МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины
«Организационное и правовое обеспечение информационной безопасности»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /Л.В. Паринова/

Заведующий кафедрой
Систем информационной
безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

Основная цель преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» - раскрыть:

-основы правового регулирования отношений в информационной сфере;

-конституционные гарантии прав граждан на получение информации и механизм их реализации;

-понятия и виды защищаемой информации по законодательству РФ;

-систему защиты государственной тайны;

-основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности;

-понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование некоторых практических навыков работы

1.2.Задачиосвоениядисциплины

1.2.1. Дать основы:

– законодательства РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации;

– понятий и видов защищаемой информации по законодательству РФ;

– правовых режимов конфиденциальной информации;

– правового режима защиты государственной тайны, системы защиты государственной
тайны;

– лицензирования и сертификации в области защиты информации, в том числе государственной тайны;

– правовых основ защиты информации с использованием технических средств (защита
от технических разведок, применение и разработка шифровальных средств, электронная
цифровая подпись и т.д.);

– защиты интеллектуальной собственности;

– правовой регламентации охранной деятельности;

– правового регулирования взаимоотношений администрации и персонала в области
защиты информации;

– международного законодательства в области защиты информации;

– знаний о преступлениях в сфере компьютерной информации, экспертизах преступлений в области компьютерной информации, криминалистических аспектах
проведения расследований.

– угроз информационной безопасности объекта;

– организации службы безопасности объекта;

– подбора и работы с кадрами в сфере информационной безопасности;

– организации и обеспечения режима конфиденциальности.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Организационноеиправовоеобеспечениеинформационной безопасности»относитсякдисциплинамбазовойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Организационноеиправовоеобеспечение информационнойбезопасности»направленнаформированиеследующихкомпетенций:

ОК-4-способностьюиспользоватьосновыправовыхзнанийвразличныхсферахдеятельности

ОПК-5-способностьюиспользоватьнормативныеправовыеактывсвоейпрофессиональнойдеятельности

ОПК-6-способностьюприменятьприемыоказанияпервойпомощи,методызащитыпроизводственногоперсоналаинаселениявусловияхчрезвычайныхситуаций

ПК-1-способностьюосуществлятьподбор,изучениеиобобщениенаучно-технической информации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности,атакженормативныхправовыхактоввсферепрофессиональнойдеятельности

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
ОК-4	знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности
	уметь применять необходимые положения нормативно-правовых актов в нужной ситуации
	владеть способностьюиспользоватьосновыправовыхзнаний вразличныхсферахдеятельности
ОПК-5	знать о возможных социальных и культурных различиях членов коллектива
	уметь эффективно преодолевать конфликты
	владеть способностьюработатьвколлективе,толерантновоспринимаясоциальные,культурныеииныеразличия
ОПК-6	знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности
	уметь использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;
	владеть

	способностьюиспользоватьнормативныеправовыеактывсвоейпрофессиональнойдеятельности
ПК-1	знать приемы быстрого нахождения качественных материалов по проблемамкомпьютернойбезопасности
	уметь осуществлятьподбор,изучениеиобобщениенаучно-технической информации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности
	владеть способностьюосуществлятьподбор,изучениеиобобщениенаучно-технической информации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности,атакженормативныхправовыхактоввсферепрофессиональнойдеятельности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Организационноеиправовоеобеспечениеинформационнойбезопасности»составляет3з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всего часов	Семестры
		10
Аудиторныезанятия (всего)	54	54
В томчисле:		
Лекции	36	36
Практическиезанятия (ПЗ)	18	18
Самостоятельнаяработа	54	54
Видыпромежуточнойаттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Практ зан.	СРС	Всего, час
1	Информационные отношения и правовой режим защиты информации ограниченного доступа	Законодательство Российской Федерации в области защиты конфиденциальной информации. Виды конфиденциальной информации по законодательству Российской Федерации. Отнесение	6	2	8	16

		сведений к конфиденциальной информации.				
2	Правовая защита различных видов конфиденциальной информации	Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия в области аттестации по требованиям безопасности информации и их определения. Системысертификациисредствзащитыинформациипотребованиямбезопасностиинформации	6	2	8	16
3	Защита персональных данных и государственное регулирование деятельности по защите информации	Нормативно-правовое содержание Федерального закона «О персональных данных». Документирование сведений конфиденциального характера. Защита конфиденциальной информации. Ответственность за нарушение режима защиты конфиденциальной информации	6	2	8	16
4	Организационное обеспечение информационной безопасности	Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации «группы риска». Понятие «допуск». Формы допусков, их назначение и классификация. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления, утверждения. Работапообучениюперсонала, допускаемому к конфиденциальнойинформации	6	4	10	20
5	Организация охраны, режима и работы с персоналом	Понятие «охрана». Организация охраны территории, зданий, помещений и персонала. Цели и задачи охраны. Объекты охраны. Виды и способы охраны. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Понятие пропуска. Понятие внутриобъектового режима. Общие требования внутриобъектового режима Требования к помещениям, в которых ведутся работы с конфиденциальной информацией, конфиденциальные переговоры.	6	4	10	20
6	Организация защиты информации в различных направлениях деятельности предприятия (организации)	Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее – система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям	6	4	10	20

		безопасности информации (добровольная, обязательная).				
			Итого	**36**	**18**	**54**	**108**

5.2Переченьлабораторныхработ

Непредусмотреноучебнымпланом

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестациионцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**Критерии оценивания**	**Аттестован**	**Неаттестован**
ОК-4	знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности	устный опрос	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять необходимые положения нормативно-правовых актов в нужной ситуации	решение прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностьюиспользоватьосновыправовыхзнанийвразличныхсферахдеятельности	контрольная работа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-5	знать о возможных социальных и культурных различиях членов коллектива	устный опрос	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь эффективно преодолевать конфликты	решение прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностьюработатьвколлективе,толерантновоспринимаясоциальные,культурныеиныеразличия	контрольная работа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-6	знать основные положения нормативно-правовых актов, направленных на обеспечение	устный опрос	Выполнение работ в срок, предусмотренны	Невыполнение работ в срок, предусмотренный

	информационной безопасности		й в рабочих программах	в рабочих программах
	уметь использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;	решение прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностьюиспользоватьнормативныеправовыеактывсвоейпрофессиональнойдеятельности	контрольная работа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-1	знать приемы быстрого нахождения качественных материалов по проблемамкомпьютернойбезопасности	устный опрос	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлятьподбор,изучениеиобобщениенаучно-техническойинформации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности	решение прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть способностьюосуществлятьподбор,изучениеиобобщениенаучно-техническойинформации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности,атакженормативныхправовыхактоввсферепрофессиональнойдеятельности	контрольная работа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв10семестредляочнойформыобученияподвухбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ОК-4	знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь применять необходимые положения нормативно-правовых актов в нужной ситуации	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть способностьюиспользоватьосновыправовыхзнанийвразличныхсферахдеятельности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ОПК-5	знать о возможных социальных и культурных различиях членов коллектива	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь эффективно преодолевать конфликты	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть	Решение	Продемонстрир	Задачинерешены

	способностьюработатьвколлективе,толерантновоспринимаясоциальные,культурныеиныеразличия	прикладных задач в конкретной предметной области	ова н верный ход решения в большинстве задач	
ОПК-6	знать основные положения нормативно-правовых актов, направленных на обеспечение информационной безопасности	Тест	Выполнениетеста на 70-100%	Выполнениеменее 70%
	уметь использовать основные положения и методы защиты конфиденциальной информации в профессиональной деятельности;	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть способностьюиспользоватьнормативныеправовыеактывсвоейпрофессиональнойдеятельности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-1	знать приемы быстрого нахождения качественных материалов по проблемамкомпьютернойбезопасности	Тест	Выполнениетеста на 70-100%	Выполнениеменее 70%
	уметь осуществлятьподбор,изучениеиобобщениенаучно-техническойинформации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть способностьюосуществлятьподбор,изучениеиобобщениенаучно-техническойинформации,методическихматериаловотечественногоизарубежногоопытапопроблемамкомпьютернойбезопасности,атакженормативныхправовыхактоввсферепрофессиональнойдеятельности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

Вопрос:

Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

Руководитель среднего звена

Высшее руководство

Владелец

Пользователь

Вопрос:

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

Сотрудники

Хакеры

Атакующие

Контрагенты (лица, работающие по договору)

Вопрос:

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

Улучшить контроль за безопасностью этой информации

Снизить уровень классификации этой информации

Вопрос:

Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

Необходимый уровень доступности, целостности и конфиденциальности

Оценить уровень риска и отменить контрмеры

Управление доступом, которое должно защищать данные

Вопрос:

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

Владельцы данных

Пользователи

Администраторы

Руководство

Вопрос:

Что такое процедура?

Варианты ответа:

Правила использования программного и аппаратного обеспечения в компании

Пошаговая инструкция по выполнению задачи

Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

Обязательные действия

Вопрос:

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Варианты ответа:

Поддержка высшего руководства

Эффективные защитные меры и методы их внедрения

Актуальные и адекватные политики и процедуры безопасности

Проведение тренингов по безопасности для всех сотрудников

Вопрос:

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Варианты ответа:

Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

Когда риски не могут быть приняты во внимание по политическим соображениям

Когда необходимые защитные меры слишком сложны

Когда стоимость контрмер превышает ценность актива и потенциальные потери

Вопрос:

Что такое политики безопасности?

Варианты ответа:

Пошаговые инструкции по выполнению задач безопасности

Общие руководящие требования по достижению определенного уровня безопасности

Широкие, высокоуровневые заявления руководства

Детализированные документы по обработке инцидентов безопасности

Вопрос:

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

Варианты ответа:

Анализ рисков

Анализ затрат / выгоды

Результаты ALE

Выявление уязвимостей и угроз, являющихся причиной риска

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

Какие меры необходимо применить для устранения угрозы несанкционированного доступа в помещения организации?

-организацию надежного пропускного режима;

-определение порядка учета, выдачи, использования и хранения съемных

магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т. п.;

-явный и скрытый контроль за работой персонала системы;

Какие меры нужны для обеспечения целостности персональных данных в организации?

-учет машинных носителей персональных данных;

-обнаружением фактов несанкционированного доступа к персональным данным и принятием мер

-восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

(минимум10вопросовдлятестированиясвариантамиответов)

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. Информационное общество: понятие, структура, признаки.
2. Понятие информационной сферы общества.
3. Информация и ее виды.
4. Сущность конституционного права на информацию и его гарантии.
5. Правовые режимы информации.
6. Понятие и виды информационных правоотношений.
7. Субъекты, объекты, содержание информационных правоотношений.
8. Законодательство Российской Федерации в области информационной безопасности.
9. Понятие информационной безопасности.
10. Особенности обеспечения информационной безопасности в различных

сферах общественной жизни.

11. Понятие правонарушений в информационной сфере.
12. Ответственность за правонарушения в информационной сфере.
13. Понятие государственной тайны. Сведения, составляющие государственную тайну.
14. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание.
15. Порядок распоряжения сведениями, составляющими государственную

тайну.

16. Защита сведений, составляющих государственную тайну.
17. Юридическая ответственность за нарушение режима государственной

тайны.

18. Понятие коммерческой тайны. Информация, составляющая

коммерческую
тайну (секреты производства).

19. Отнесение информации к информации, составляющей коммерческую тайну
(секрет производства).

20. Содержание и реализация исключительного права на секрет производства.

21. Ответственность за нарушение исключительного права на секрет производства.

22. Понятие и виды персональных данных.

23. Принципы обработки персональных данных.

24. Порядок и условия обработки персональных данных.

25. Права и обязанности субъекта персональных данных.

26. Права и обязанности оператора при обработке персональных данных.

27. Контроль и надзор за обработкой персональных данных.

28. Ответственность за нарушение положений законодательства о персональных данных.

29. Понятие электронного документа и электронного документооборота.

30. Правовое регулирование и юридические риски электронного документооборота.

31. Общая характеристика законодательства в сфере электронного документооборота.

32. Понятие и виды электронной подписи.

33. Правовой статус удостоверяющего центра.

34. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.

35. Правовое регулирование отношений в сфере библиотечного дела.

36. Правовое регулирование отношений в области формирования обязательного экземпляра документов.

37. Правовое регулирование общественных отношений в сфере формирования,
хранения, учета и использования архивов и архивных фондов.

38. Понятие связи, ее структура, принципы функционирования.

39. Общая характеристика отношений в сфере связи и массовых коммуникаций.

40. Государственной регулирование деятельности в области связи.

41. Право и Интернет как социальные явления.

42. Особенности регулирования интернет-отношений.

43. Правовое регулирование деятельности в киберпространстве.

44. Киберпреступления: понятие, основные черты, формы проявления.

45. Понятие и распространение массовой информации.

46. Понятие и правовой статус средства массовой информации.

47. Правовые формы организации деятельности средств массовой

информации.

48. Общие принципы работы средств массовой информации.

49. Правовые формы организации деятельности средств массовой информации.

50. Специальная редакционная ответственность средств массовой информации.

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Непредусмотреноучебнымпланом

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Информационные отношения и правовой режим защиты информации ограниченного доступа	ОК-4, ОПК-5, ОПК -6, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Правовая защита различных видов конфиденциальной информации	ОК-4, ОПК-5, ОПК -6, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Защита персональных данных и государственное регулирование деятельности по защите информации	ОК-4, ОПК-5, ОПК -6, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Организационное обеспечение информационной безопасности	ОК-4, ОПК-5, ОПК -6, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому

			проекту….
5	Организация охраны, режима и работы с персоналом	ОК-4, ОПК-5, ОПК -6, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Организация защиты информации в различных направлениях деятельности предприятия (организации)	ОК-4, ОПК-5, ОПК -6, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценки припроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

8.1.1. Основы организационного обеспечения информационной безопасности объектов информации : учеб. пособие / С. Н. Семкин [и др.]. - М. : Гелиос АРВ, 2005. - 192 с. - ISBN 5-85438-042-0 : 87-00

8.1.2. Математические модели организационно- правовых аспектов противодействия информационным операциям и атаками на региональном уровне [Электронный ресурс] : учеб. пособие / В. П. Дуров [и др.]. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

8.1.3. Гончаров, И.В. Организационное обеспечение информационной безопасности [Электронный ресурс] : учеб. пособие / И. В. Гончаров. - Электрон. дан. (1 файл : 671Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

8.1.4. Язов, Ю.К. Анализ и управление рисками нарушения безопасности персональных даннывх при обработке в информационных системах [Электронный ресурс] / Ю. К. Язов ; под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (3307234 байт) . - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.

8.1.5. Замедлина, Е.А. Организационная культура : Учеб. пособие / Е. А. Замедлина. - М. : ИД РИОР, 2014. - 126 с. - (Высшее профессиональное образование. Бакалавриат). - ISBN 978-5-369-00360-2 : 120-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлениии образовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

8.2.1. Электронная информационная образовательная среда ВГТУ, код доступа: http://eios.vorstu.ru/

8.2.2. Университетская библиотека онлайн, код доступа: http://biblioclub.ru/;

8.2.3. Научная электронная библиотека eLIBRARY.RU, код доступа: http://elibrary.ru/.

8.2.4. Портал федеральных государственных образовательных стандартов высшего образо-вания, код доступа http://fgosvo.ru;

6.2.5. Открытое образование, код доступа: https://openedu.ru/.

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Лекционная аудитория, оснащённая оборудованием для лекционных демонстраций и проектором.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Организационноеиправовоеобеспечениеинформационнойбезопасности»читаютсялекции,проводятсяпрактическиезанятия.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяна иболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражения вучебнойлитературе.

Практическиезанятиянаправленынаприобретениепрактическихнавыков расчетанеобходимых пер по защите информации.Занятияпроводятсяпутемрешенияконкретныхзадачваудитории

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием

	толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.