В. Информационная безопасность предприятия [Электронный ресурс]: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.- (Высшее образование:Бакалавриат).–ISBN 978-5-00091-007-8. Режим доступа: http://znanium.com/bookread.php?book=491597.–Заглавие с экрана. –ISBN 978-5-00091-007-8.

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) Программное обеспечение и Интернет-ресурсы:

1. ФСТЭК России Федеральная служба по техническому и экспортному контролю http://fstec.ru
2. Журнал InformationSecurity. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
3. Журнал «Безопасность информационных технологий» :периодич. интернет-изд. URL: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.
4. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
5. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". URL: http://www.osp.ru/os/– Загл. с экрана. Яз. рус.

6. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.
7. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. – Загл. с экрана. Яз. рус.
8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные :периодич. интернет-изд. URL: http://www.computerra.ru/ – Загл. с экрана. Яз.рус.
9. http://www.безопасник.рф– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины(модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Мультимедийные поточные аудитории университета	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс	Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета
Программные средства:	Windows(Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021) MS Office(Microsoft Open License 42649837, бессрочная) и выходом в Интернет
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.