ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол№ 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института
_____ / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Аттестация объектов информатизации по требованиям безопасности

Часть, формируемая участниками образовательных отношений (Б1.В.ДВ.02.02)

программа магистратуры

Направление подготовки
10.04.01 Информационная безопасность

Направленность подготовки (программа магистратуры)
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчики: К.филос.н., доц. каф. Управления информационной безопасностью; ст. преподаватель каф. УИБ	_____ / Миронова Н.Г. _____ / Салов И.В.

Для приема: 2021 г.

Уфа 2021 г.

Составители: к.филос.н. Миронова Наталия Геннадьевна, Салов Игорь Владимирович

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от «_24_» _февраля_____ 2021 г. № _8_

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
	ПК-1. Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.	ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знать методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
		ПК-1.2 Знает методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Знать методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.
		ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Уметь применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
		ПК-1.4 Умеет применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Уметь применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.
		ПК-1.5. Владеет навыками проведения предпроектного	Владеть навыками проведения предпроектного

		обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
		ПК-1.6 Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Владеть навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.
	ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах.	ПК-2.3. Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Знать технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.
		ПК-2.6. Умеет применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Уметь применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.
		ПК-2.10. Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Владеть навыками применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Аттестация объектов информатизации по требованиям безопасности» относится к части, формируемой участниками образовательных отношений, дисциплинам по выбору.

Дисциплина изучается на 2 курсе магистратуры в 3 семестре.

Целью учебной дисциплины «Аттестация объектов информатизации по требованиям безопасности» является формирование навыков проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений, разработки проектных решений по защите информации в автоматизированных системах.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

ПК-1. Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знать методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Не знает или показывает очень слабые знания.	Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
ПК-1.2 Знает методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Знать методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Не умеет.	Знает методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.
ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей	Уметь применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей	Не владеет.	Умеет применять основные методы проведения предпроектного обследования служебной деятельности и информационных потребностей

автоматизируемых подразделений.	автоматизируемых подразделений.		автоматизируемых подразделений.
ПК-1.4 Умеет применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Уметь применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Не умеет.	Умеет применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.
ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Владеть навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Не владеет.	Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.
ПК-1.6 Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Владеть навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Не владеет.	Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.

ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК-2.3. Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Знать технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Не знает или показывает очень слабые знания.	Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.
ПК-2.6. Умеет применять технологии аттестации объектов информатизации по	Уметь применять технологии аттестации объектов информатизации по	Не умеет.	Умеет применять технологии аттестации объектов информатизации по

требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.		требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.
ПК-2.10. Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Владеть навыками применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Не владеет.	Имеет навыки применения технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

ПК-1. Способен проводить предпроектное обследование служебной деятельности и информационных потребностей автоматизируемых подразделений.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-1.1 Знает методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Знать методы проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	тестирование, практическое задание; лабораторная работа
ПК-1.2 Знает методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Знать методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	тестирование, практическое задание; лабораторная работа
ПК-1.3 Умеет применять основные методы проведения предпроектного обследования служебной	Уметь применять основные методы проведения предпроектного обследования	тестирование, практическое задание; лабораторная работа

деятельности и информационных потребностей автоматизируемых подразделений.	служебной деятельности и информационных потребностей автоматизируемых подразделений.	
ПК-1.4 Умеет применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Уметь применять основные методы проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	тестирование, практическое задание; лабораторная работа
ПК-1.5. Владеет навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	Владеть навыками проведения предпроектного обследования служебной деятельности и информационных потребностей автоматизируемых подразделений.	тестирование, практическое задание; лабораторная работа
ПК-1.6 Владеет навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	Владеть навыками проведения предпроектного обследования информационных потребностей автоматизируемых подразделений.	тестирование, практическое задание; лабораторная работа

ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-2.3. Знает технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Знать технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	тестирование, практическое задание; лабораторная работа
ПК-2.6. Умеет применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	Уметь применять технологии аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	тестирование, практическое задание; лабораторная работа
ПК-2.10. Имеет навыки применения технологии	Владеть навыками применения технологии аттестации объектов	тестирование, практическое задание; лабораторная

аттестации объектов информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	информатизации по требованиям безопасности для разработки проектных решений по защите информации в автоматизированных системах.	работа

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины. Для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для зачета:

- зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Аттестация объектов информатизации по требованиям безопасности»

Специальность: 10.04.01 Информационная безопасность

курс 2, семестр 3

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации.				
Текущий контроль			**0**	**40**
Лабораторная работа	5	4	0	20
Практическая работа	5	4	0	20
Рубежный контроль				**10**
Тест	10	1	0	10
Всего		**4**	**0**	**50**
Модуль 2. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации.				
Текущий контроль				**40**
Лабораторная работа	5	4	0	20
Практическая работа	5	4	0	20
Рубежный контроль				**10**
Тест	10	1	0	10
Всего		**5**	**0**	**50**
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Зачет	60	1	60	100

Зачетное собеседование

Вопросы зачета:

1. Определение понятия и краткая характеристика аттестация объектов информатизации.
2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.
3. Специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности.

4. Специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственного регулирования.
5. Функции службы безопасности предприятия для решения задачи обеспечения информационной безопасности, их роль в подготовке, проведении аттестации.
6. Задачи, функции, права и обязанности органов по аттестации. Деятельность аттестационных комиссий.
7. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.
8. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная).
9. Виды аттестации и нормативные документы, регламентирующие и регулирующие порядок и состав аттестационных мероприятия для каждого вида аттестации.
10. Участники аттестации и их полномочия (компетенции).
11. Основной перечень работ по аттестации объектов информатизации (кроме аттестации объектов КИИ).
12. Критически важные объекты инфраструктуры Российской Федерации: классификация и категории. Особенности аттестации объектов КИИ.
13. Основные мероприятия по проведению аттестации объектов информатизации критически важных объектов на соответствие требованиям безопасности информации.
14. Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации критически важных объектов.
15. Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации критически важных объектов.
16. Экспертно-документальный метод проверки, применяемый при проведении аттестационных испытаний.
17. Инструментальный метод проверки, применяемый при проведении аттестационных испытаний с использованием контрольно-измерительной аппаратуры.
18. Этапы аттестации объектов информатизации критически важных объектов.
19. Подача заявки на рассмотрение и проведение аттестации. Анализ исходных данных по аттестуемому объекту информатизации.
20. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.
21. Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации
22. Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний.
23. Проведение аттестационных испытаний объекта информатизации. Заключение договоров на аттестацию.
24. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.
25. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций.
26. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации критически важных объектов.
27. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации критически важных объектов.
28. Заключение аттестационной проверки: структура, содержание. Протокол аттестационного испытания: структура, содержание.
29. Аттестат соответствия объектов информатизации критически важных объектов требованиям безопасности.
30. Типовые организационные структуры государственной системы защиты информации.
31. Функции контроля и надзора органа государственной власти в области обеспечения безопасности и защиты информации.

32. Специальные мероприятия и действия сотрудников службы безопасности по организации объектовых режимов. Основное назначение корпоративной нормативной базы службы безопасности. Структура корпоративной нормативной базы службы безопасности.
33. Перечень контрольных мероприятий и действий по оценке уровня безопасности объекта.
34. Определение понятия «режимный объект» и видов обеспечения его безопасности. Особенности организации охраны режимного объекта. Суть и содержание нормативной основы организации охранных мероприятий.
35. Назначение и содержание «Концепции обеспечения информационной безопасности организации».
36. Особенности документального оформления политики безопасности, и чем они объясняются. Типовое содержание политики безопасности, оформленной в виде единого документа.
37. Разделы типового формата положений о структурных подразделениях службы безопасности.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:
зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов).

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Тестовые задания

В течение курса проводится 2 теста (до 10 баллов каждый).

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме. Необходимо выбрать один или несколько вариантов ответов из предложенных вариантов.

Примерные вопросы тестов приводится ниже.

Тест 1 по результатам модуля 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации

1. Анализ защищенности - это …

a) выбор обоснованного набора контрмер, позволяющих снизить уровень рисков до приемлемой величины

b) независимая экспертиза отдельных областей функционирования предприятия

c) процедура учета действий, выполняемых пользователем на протяжении сеанса доступа

d) поиск уязвимых мест информационной системы

2. Воздействие на систему с целью создания условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

a) DoS-атака

b) несанкционированный доступ
c) незаконное использование привилегий
d) программная закладка

3. Программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей.
a) агент безопасности
b) политика безопасности
c) средство делегирования административных полномочий
d) сканер безопасности

И т.д. - см. подробнее в ФОС дисциплины.

Тест 2 по результатам модуля 2. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации

1. Защита ресурсов сети от несанкционированного использования - это
a) охрана оборудования сети
b) защита ядра безопасности
c) контроль доступа
d) защита периметра безопасности

2. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика
a) межсетевой экран
b) средство антивирусной защиты
c) DLP-система
d) сканер безопасности

3. Средство, решающее задачи консолидации и хранения журналов событий от различных источников, а также имеющее инструменты для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам – это …
a) DLP-система
b) система обнаружения вторжений
c) SIEM-система
d) сканер безопасности

И т.д. - см. подробнее в ФОС дисциплины.

Критерии оценки тестовых заданий:
1 тест состоит из 10 тестовых заданий.

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста	Неправильный ответ / Правильный ответ	0/1

Планы практических и лабораторных занятий

Тематика и содержание практических работ

Цель проведения практических работ – практическое освоение материала дисциплины.

Модуль 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации

Практическая работа № 1-2. Нормативно–правовые основы аттестации ОИ (4 часа)

Цель: Освоить Нормативно–правовые основы аттестации ОИ.

Задание: На практике ознакомиться с нормативно–правовыми документами по аттестации ОИ.

Порядок выполнения:

1. Изучить Постановлении Правительства РФ от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
2. Ознакомиться с приказом ФСТЭК России от 29 апреля 2021 г. № 77 «Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».
3. Изучить «Информационное сообщение об утверждении порядка аттестации объектов информатизации и особенностях его реализации» ФСТЭК от 29 апреля 2021 г. N 240/24/2087
4. Изучить «Информационное сообщение об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» ФСТЭК от 2 сентября 2021 г. N 240/24/4303Изучить «Информационное сообщение о порядке представления документов по аттестации объектов информатизации, обрабатывающих информацию ограниченного доступа, не составляющую государственную тайну» ФСТЭК от 11 апреля 2022 г. N 240/24/1950
5. Нормативные документы по видам аттестуемого объекта информатизации (защищаемое помещение или автоматизированная система).
6. Изучить требования нормативных документов для аттестации автоматизированных информационных систем по видам аттестации:
   а. Автоматизированные системы обработки конфиденциальной информации (далее — АС ОКИ, требования предъявляются: СТР-К и РД АС);
   б. Информационные системы персональных данных (далее — ИСПДн, требования предъявляются: приказ ФСТЭК России № 21);
   в. Государственные информационные системы (далее — ГИС, требования предъявляются: приказ ФСТЭК России № 17);
   г. Автоматизированные системы управления технологическими процессами (далее – АСУ ТП, требования предъявляются: приказ ФСТЭК России № 31);
   д. Информационные системы общего пользования (требования предъявляются: приказ ФСТЭК России № 489);
   е. Объекты критической информационной инфраструктуры (требования предъявляются: приказами ФСТЭК России № 235 и № 239);
   ж. Автоматизированные банковские системы (далее – АБС, требования предъявляются: положение ЦБ РФ № 382-П и СТО БР ИББС).

Дать ответы на вопросы по теме занятия:

а. по какому принципу согласуются прежние и новые законодательные нормативные документы по аттестации объектов информатизации (с учетом иерархии органов-регуляторов, времени издания ПП или приказа)?
б. Для каких объектов аттестация является обязательной (необходимой), с **учетом** Федеральным законом № 152-ФЗ «О персональных данных», ГОСТ Р 51583 «Защита информации», для подтверждения требований стандартов и нормативно-методических документов по информационной безопасности**?**
в. Является ли аттестация обязательной для коммерческих организаций, с учетом нормативно-законодательных положений?
г. Каков срок действия аттестата?
д. Чем определяется срок жизненного цикла корпоративной нормативной базы по информационной безопасности?
е. В чем отличие нормативно-методических документов политики безопасности от нормативных документов процедурного уровня?
ж. Особенности документального оформления политики безопасности, и чем они объясняются.

Защита практической работы.

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Практическая работа № 3. Категорирование информации, обрабатываемой на ОИ (2 часа)

Цель: Освоить принципы определения категории активов ОИ.
Задание: На практике ознакомиться с системой классификации ресурсов.
Порядок выполнения:

1) Ознакомиться с разделом 7 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности и ГОСТ Р 58545-2019 Менеджмент знаний. Руководящие указания по сбору, классификации, маркировке и обработке информации.

Дать ответы на **вопросы:**

2) Назовите типы активов и приведите примеры названных типов.
3) Указать типичные проблемы, возникающие при обработке указанных журналов.
4) Перечислить типовые пути решения возникающих проблем.
5) Ответить на контрольные вопросы:
    a) Дайте определение терминов «ICMH-система», «информационные активы», «маркировка», «материальные носители информации», «жизненный цикл информации».
    b) Кто определяет ценность актива?
    c) В чем заключается процесс инвентаризации активов.
    d) Что входит в информационные активы организации?
    e) Для чего производится опись активов?

Защита практической работы. Проводится в форме устного опроса после

выполнения работы.

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Практическая работа № 4. Система аттестации объектов информатизации в РФ (2 часа)

Цель: изучить виды аттестации и систему аттестации объектов информатизации в РФ.
Задание: теоретически ознакомиться с системой аттестации.
Порядок выполнения: изучить следующие вопросы:

1. Система аттестации объектов информатизации в РФ: участники, органы аттестации, их полномочия, задачи, функции, обязанности. Деятельность аттестационных комиссий
2. Виды аттестации ОИ, порядок аттестации объектов информатизации.
3. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации
4. Функции служба безопасности предприятия для решения задачи обеспечения информационной безопасности.
5. Структура полномасштабной системы обеспечения безопасности и защиты информации

Дать ответы на вопросы по теме занятия.

а. Кто является участниками аттестации и их полномочия (компетенции).?
б. Критически важные объекты инфраструктуры Российской Федерации: классификация и категории.
в. Типовые организационные структуры государственной системы защиты информации.
г. Функции контроля и надзора органа государственной власти в области обеспечения безопасности и защиты информации.
д. Специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности.

Защита практической работы. Проводится в форме устного опроса после выполнения работы.

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Практическая работа № 5-6. **Этапы аттестации объектов информатизации** (4 часа)

Цель: Этапы аттестации ОИ.
Задание: исследовать темы/вопросы, указанные ниже.
Порядок выполнения: изучить следующие вопросы (3 часа):

I. Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации критически важных объектов, в т.ч.
- Этапы аттестации объектов информатизации критически важных объектов.

- Подача заявки на рассмотрение и проведение аттестации. Анализ исходных данных по аттестуемому объекту информатизации.

II. Изучить, кратко описать содержание этапов подготовки (защиты) аттестуемого объекта, необходимую для его аттестации. (в соответствии с нормативными документами ФСТЭК России):

1. Обследование:
    - отчет об обследовании,
    - модель угроз и нарушителя безопасности информации,
    - акт классификации,
    - техническое задание на создание системы защиты.
2. Проектирование системы защиты:
    - технический проект на систему защиты информации,
    - эксплуатационная документация на систему защиты информации.
3. Внедрение системы защиты:
    - установка и настройка средств защиты информации,
    - разработка организационно-распорядительной документации по защите информации.

III. Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации критически важных объектов.

IV. Состав и порядок разработки и согласования «Технического задания на создание системы и (или) модель угроз безопасности информации» с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации»)

Опрос: дать устные ответы на вопросы по теме занятия.

а. Основной перечень работ по аттестации объектов информатизации.
б. Основные мероприятия по проведению аттестации объектов информатизации критически важных объектов на соответствие требованиям безопасности информации.
в. Основные требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации критически важных объектов.
г. Основные требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации критически важных объектов.
д. Подача заявки на аттестацию (какие документы, кому, в какой срок, что предшествует подаче заявления?).
и проч.

Защита практической работы (0,5 часа). Проводится в форме устного опроса после выполнения работы.

Тестирование (тест 1) (0,5 часа)

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в

конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Модуль 2. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации

Практическая работа № 7. Проведение аттестационных испытаний объектов информатизации (2 часа)

Цель: Освоить аттестационных испытаний ОИ.
Содержание практического занятия:

1. Специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности.
2. Специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственного регулирования.
3. Услуги организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности.
4. Проведение аттестационных испытаний объекта информатизации.
5. Методы аттестационных испытаний:
   a. Документарный метод (экспертно-документальный метод проверки, применяемый при проведении аттестационных испытаний).
   б. Инструментальный метод проверки, применяемый при проведении аттестационных испытаний с использованием контрольно-измерительной аппаратуры.
   в. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.
   г. Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации
   д. Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний.
   е. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

Дать ответы на вопросы по теме занятия.

Защита практической работы. Проводится в форме устного опроса после выполнения работы.

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Практическая работа № 8. Аттестат соответствия (2 часа)

Цель: Знакомство с составом и содержанием документов по аттестации ОИ.
Содержание занятия (темы для освоения):

1. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации критически важных объектов.
2. Заключение аттестационной проверки: структура, содержание.

3. Протокол аттестационного испытания: структура, содержание.
4. Аттестат соответствия объектов информатизации критически важных объектов требованиям безопасности.

Дать ответы на вопросы по теме занятия.

Защита практической работы. Проводится в форме устного опроса после выполнения работы.

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Практическая работа № 9. Протокол аттестационных испытаний. Заключение аттестационной проверки (2 часа)

Цель: Освоить принципы определения категории активов ОИ.
Задание: На практике ознакомиться с системой классификации ресурсов.
Порядок выполнения:

1. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации критически важных объектов.
2. Заключение аттестационной проверки: структура, содержание.
3. Протокол аттестационного испытания: структура, содержание.
4. Аттестат соответствия объектов информатизации критически важных объектов требованиям безопасности.

Защита практической работы. Проводится в форме устного опроса после выполнения работы.

Тестирование итоговое (Тест №2).

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении практической работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Критерии оценки результатов выполнения заданий практических занятий 1-2 разделов (в баллах*)*:

- 4-5 баллов выставляется студенту, если работа практического занятия выполнена без ошибок и без замечаний и получены ответы на все контрольные вопросы (меньше баллов – 4 - выставляется, если есть мелкие замечания к качеству и содержанию ответа);
- 2-3 балла выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (ок. 31-50%); либо работа выполнена, но не получены ответы на все контрольные вопросы.
- 1 балл выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (менее, чем на 30%). При опросе студент не дал ответы на все контрольные вопросы

Лабораторные работы

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Примерная тематика лабораторных работ

Модуль 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации

1) Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (2 часа).
2) Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации (2 часа).
3) Деятельность аттестационных комиссий (2 часа).
4) Государственный надзор за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации (4 часа)

Модуль 2. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации

5) Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (2 часа).
6) Оформление, регистрация и выдача «Аттестата соответствия» (2 часа).
7) Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации (2 часа).
8) Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации (2 часа).

Типовое лабораторное задание

Модуль 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации

Лабораторная работа № 1. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (2 часа)

Цель: Изучить организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации.

Содержание: Выполните задания и ответы на вопросы по результатам работы (защита отчета о проделанной работе):

Порядок выполнения:

1) Ознакомиться с Положением «по аттестации объектов информатизации по требованиям безопасности информации» (утв. председателем Гостехкомиссии 25.11.94).
   Указать письменно в отчете и быть готовыми устно ответить на **вопросы:**
2) Какие органы образуют организационную структуру системы аттестации объектов информатизации?
3) Перечислите функции, осуществляемые Федеральным органом по сертификации и аттестации.
4) Какие действия осуществляют Федеральные органы по сертификации и

аттестации.

5) Какой орган проводит испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с "Положением о сертификации средств защиты информации по требованиям безопасности информации"
6) На основании какого документа испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации.

Защита выполненной работы. - Проводится в форме устного опроса в конце занятия. Вопросы соответствуют вышеперечисленным вопросам.

Методические указания: студент выполняет задания, ответы вносит в отчет о выполнении лабораторной работы. В случае применения системы дистанционного обучения для сдачи отчетности, свой электронный отчет студент прикрепляет для проверки и оценки в СДО в дистанционный курс в нужный пункт. При очной форме сдачи отчетности студент в конце занятия отвечает на устные вопросы по результатам выполнения практического/лабораторного задания.

Критерии оценки результатов выполнения заданий лабораторных занятий 1-2 разделов (в баллах*):*

- 4-5 баллов выставляется студенту, если работа практического занятия выполнена без ошибок и без замечаний и получены ответы на все контрольные вопросы (меньше баллов – 4 - выставляется, если есть мелкие замечания к качеству и содержанию ответа);
- 2-3 балла выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (ок. 31-50%); либо работа выполнена, но не получены ответы на все контрольные вопросы
- 1 балл выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (менее, чем на 30%). При опросе студент не дал ответы на все контрольные вопросы

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Милославская, Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 130 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 2). - Библиогр. в кн. - ISBN 978-5-9912-0272-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253576.

2. Курило А.П. Основы управления информационной безопасностью : учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 244 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр. в кн. - ISBN 978-5-9912-0271-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253575.

Дополнительная литература

3. Милославская, Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 166 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 5). - Библиогр. в кн. - ISBN 978-5-9912-0275-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253579.

4. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 216 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 4). - Библиогр. в кн. - ISBN 978-5-9912-0274-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253578.

5. Веселов, Г.Е. Менеджмент риска информационной безопасности : учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. - Таганрог : Издательство Южного федерального университета, 2016. - 109 с. : схем., табл. - Библиогр.: с.85-86 - ISBN 978-5-9275-2327-5; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493331.

6. Уколов, А.И. Управление корпоративными рисками: инструменты хеджирования : учебник / А.И. Уколов, Т.Н. Гупалова. - 2-е изд., стер. - Москва : Директ-Медиа, 2017. - 554 с. : ил., схем., табл. - Библиогр.: с. 547 - ISBN 978-5-4475-9318-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=273678.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г

6. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
8. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty)

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ - http://www.scli.ru
2. Официальный интернет-портал правовой информации - http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» - http://pravo.fso.gov.ru
4. Модуль «Документы - Президент России» - http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России - http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» - http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - http://asozd.duma.gov.ru/
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) - Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).
9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - http://duma.consultant.ru/

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - Ссылка: http://search.ebscohost.com/
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
6. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы,

стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Line- http://www.dic.academic.ru

Программное обеспечение

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.

6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. Учебная аудитория для проведения занятий лекционного типа: Аудитория № 419 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	Лекции,	**Аудитория № 419** Оборудование: учебная мебель, доска, проектор OptomaEx542 i, Экран настенный Dinon **Перечень лицензионного программного обеспечения:** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.
2. Учебная аудитория для проведения практических занятий: Аудитория № 608 Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации. Аудитория № 507. Лаборатория управления информационной безопасностью. 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	лабораторные и практические занятия	**Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 404. Специализированный кабинет с лабораторным оборудованием.** Оборудование: учебная мебель, системные блоки\i5-10400 (2.9GHz)\H510M\8Gb\HDD 1Tb\корпус Micro ATX\Win10 Pro, мониторы ЖК 23.8" LG 24MK430H-B (1920x1080, IPS,75 Гц, 5 мс, 1000:1, 250 кд/м2, D-Sub, HDMI, кабель HDMI в комплекте), виртуальный тренажер «Аттестация объекта по требованиям защиты от утечек информации по техническим каналам». **Перечень лицензионного программного обеспечения:** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. **Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.** Оборудование: учебная мебель, доска, комплект учебного оборудования «Блочное кодирование», комплект учебного оборудования «Основы криптографии», учебно-лабораторный стенд «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ»

		Аудитория № 507. Лаборатория управления информационной безопасностью. Оборудование: учебная мебель, доска, мультимедиа, комплекс мониторинга WiFi сетей "Зодиак II", универсальный комплект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608 **4. Учебная аудитория для текущего контроля и промежуточной аттестации:** Аудитория № 610 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	Консультации, текущий контроль, промежуточная аттестация	**Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 610** Оборудование: учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK, кронштейн для телевизора NBP 5, Кабель HDMI (m)-HDH(m)ver14,10м.

Приложение № 1

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Аттестация объектов информатизации по требованиям безопасности** на 3 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часа
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	_
Учебных часов на самостоятельную работу обучающихся (СР)	53,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	_
Учебных часов на подготовку к экзамену (Контроль)	-

Форма контроля
Зачет 3 семестр

Семестр 3

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
	Модуль 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации.						
1	Тема 1.1. Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации.	2	4	–	6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа,
2	Тем 1.2. Организационная структура системы аттестации объектов информатизации (ОИ) по требованиям безопасности информации, как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.	2	2	2	6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа,
3	Тема 1.3. Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации. Участники аттестации и их полномочия (компетенции).	2	2	2	6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа,
4	Тема 1.4. Задачи, функции, права и обязанности органов по аттестации. Требования к органам по	2	2	2	6	Самостоятельное изучение	практическая работа, лабораторная работа,

	аттестации объектов информатизации. Деятельность аттестационных комиссий.					рекомендуемой основной и дополнительной литературы	
5	Тема 1.5. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации. Государственный надзор за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.	2	4	4	6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа, тест
	Модуль 2. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации						
6	Тема 2.1. Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации (требования к содержанию программ и методик аттестационных испытаний автоматизированных систем, защищаемых помещений). Требования обеспечения защиты информации ограниченного доступа при проведении аттестации объектов информатизации.	2	1	–	6		практическая работа, лабораторная работа
7	Тема 2.2. Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (экспертно- документальный метод; измерение и оценка уровней; ПЭМИН для отдельных технических средств автоматизированной системы и каналов утечки информации; проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного пуска средств защиты информации от НСД и наблюдения за их работой; попытки «взлома систем защиты информации»).	2	1	2	6		практическая работа, лабораторная работа
8	Тема 2.3. Разработка заключения и протоколов испытаний по результатам аттестации объектов информатизации. Оформление, регистрация и выдача	2	2	2	6		практическая работа, лабораторная работа

	«Аттестата соответствия». Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации (подача и рассмотрение заявки на аттестацию объектов информатизации; предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний; проведение аттестационных испытаний объектов информатизации; оформление, регистрация и выдача аттестата соответствия). Порядок рассмотрения апелляций.						
9	Тема 2.4. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации. Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации.	2	2	4	5,8		практическая работа, лабораторная работа, тест
Всего часов		18	18	18	53,8		