Аннотация к рабочей программе дисциплины «Порядок проведения аттестации объектов информатизации»

Цель преподавания дисциплины

Дисциплина "Порядок проведения аттестации объектов информатизации" изучается с целью изучения порядка проведения процедур сертификации и лицензирования в области обеспечения информационной безопасности телекоммуникационных систем.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны изучить:

1) Изучение нормативно-правовой базы процедур сертификации и лицензирования;

2) Формирование у обучаемых понимания требований регуляторов к деятельности в области информационной безопасности;

3)Ознакомление обучаемых с порядком проведения сертификационных и лицензирующих процедур.

4) Компетенции, формируемые в результате освоения дисциплины

Компетенции, формируемые в результате освоения дисциплины

Способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9),

Способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-10).

Разделы дисциплины

Основные понятия в области технической защиты информации. Концептуальные основы защиты информации. Система документов по технической защите информации. Органы по технической защите информации в РФ. Органы по технической защите информации в РФ. Объект информатизации. Классификация объектов защиты. Общий порядок сертификации средств защиты информации. Порядок сертификации во ФСТЭК России. Аттестация объекта информатизации по требованиям безопасности информации. Требования и рекомендации по защите информации, обрабатываемой средствами.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
информатики
(наименование ф-та полностью)

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«*01*» *февраля* 20*17* г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Порядок проведения аттестации объектов информатизации

направление подготовки (специальность) *10.05.02*
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

Защита информации в системах связи и управления
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 20*17*

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» и на основании учебного плана подготовки специалистов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» на заседании кафедры информационной безопасности.
«28» 08 2017. Протокол № 1

И. о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Карасовский В.В.

Согласовано:
Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры. ИБ, протокол №12 от 29.06.18г.

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №___ «___» _____ 20__ г. на заседании кафедры. Информационной безопасности 27.06.2019 №11

Зав. кафедрой к.т.н доцент Таныгин М.О

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_1_ от «_31_» _08_ 20_20_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_28_» _06_ 20_21_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_30_» _06_ 20_22_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина "Порядок проведения аттестации объектов информатизации" изучается с целью изучения порядка проведения процедур сертификации и лицензирования в области обеспечения информационной безопасности телекоммуникационных систем.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны изучить:

- Изучение нормативно-правовой базы процедур сертификации и лицензирования;
- формирование у обучаемых понимания требований регуляторов к деятельности в области информационной безопасности;
- ознакомление обучаемых с порядком проведения сертификационных и лицензирующих процедур.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

– нормативно-правовую базу в области информационной безопасности;

– требования, предъявляемые к информационным системам и объектам информатизации;

– основные тенденции и закономерности развития средств и методов защиты информации в ИС;

– основы организации и функционирования ЗИС, их стандарты;

– порядок проведения лицензирующих процедур.

уметь:

– анализировать требования нормативно-правовых актов, предъявляемые к информационным системам;

– определять класс защищённости информационных систем;

– применять стандартные решения для защиты информации в ИС;

владеть:

– навыками определения порядка приведения в соответствие информационных систем требованиям регуляторов;

– работы с нормативно-правовой документацией ФСТЭК и ФСБ.

У обучающихся формируются следующие компетенции:

– способность участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9),

– способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-10).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам вариативной части, дисциплинам по выбору (Б1.В.ДВ.6.2). Изучается на 5 курсе в 9 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 2 зачётные единицы, 72 часа

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36,1
лекции	18
лабораторные занятия	18
практические занятия	0
экзамен	не предусмотрен
зачет	0,1
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	0
Самостоятельная работа обучающихся (всего)	36
Контроль/экз (подготовка к экзамену)	0

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Основные понятия в области технической защиты информации	Цель построения системы защиты информации. Основные понятия проблематики построения СЗИ. Виды защиты информации
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	Концептуальные основы защиты информации. Доктрина информационной безопасности РФ. Законодательные и иные правовые акты в области технической защиты информации.
3.	Органы по технической защите информации в РФ.	Государственные органы в области защиты информации. Фунции ФСТЭК России. Правовые основы деятельности ФСТЭК
4.	Лицензирование деятельности в области ТЗИ.	Общий порядок лицензирования. Порядок получения лицензии следующий. Документы при лицензировании. Прекращение лицензии. Виды деятельности на осуществление которых требуется получение лицензии. Контроль за соблюдением лицензионных требований и условий.
5.	Объект информатизации. Классификация объектов защиты.	Классификация информации. Классификация АС. Классификация СВТ. Политики разграничения доступа
6.	Общий порядок сертификации средств защиты информации.	Понятие сертификации. Органы сертификации, их функции. Порядок проведения процедуры сертификации. Схемы проведения сертификации средств защиты информации.
7.	Порядок сертификации во ФСТЭК России	Подача заявки на сертификацию во ФСТЭК России. Решение на проведение сертификационных испытаний. Заключение договора с испытательной лабораторией. Подготовка исходных данных. Сертификационные испытания.
8.	Аттестация объекта информатизации по требованиям безопасности информации	Необходимость аттестации. Органы, проводящие аттестацию. Ответственность при проведении аттестации. Документальное сопровождение процедуры аттестации. Структура аттестата соответствия.
9.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	Структура и содержание СТР-К. Обязательные требования. Желательные требования к объектам информатизации. Порядок обеспечения защиты информации в АС. Требования и рекомендации в зависимости от типа АС. Основные рекомендации по защите информации, составляющей коммерческую тайну.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ Пп /п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Основные понятия в области технической защиты информации	2			У-1	С	ПК-9, ПК-10
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	2	1		У-1-3 МУ-1	С	ПК-9, ПК-10
3.	Органы по технической защите информации в РФ.	2			У-4,5 МУ-3	С	ПК-9, ПК-10
4.	Лицензирование деятельности в области ТЗИ.	2			У-1,6,7	С	ПК-9, ПК-10
5.	Объект информатизации. Классификация объектов защиты.	2			У-1,2	С	ПК-9, ПК-10
6.	Общий порядок сертификации средств защиты информации.	2	2		У-4,5 МУ-3	С	ПК-9, ПК-10
7.	Порядок сертификации во ФСТЭК России	2			У-4,5	С	ПК-9, ПК-10
8.	Аттестация объекта информатизации по требованиям безопасности информации	2	3		У-4,5 МУ-3	С	ПК-9, ПК-10
9.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	2			У-4,5	С	ПК-9, ПК-10

С – собеседование

4.2. Лабораторные работы и практические занятия

4.2.1. Практические занятия

Таблица 4.3 – Практические занятия

№	Наименование лабораторного занятия	Объем, час.
1	2	3
1.	Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы	6
3.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности : методические указания по выполнению практической работы	6
2.	Определение класса государственной информационной системы: методические указания по выполнению практической работы	6
Итого**:**		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Основные понятия в области технической защиты информации	2 неделя	4
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	4 неделя	4
3.	Органы по технической защите информации в РФ.	6 неделя	4
4.	Лицензирование деятельности в области ТЗИ.	8 неделя	4
5.	Объект информатизации. Классификация объектов защиты.	10 неделя	4
6.	Общий порядок сертификации средств защиты информации.	12 неделя	4
7.	Порядок сертификации во ФСТЭК России	14 неделя	4
8.	Аттестация объекта информатизации по требованиям безопасности информации	16 неделя	4
9.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	18 неделя	4
Итого			36

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. № 301 по направлению подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем» реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, 19,6 процента от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической №1 «Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы»	Выполнение студентом интерактивных заданий по изучению системного подхода при создании структуры ГОСТ и ИСО.	4
2.	Выполнение практической работы №2 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности »	Выполнение студентом интерактивных заданий по анализу сертифицированных продуктов в заданной области информационной безопасности	4
	Итого		8

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4

способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям защиты информации (ПК-9)			Измерения в телекоммуникационных системах Планирование и управление информационной безопасностью Основы мониторинга безопасности инфокоммуникационных систем и сетей Система сертификации и аттестации телекоммуникационных систем Порядок проведения аттестации объектов информатизации Технологическая практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
Способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (ПК-10)			Система сертификации и аттестации телекоммуникационных систем Порядок проведения аттестации объектов информатизации Технологическая практика Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкал оценивания

Наименование компетенции	Критерии освоения		
	Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-9способность участвовать в проведении аттестации телекоммуникационных систем по	**Знать**: общие принципы лицензирования и сертификации в области ИБ **Уметь**: определять перечень действий для	**Знать**: порядок проведения лицензирования и аттестации **Уметь**: определять несоответсвия	**Знать**: требования к лицензиатам и сертифицированным объектам **Уметь**: сопоставлять текущую структуру

требованиям защиты информации (завершающий)	проведения анализа ИБ **Владеть навыками**: Участия в анализе требований регуляторов в области ИБ;	между текущим состоянием объекта информатизации и требованиями регуляторов в области ИБ; **Владеть навыками**: Анализа информационных систем на предмет соответствия нормативно-правовым документам	предприятия требованиям регуляторов в области ИБ; **Владеть навыками**: Формирования программ лицензирования и сертификации;
ПК-10 способность оценивать выполнение требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных телекоммуникационных систем, выполнять подготовку соответствующих заключений (завершающий);	**Знать:** порядок перечень требований регуляторов к защищенным телекоммуникационным системам **Уметь:** работать с нормативными документами регуляторов в области информационной безопасности **Владеть навыками:** анализа нормативных требований регуляторов	**Знать:** требования регуляторов к защищенным телекоммуникационным системам. **Уметь:** оценивать технологический процесс обеспечения информационной безопасности ТКС. **Владеть навыками:** составления проектов организации защиты ТКС;	**Знать:** полный перечень и сферу применения требований регуляторов к защищенным телекоммуникационным системам. **Уметь:** оценивать по разнообразным критериям и нормам процесс обеспечения информационной безопасности ТКС **Владеть навыками:** организации защиты ТКС

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся: а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контроли-руемой	Технология формирова-ния	Оценочные средства		Описание шкал оценивания
				наимено вание	№№ заданий	
1	2	3	4	5	6	7
1.	Основные понятия в области технической защиты информации	ПК-9, ПК-10	Лекция, СРС,	Собеседов ание	1-7	Согласно табл.7.2
2.	Концептуальные основы защиты информации. Система документов по технической защите информации.	ПК-9, ПК-10	Лекция, СРС, практическое занятие	Собеседов ание	1-7	Согласно табл.7.2
				контроль ные вопросы к ПР№1		
3.	Органы по технической защите информации в РФ.	ПК-9, ПК-10	Лекция, СРС	собеседо вание	1-6	Согласно табл.7.2
4.	Лицензирование деятельности в области ТЗИ.	ПК-9, ПК-10	Лекция, СРС	собеседо вание	1-10	Согласно табл.7.2
5.	Объект информатизации. Классификация объектов защиты.	ПК-9, ПК-10	Лекция, СРС	собеседо вание	1-9	Согласно табл.7.2
6.	Общий порядок сертификации средств защиты информации.	ПК-9, ПК-10	Лекция, СРС, практическое занятие	Собеседов ание	1-8	Согласно табл.7.2
				контроль ные вопросы к ПР№2		
7.	Порядок сертификации во ФСТЭК России	ПК-9, ПК-10	Лекция, СРС,	Собеседов ание,	1-7	Согласно табл.7.2
8.	Аттестация объекта информатизации по	ПК-9, ПК-10	Лекция, СРС, практическое	Собеседов ание	1-10	Согласно табл.7.2

	требованиям безопасности информации		занятие	контрольные вопросы к ПР№3		
9.	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники	ПК-9, ПК-10	Лекция, СРС,	Собеседование,	1-10	Согласно табл.7.2

Примеры типовых контрольных заданий для текущего контроля

Вопросы для собеседования по темам курса

Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

1. Основные аспекты документа "Специальные требования и рекомендации по технической защите конфиденциальной информации".
2. Рекомендованные основные меры по защите информации.
3. Стадии создания средств защиты информации в автоматизированных системах.
4. Порядок обеспечения защиты информации в АС.
5. Защита информации в локальных вычислительных сетях и при межсетевом взаимодействии.
6. Защита информации при работе с системами управления базами данных.
7. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
8. Рекомендации при создании абонентского пункта.
9. Основные требования при разработке и эксплуатации АС предполагающих использование информации, составляющей служебную тайну, а также персональных данных.
10. Организационно-технические мероприятия, рекомендуемые к выполнению при разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Промежуточная аттестация проводится либо в форме устного зачёта, либо в форме компьютерного тестирования

7.4Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

Положение П 02.016–2018 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1 «Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы»	8	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение лабораторной работы №2 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	8	Выполнил, но «не защитил»	10	Выполнил и «защитил»
Выполнение лабораторной работы №3 «Определение класса государственной информационной системы: методические указания по выполнению практической работы»	8	Выполнил, но «не защитил»	10	Выполнил и «защитил»
СРС	0		18	
ИТОГО	24		48	
Посещаемость	0		16	
Зачёт	0		36	
ИТОГО	24		100	

При промежуточной аттестации в форме компьютерного теста студенту предлагается 20 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 100) переводят в баллы на зачёт (максимум 36) путём умножения на 0.36 и округления до целого значения. Список вопросов для проведения зачёта в тестовой форме размещён в Электронной образовательной системы

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1 Аверченков, В. И. Служба защиты информации: организация и управление [Электронный ресурс] : учебное пособие для вузов / В.

И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - М. : Флинта, 2016. - 186 с. - Режим доступа:http://biblioclub.ru/index.php?page=book&id=93356.

2 Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245

3 Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

8.2 Дополнительная литература

1 Аверченков, В. И. Защита персональных данных в организации [Электронный ресурс]: монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. — 3-е изд., стереотипное — М. : Флинта, 2016. - 124 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93260

2 Аверченков, В. И. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков [и др.]. -4-е изд., стереотипное — М. : Флинта, 2016. - 224 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93351

3 Системы защиты информации в ведущих зарубежных странах вузов [Электронный ресурс] : учебное пособие для / В. И. Аверченков [и др.]. - 4-е изд., стер. - М. : Флинта, 2016. - 224 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93351

4 Положение по аттестации объектов информатизации по требованиям безопасности информации (Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.)

5 Фороузан, Б. А. Математика криптографии и теория шифрования [Электронный ресурс] / Б. А. Фороузан. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=428998

8.3 Перечень методических указаний

1) Анализ заданного нормативно-правового акта: методические указания по выполнению практической работы методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц

2) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

3) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности : методические указания по выполнению практической работы [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. - Курск : ЮЗГУ, 2017. - 12 с. : ил., табл. - Библиогр.: с. 12. - Б. ц.

9 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3) Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
4) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
7) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
8) База данных "Патенты России"

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Порядок проведения аттестации объектов информатизации» являются лекции, лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение

опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Порядок проведения аттестации объектов информатизации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Порядок проведения аттестации объектов информатизации» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Порядок проведения аттестации объектов информатизации» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)