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

Утверждено:
на заседании кафедры
протокол №6 от 31 января 2022 г.
Зав. кафедрой _____ /Исмагилова А.С.

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Основы аудита и аттестации объектов информатизации

Обязательная часть (Б1.О.49)

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль) подготовки
Организация и технологии защиты информации (в системе государственного и муниципального управления)

Квалификация
бакалавр

Разработчик (составитель) . _____ .	_____ / Салов И.В.

Для приема: 2022г.

Уфа 2022 г.

Составитель: Салов Игорь Владимирович

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол № 6 от 31 января 2022 г.

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 4
2. Цель и место дисциплины в структуре образовательной программы 4
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся) 4
4. Фонд оценочных средств по дисциплине 5
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. 5
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. 5
5. Учебно-методическое и информационное обеспечение дисциплины 14
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 14
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы 15
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 17

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**
	ОПК-2.4 Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами.	ПК-3.1 Знает методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Знать методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами..
		ПК-3.2 Умеет разрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Уметьразрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.
		ПК-3.3 Владеет методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Владеть методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами..

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы аудита и аттестации объектов информатизации» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 4 курсе в 8 семестре.

Целью учебной дисциплины «Основы аудита и аттестации объектов информатизации», является формирование навыков организации мониторинга защищенности информации и проведения аттестационных испытаний на объектах информатизации.

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

ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами..

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК-3.1 Знает методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Знать методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами..	Не знает.	Знает методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.
ПК-3.2 Умеет разрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Уметьразрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Не умеет.	Умеет разрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.
ПК-3.3 Владеет методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Владеть методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами..	Не владеет	Владеет методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.

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

ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами..

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-3.1 Знает методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Знать методику проведения аудита защищенности объекта информатизации в соответствии с нормативными документами..	тестирование, практическое задание
ПК-3.2 Умеет разрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Уметьразрабатывать и реализовывать планы проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	тестирование, практическое задание
ПК-3.3 Владеет методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами.	Владеть методикой и принципами проведения аудита защищенности объекта информатизации в соответствии с нормативными документами..	тестирование, практическое задание

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 экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).
Шкалы оценивания:

(для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Основы аудита и аттестации объектов информатизации»

Направление подготовки: 10.03.01 Информационная безопасность

курс 4, семестр8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Базовые понятия аттестации объектов информатизации.				
Текущий контроль			0	

Практическая работа	7	5	0	35
Рубежный контроль				
Тест	16	1	0	16
Всего		4	0	50
Модуль 2. . Система документационного сопровождения аттестации объекта информатизации.				
Текущий контроль				
Практическая работа	4	4	0	36
Рубежный контроль				
Тест	14	1	0	14
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

Зачет

Вопросы для зачета:

1. 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.
2. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная).
3. Участники аттестации и их полномочия (компетенции).
4. Критически важные объекты инфраструктуры Российской Федерации: классификация и категории.
5. Задачи, функции, права и обязанности органов по аттестации. Деятельность аттестационных комиссий.
6. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.
7. Основные мероприятия по проведению аттестации объектов информатизации критически важных объектов на соответствие требованиям безопасности информации.
8. Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации критически важных объектов.
9. Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации критически важных объектов.
10. Экспертно-документальный метод проверки, применяемый при проведении аттестационных испытаний.

11. Инструментальный метод проверки, применяемый при проведении аттестационных испытаний с использованием контрольно-измерительной аппаратуры.

12. Этапы аттестации объектов информатизации критически важных объектов.

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

14. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

15. Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации

16. Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний.

17. Заключение договоров на аттестацию. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

18. Проведение аттестационных испытаний объекта информатизации.

19. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций.

20. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации критически важных объектов.

21. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации критически важных объектов.

22. Заключение аттестационной проверки: структура, содержание.

23. Протокол аттестационного испытания: структура, содержание.

24. Аттестат соответствия объектов информатизации критически важных объектов требованиям безопасности.

25. Типовые организационные структуры государственной системы защитыинформации.

26. Функции контроля и надзора органа государственной власти в области обеспечения безопасности и защитыинформации.

27. Специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечениябезопасности.

28. Классификация услуг организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационнойбезопасности.

29. Специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственногорегулирования.

30. Какие функции выполняет служба безопасности предприятия для решения задачи физическойзащиты.

31. Функции служба безопасности предприятия для решения задачи обеспечения информационнойбезопасности.

32. Структура полномасштабной системы обеспечения безопасности и защиты информации.

33. Специфика организации и выполнения охранныхфункций.

34. Специальные мероприятия и действия сотрудников службы безопасности по организации объектовыхрежимов.

35. Основное назначение корпоративной нормативной базы службы безопасности.

36. Структура корпоративной нормативной базы службыбезопасности.

37. Разделы типового формата положений о структурных подразделениях службы безопасности.

38. Перечень и краткая характеристика основных нормативных документов процедурного уровняИБ.

39. Чем определяется срок жизненного цикла корпоративной нормативной базы по информационнойбезопасности.

40. Различие в определениях политики информационнойбезопасности.
41. Отличие нормативно-методических документов политики безопасности от нормативных документов процедурногоуровня.
42. Особенности документального оформления политики безопасности, и чем они объясняются.
43. Типовое содержание политики безопасности, оформленной в виде единогодокумента.
44. Назначение Концепции обеспечения информационной безопасностиорганизации.
45. Содержание Концепции обеспечения информационной безопасностиорганизации.
46. Цель и задача аудита информационнойбезопасности.
47. Методология деятельности по обеспечению безопасности объекта на основе политики безопасности.
48. Перечень контрольных мероприятий и действий по оценке уровня безопасности объекта.
49. Определение понятия «режимный объект» и видов обеспечения егобезопасности.
50. Цель и задачи организации пропускногорежима.
51. Нормативная основа организации пропускного режима и каково ее общеесодержание.
52. Порядок пропуска (прохода) физических лиц на территорию режимногообъекта.
53. Правила въезда (выезда) транспортных средств на территорию режимногообъекта.
54. Особенности организации охраны режимногообъекта.
55. Суть и содержание нормативной основы организации охранныхмероприятий.
56. Действия охраны при тревоге и других чрезвычайныхситуациях.
57. Цель и задачи организационного обеспечения внутриобъектовогорежима.
58. Содержание организационного обеспечения режимасекретности.
59. Организация конфиденциальногоделопроизводства.
60. Организационные процедуры обеспечения режимасекретности.
61. Организация засекречивания сведений, составляющих государственнуютайну.
62. Организация допуска и доступа к сведениям, составляющим государственнуютайну.
63. Правила обращения секретныхдокументов.
64. Основные правила организации секретногоделопроизводства.
65. Организационный режим делопроизводства и обращения документов с грифом «Для служебного пользования»(ДСП).
66. Особенности современных систем автоматизированногодокументооборота.
67. Принципиальные отличия технологии workflow от традиционных систем автоматизации управленческойдеятельности.
68. Суть и содержание работ по противодействию технической разведке.
69. Определение понятия и краткая характеристика аттестация объектовинформатизации.
70. Основной перечень работ по аттестации объектовинформатизации.
71. Цель и задачи проведения служебных расследований инцидентов нарушений информационнойбезопасности.
72. Организация проведения служебного расследование инцидента при реализации угрозы информационнойбезопасности.
73. Определение эффективности менеджмента в области информационнойбезопасности.
74. Суть и содержание использования организационных схем определения надежности персонала
75. Суть и содержание использования организационных схем определения профессиограмм при подборекадров.
76. Нормативно-правовая основа для введения дополнительных ограничений по контролю за деятельностьюперсонала.

77. Организационные процедуры для составления психологического портретаработника.
78. Особенности верификации сведений о работнике при его приеме наработу.
79. Методы психологического тестирования и графологическойэкспертизы.
80. Специфика использования метода психофизиологическоготестирования.
81. Цель ранжирования должностей по степени риска управлениябизнес-процессами.
82. Участие службы безопасности в процедурах увольненияисотрудников.
83. Определение мотивации как метода управленияперсоналом.
84. Суть и содержание метода положительногостимулирования.
85. Особенности метода отрицательногостимулирования.
86. Создание ориентирующих условий дляперсонала.
87. Актуальность вопросов самообучения и повышенияквалификации.
88. Основные специальности, по которым осуществляется подготовка кадров в области обеспечения информационнойбезопасности.
89. Основные направления образовательной деятельности в области обеспечения информационнойбезопасности.

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

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 ответов из предложенных вариантов.

1) Выберите виды организационных мер по защите информации?
1) Установление пространственных ограничений
2) Временные ограничения на условия использования и режимы работы объекта информатизации
3) Установка сертифицированного средства защиты информации от несанкционированного доступа
4) Пространственное зашумление путем установки генератора шума
2) На какое количество подсистем условно делится система защиты информации от несанкционированного доступа?
1) 7
2) 4
3) 6
4) 5
3) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты информации от несанкционированного доступа посредством использования механизмов шифрования пользовательских данных?

1) Регистрации и учета
2) Криптографической защиты
3) Обеспечения целостности
4) Управления доступом

4) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты от несанкционированных изменений программной и аппаратной среды ПЭВМ?

1) Регистрации и учета
2) Криптографической защиты
3) Обеспечения целостности
4) Управления доступом

5) В каких случаях необходимо применять активные технические меры по защите информации?

1) В случае использования на ОИ несертифицированных средств вычислительной техники
2) В случае недостаточности использованных организационных и пассивных технических мер защиты информации
3) В случае большой границы контролируемой зоны
4) В случае обработки информации, содержащей сведения, составляющие государственную тайну

6) Меры по защите информации, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации – это:

1) Пассивные технические меры
2) Криптографическиемеры
3) Организационные меры
4) Активные технические меры

7) Подлежат ли реализации меры защиты информации - обнаружение (предотвращение) вторжений при защите государственных информационных систем?

1) Да

2) Нет

8) Какой документ должны иметь средства защиты информации для подтверждения их соответствия установленным требованиям по защите информации?

1) Аттестат соответствия
2) Лицензию
3) Аттестат аккредитации
4) Сертификат соответствия

9) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для фиксации системных событий в специальном журнале?

1) Регистрации и учета
2) Криптографической защиты
3) Обеспечения целостности
4) Управления доступом

10) Какие виды средств используются при реализации технических мер защиты информации?

1) Инструментальные
2) Технические
3) Программно-технические
4) Контрольные

11) Подсистема управления доступом предназначена для:

1) Защиты объекта информатизации от сторонних пользователей, не имеющих прав доступа к ОИ и пытающихся осуществить несанкционированный доступ к информации
2) Защиты ПЭВМ от внедрения программных закладок, вирусов и прочих специальных математических воздействий на систему
3) Защиты информации от несанкционированного доступа посредством использования механизмов шифрования пользовательских данных
4) Управления доступом уполномоченных пользователей к объекту информатизации в соответствии с правилами разграничения доступа

12) К какому виду мер относится мера: размещение дисплеев и других средств отображения информации таким образом, чтобы исключить несанкционированный или непреднамеренный просмотр защищаемой информации?
1) Организационная
2) Техническая

13) Применение каких мер защиты может исключить утечку информации по акустическому каналу?
1) Проведение специальной проверки технических средств, установленных в помещении
2) Увеличение границы контролируемой зоны на время проведения «закрытых» совещаний
3) Использование аналоговых телефонных аппаратов
4) Использование специальных материалов для облицовки стен, для пола и потолка, повышающих звукоизоляцию защищаемого помещения
5) Использование системы активной защиты речевой информации
6) Использование специальных звукоизолирующих экранов на элементах систем отопления и вентиляции

14) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты ОИ от сторонних пользователей, не имеющих прав доступа к ОИ и пытающихся осуществить несанкционированный доступ к информации?
1) Регистрации и учета
2) Криптографической защиты
3) Обеспечения целостности
4) Управления доступом

15) Что лежит в основе формирования перечня достаточных мер защиты информации?
1) Результаты обследования объекта информатизации
2) Сформулированные требования по защите информации
3) Перечень установленных на объекте информатизации средств защиты информации
4) Результаты аттестации объекта информатизации

16) При каком принципе управления доступом уполномоченный пользователь получает доступ к документам заданного уровня конфиденциальности?
1) Дискреционный
2) Мандатный

17) К какому виду мер относится мера: использование специальных звукоизолирующих экранов на элементах систем отопления и вентиляции?
1) Организационная
2) Техническая

18) Выберите верный номер сертификата соответствия на фильтр сетевой помехоподавляющий ФСП-1Ф-7А
1) 2533/1 до 09.11.2021
2) 633/1 до 15.06.2020
3) 148/2 до 01.04.2019
4) 3552 до 14.04.2019

Модуль 1. Представление информации

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	
Модуль 1		0,64
Модуль 2		0,56

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

Модуль 1. Базовые понятия аттестации объектов информатизации.

1. Категорирование информации, обрабатываемой на ОИ.
2. Нормативно–правовые основы аттестации ОИ.
3. Система аттестации объектов информатизации в РФ.
4. Лицензирование деятельности в сфере аттестации ОИ.
5. Этапы аттестации объектов информатизации.

Модуль 2. Система документационного сопровождения аттестации объекта информатизации.

6. Проведение аттестационных испытаний объектов информатизации.
7. Аттестат соответствия.
8. Протокол аттестационных испытаний.
9. Заключение аттестационной проверки.

Практическая работа № 1

Модуль 1. Базовые понятия аттестации объектов информатизации

Тема: Категорирование информации, обрабатываемой на ОИ.

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
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?

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

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание Модуль 1 Модуль 2	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	 0/3/7 0/2/4

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 EastView) - 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 EastView) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. AnnualReviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступвсетивуза, языканглийский. - 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. TaylorandFrancis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. WebofScience - наукометрическая, библиографическая и реферативная база данных издательской корпорации ThomsonReuters. 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

Программноеобеспечение

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. Лицензиибессрочные.
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).GNUGeneralPublicLicense. 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 № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **3.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс	Лекции, практические занятия, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный ClassicNorma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный LumienMasterPikture 153*203 MatteWhiteFiberClas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Thermaltake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование:

аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **4.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6.** ***помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Основы аудита и аттестации объектов информатизации** на 8 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	44,2
лекций	22
практических/ семинарских	22
лабораторных	–
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)	27,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 8 семестр

Семестр 8

№	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
1	Модуль 1. Базовые понятия аттестации объектов информатизации.					Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест
	Тема: Общая характеристика процесса аттестации объектов информатизации.	4	4		4		
	Тема: Нормативная правовая база по аттестации объектов информатизации.	2	2		2		
	Тема: Организационная структура системы аттестации объектов информатизации в РФ: характеристика отдельных подсистем.	2	2		2		
	Тема: Этапы аттестации объектов информатизации.	2	2		2		
	Тема:Проведение аттестационных испытаний объектов информатизации.	2	2		4		
2	Модуль 2. Система документационного сопровождения аттестации объекта информатизации.					Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест
	Тема: Оформление, регистрация и выдача «Аттестата соответствия».	2	2		4		
	Тема: Заключение аттестационной проверки.	2	2		2		
	Тема: Протокол аттестационных испытаний.	2	2		2		

	Тема: «Аттестат соответствия» на объект информатизации	2	2		2		
	Тема: Специфика процедуры аттестации объекта информатизации критической информационной инфраструктуры.	2	2		3,8		
Всего часов		22	22	0	27,8		