


МИНОБРНАУКИ РОССИИ
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 (МОДУЛЯ)

Дисциплина
Организационное и правовое обеспечение информационной безопасности
Обязательная часть

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации
(в системе государственного и муниципального управления)

Квалификация
бакалавр

Разработчик (составитель)
к.ф.-м.н., доцент



/И.А. Шагапов

Для приема: 2021 г.

Уфа – 2021

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры, протокол № 8 от «24» февраля 2021 г.

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)	5
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	8
5. Учебно-методическое и информационное обеспечение дисциплины	20
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	20
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	21
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	21

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

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ОПК- 5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК 5.1 Знать значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации
		ОПК-5.2 Уметь применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации
		ОПК-5.3 Владеть технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации
	ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК 8.4 Знать важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Знает важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе
		ОПК-8.5 Уметь подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в современном обществе	Умеет подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в современном обществе
		ОПК-8.6 Владеть методами подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Владеет методами подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасно-

сти) относится к группе дисциплин обязательной части образовательной программы.

Дисциплина изучается на 2-3 курсе в 4-5 семестрах.

Целью дисциплины «Организационное и правовое обеспечение информационной безопасности» является приобретение обучающимися знаний по организационному и правовому обеспечению защиты информации, а также формирование практических навыков работы в реальных условиях деятельности по защите информации.

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

ОПК- 5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (зачет)	
		«Незачтено»	«Зачтено»
ОПК 5.1 Знать значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Не знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации
ОПК-5.2 Уметь применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Не умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации
ОПК-5.3 Владеть технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Не владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»

ОПК 5.1 Знать значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Не знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает некоторую значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации, делает ошибки	Частично знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации
ОПК-5.2 Уметь применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Не умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять некоторые нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации, делает ошибки	Частично умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации
ОПК-5.3 Владеть технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Не владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения некоторых нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации, делает ошибки	Частично владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации

ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (зачет)	
		«Незачтено»	«Зачтено»
ОПК 8.4 Знать важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Знает важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Не знает важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Знает важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе
ОПК-8.5 Уметь подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации	Умеет подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в со-	Не умеет подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в современном обществе	Умеет подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в современном обществе

тов для решения задач защиты информации в современном обществе	ментов для решения задач защиты информации в современном обществе		стве, делает ошибки	ских документов для решения задач защиты информации в современном обществе	ментов для решения задач защиты информации в современном обществе
--	---	--	---------------------	--	---

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

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК 5.1 Знать значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Знает значимость нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4
ОПК-5.2 Уметь применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Умеет применять нормативные акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4
ОПК-5.3 Владеть технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Владеет технологией применения нормативных актов, нормативных и методических документов, регламентирующих деятельность по защите информации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК 8.4 Знать важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Знает важность подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4
ОПК-8.5 Уметь подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в современном обществе	Умеет подбирать, изучать и обобщать научно-техническую литературу для решения задач защиты информации в современном обществе	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4
ОПК-8.6 Владеть методами подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Владеет методами подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов для решения задач защиты информации в современном обществе	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2,3,4

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 зачета:

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

(*для экзамена*):

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины

Организационное и правовое обеспечение информационной безопасности

Направление подготовки 10.03.01 ИБ

Курс 2, семестр 4

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №1	15	1	0	15
1. Лабораторная работа №1	15	1	0	15
Всего				50
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №2	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №2	15	1	0	15
1. Лабораторная работа №2	15	1	0	15
Всего				50
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практиче-				-10

ских занятий				
Итоговый контроль				
Зачет				

Рейтинг – план дисциплины

Организационное и правовое обеспечение информационной безопасности
Направление подготовки 10.03.01 ИБ
Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №3	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	5	1	0	5
1. Лабораторная работа №3	10	1	0	10
Всего				35
Модуль 4.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №4	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №4	5	1	0	5
1. Лабораторная работа №4	10	1	0	10
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен				30

Комплект контрольных работ

Модуль 1

Письменная контрольная работа №1
Основные силы и средства организации по ЗИ

Вопросы

1. С какой целью создается самостоятельное подразделение по защите информации в организации? Примеры.
2. Что означает аутсорсинг в области информационной безопасности? Примеры.
3. Обязанности руководителя организации в области защиты информации.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-3	15
Максимальный балл	15

Модуль 2

Письменная контрольная работа №2 Угрозы и уязвимости информационной безопасности

Вопросы

1. Зайти на сайт ФСТЭК, изучить содержание сайта
2. Выбрать на свое усмотрение 3-4 угрозы и 3-4 уязвимости из предложенного банка
3. Изучить их и подготовить краткий отчет.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-3	15
Максимальный балл	15

Модуль 3

Письменная контрольная работа №3 Отнесение сведений к конфиденциальной информации

Вопросы

1. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
2. Разработка комплекта документов при организации пропускного режима на предприятии.
3. Основные документы, разрабатываемые на охраняемых объектах.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-3	5
Максимальный балл	5

Модуль 4

Письменная контрольная работа №4 Работа с персоналом, допущенным к конфиденциальной информации

Вопросы

1. Права и обязанности оператора персональных данных.
2. Правовые основания работы с персональными данными.
3. Права субъекта персональных данных.
4. Права и обязанности держателя (обладателя) массивов персональных данных.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-4	5
Максимальный балл	5

Комплект практических заданий

Модуль 1

Типовое практическое задание 1

Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель угроз информационной безопасности.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Модуль 2

Типовое практическое задание 2

Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.

Методические указания

- а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.
- б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Модуль 3

Типовое практическое задание 3
Разработка технического задания (ТЗ) в области информационной безопасности

1. Выбрать вариант для написания ТЗ объект (услуга, работа, разработка, модификация и т.д. в области ИБ)
2. Собрать необходимую информацию.
3. Разработать техническое задание.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Методические указания

- а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.
- б. Помнить, для чего и для кого разрабатывается ТЗ.

Модуль 4

Типовое практическое задание 4
Разработка перечня информации, составляющей коммерческую тайну организации

1. Выбрать (придумать гипотетическую) коммерческую организацию.
2. Изучить деятельность организации.
3. Составить перечень информации (всей), циркулирующей в организации.
4. Провести анализ перечня с фильтрацией информации, имеющей коммерческую ценность для организации.
5. Составить перечень информации, составляющей коммерческую тайну организации

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	10
Максимальный балл	10

Комплект лабораторных работ

Модуль 1

Типовая лабораторная работа №1
Информационная безопасность технической системы

Цель работы: закрепление на практике понятия информационная безопасность технической системы

1. Выбрать произвольным образом техническую систему.
2. Привести подробное описание данной технической системы.
3. Расписать максимально подробно, что означает информационная безопасность для данной технической системы. Подобрать типичные примеры, аналогии.
4. Составить отчет по работе.

Методические рекомендации по выполнению работы.

Перед выполнением работы полезно ответить на следующие вопросы:

- Какие сложности возникли при описании технической системы?
- Чем отличается информационная безопасность технической системы от информационной безопасности личности?
- Чем отличается информационная безопасность от защиты информации?:

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	10
Выполнены пункты 1-4	15
Максимальный балл	15

Модуль 2

Типовая лабораторная работа №2

Информационная война и информационное оружие

Цель работы: закрепление на практике понятия информационная война

1. Группа делится на две подгруппы..
2. Выбирается область (вид) деятельности.
3. Каждая подгруппа выбирает тип «информационного оружия» и разрабатывает план «информационной войны» против другой подгруппы и пытается ее «реализовать», одновременно «защищаясь» от противника.
4. По результатам проводится анализ и «эффективность» действий каждой стороны.
5. Составить отчет по работе каждой подгруппы.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- Чем руководствовались при выборе информационного оружия?
- Какие методы защиты от информационного оружия противника применялись?
- Что означает эффективность применения информационного оружия?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	10
Выполнены пункты 1-5	15
Максимальный балл	15

Модуль 3

Типовая лабораторная работа №3

Объекты и угрозы информационной безопасности

Цель работы: закрепление умений распознавать на практике угрозы объектам информационной безопасности

1. Выбрать произвольным образом объект обеспечения информационной безопасности.
2. Привести подробное описание объекта.
3. Составить перечень угроз объекту. Произвести классификацию по выбранному признаку.

4. Оценить актуальность этих угроз. Попытаться определить источники этих угроз. Насколько возможно, выявленные угрозы связать с уязвимостями объектов.
5. Составить отчет по работе.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- Чем руководствовались при составлении перечня угроз?
- Какие преимущества и недостатки имеет выбранная классификация угроз?
- Какова связь между угрозами и уязвимостями?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	10
Максимальный балл	10

Модуль 4

Типовая лабораторная работа №4

Обеспечение информационной безопасности объекта

Цель работы: закрепление умений обеспечивать информационную безопасность объекта

1. Для объекта из лабораторной работы №3 составить несколько вариантов для противодействия выявленным угрозам .
2. оценить эффективность каждого варианта.
3. Выбрать наиболее эффективный вариант.
4. Подробно расписать, как можно реализовать выбранный вариант противодействия угрозам.
5. Составить отчет по работе.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- На сколько типичным является объект?
- Из каких соображений были составлены варианты противодействия угрозам?
- На сколько «законным» является наиболее эффективный вариант?
- Что можно сказать, на счет экономической эффективности выбранного варианта?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	10
Максимальный балл	10

Перечень вопросов для зачета:

Типовые вопросы для зачета

1. Концептуальные основы информационной безопасности
2. Основные принципы и условия организационной защиты информации.
3. Основные подходы и требования к организации системы защиты информации.
4. Основные силы и средства, используемые для организации защиты информации
5. Отнесение сведений к различным видам конфиденциальной информации.
6. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
7. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну
8. Отнесение сведений к государственной тайне.
9. Засекречивание сведений и их носителей
10. Отнесение сведений к коммерческой тайне.
11. Основания и порядок рассекречивания сведений и их носителей.
12. Основные положения допуска персонала предприятия к конфиденциальной информации.
13. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска.
14. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.
15. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну
16. Порядок доступа к конфиденциальной информации командированных лиц
17. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации
18. Роль и место внутриобъектового режима в общей системе защиты информации на предприятии.
19. Основные цели, подходы и принципы организации внутриобъектового режима.
20. Силы и средства, используемые при организации внутриобъектового режима
21. Роль и место пропускного режима в общей системе защиты информации на предприятии.
22. Цели и задачи пропускного режима.
23. Основные элементы системы организации пропускного режима, используемые силы и средства
24. Организация охраны предприятий.

Экзаменационные билеты

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

Перечень вопросов для экзамена:

1. Основные принципы и условия организационной защиты информации.
2. Основные подходы и требования к организации системы защиты информации.
3. Основные силы и средства, используемые для организации защиты информации
4. Отнесение сведений к различным видам конфиденциальной информации.
5. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
6. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну
7. Отнесение сведений к государственной тайне.
8. Засекречивание сведений и их носителей
9. Отнесение сведений к коммерческой тайне.
10. Основания и порядок рассекречивания сведений и их носителей.

11. Основные положения допуска персонала предприятия к конфиденциальной информации.
12. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска.
13. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.
14. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну
15. Порядок доступа к конфиденциальной информации командированных лиц
16. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации
17. Роль и место внутриобъектового режима в общей системе защиты информации на предприятии.
18. Основные цели, подходы и принципы организации внутриобъектового режима.
19. Силы и средства, используемые при организации внутриобъектового режима
20. Роль и место пропускного режима в общей системе защиты информации на предприятии.
21. Цели и задачи пропускного режима.
22. Основные элементы системы организации пропускного режима, используемые силы и средства
23. Организация охраны предприятий
24. Организация защиты информации при проведении совещаний.
25. Порядок проведения совещания и использования его материалов
26. Организация защиты информации в ходе издательской и рекламной деятельности.
27. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации
28. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу.
29. Порядок передачи различных видов конфиденциальной информации иностранным государствам при осуществлении международного сотрудничества.
30. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу.
31. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам
32. Допуск предприятий к проведению работ с конфиденциальной информацией.
33. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну.
34. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий
35. Допуск предприятий к проведению работ с конфиденциальной информацией.
36. Организация проведения государственной аттестации руководителей предприятий
37. Организация аналитической работы и контроля состояния защиты конфиденциальной информации
38. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений
39. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну
40. Уголовно-правовая защита в сфере компьютерной информации
41. Уголовно-правовая защита сведений, составляющих государственную тайну
42. Административно-правовая защита информации с ограниченным доступом
43. Гражданско-правовая защита служебной и коммерческой тайны

44. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений
45. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

Образец экзаменационного билета:

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

Специальность 10.03.01 ИБ

Дисциплина: ОПОИБ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Основные подходы и требования к организации системы защиты информации. Организация защиты информации при проведении совещаний.

Зав. кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки (в баллах):

- **25-30 баллов** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- **17-24 баллов** выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- **10-16 баллов** выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- **0-10 баллов** выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Темы лекционных занятий (4 семестр)

(16 часов)

1. Концептуальные основы информационной безопасности. Организационные основы защиты информации
2. Отнесение сведений к конфиденциальной информации.
3. Засекречивание и рассекречивание сведений
4. Организация допуска и доступа персонала к конфиденциальной информации
5. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

6. Организация внутриобъектового и пропускного режимов на предприятии.
Организация охраны предприятий.
7. Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности
8. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу

Темы лекционных занятий (5 семестр)

(18 часов)

9. Допуск предприятий к проведению работ с конфиденциальной информацией
10. Организация аналитической работы по защите конфиденциальной информации
11. Организация контроля состояния защиты конфиденциальной информации
12. Организация служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений
13. Проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений
14. Уголовно-правовая защита сведений, составляющих коммерческую тайну. Уголовно-правовая защита в сфере компьютерной информации. Уголовно-правовая защита сведений, составляющих государственную тайну
15. Административно-правовая защита информации с ограниченным доступом. Гражданско-правовая защита служебной и коммерческой тайны
16. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений
17. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

Темы семинарских занятий (4 семестр)

(16 часов)

9. Концептуальные основы информационной безопасности. Организационные основы защиты информации
10. Отнесение сведений к конфиденциальной информации.
11. Засекречивание и рассекречивание сведений
12. Организация допуска и доступа персонала к конфиденциальной информации
13. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации
14. Организация внутриобъектового и пропускного режимов на предприятии.
Организация охраны предприятий.
15. Организация защиты информации при проведении совещаний, в ходе издательской и рекламной деятельности
16. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу

Темы семинарских занятий (5 семестр)

18 (часов)

18. Допуск предприятий к проведению работ с конфиденциальной информацией
19. Организация аналитической работы по защите конфиденциальной информации
20. Организация контроля состояния защиты конфиденциальной информации
21. Организация служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений
22. Проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений

23. Уголовно-правовая защита сведений, составляющих коммерческую тайну. Уголовно-правовая защита в сфере компьютерной информации. Уголовно-правовая защита сведений, составляющих государственную тайну
24. Административно-правовая защита информации с ограниченным доступом. Гражданско-правовая защита служебной и коммерческой тайны
25. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений
26. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

Критерии оценки (в баллах) (должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):

- 0,55 баллов выставляется студенту, если выполнил задание на 100%
- 0,36 баллов выставляется студенту, если выполнил задание на 75%
- 0,2 баллов выставляется студенту, если выполнил задание на 50%
- 0 баллов выставляется студенту, если не выполнил задание

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
2. Малюк, А.А. Теория защиты информации / А.А. Малюк. - Москва : Горячая линия - Телеком, 2012. - 184 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0246-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253553>
3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>

Дополнительная литература

4. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93245>
5. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457170>
6. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю.И. Коваленко. - Москва : Горячая линия - Телеком, 2012. - 140 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-

0261-9 ; То же [Электронный ресурс]. -

URL: <http://biblioclub.ru/index.php?page=book&id=253538>

7. Шишкин, В.В. МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. [Электронный ресурс] / В.В. Шишкин, Н.К. Юрков, Н.Ж. Мусин. — Электрон. дан. // Надежность и качество сложных систем. — 2013. — № 4. — С. 9-13. — Режим доступа: <http://e.lanbook.com/journal/issue/298784> — Загл. с экрана.
8. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: <https://e.lanbook.com/book/97352>. — Загл. с экрана.

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

1. Справочная правовая система «КонсультантПлюс» – <http://www.consultant-plus.ru>.
2. Электронная библиотечная система «Университетская библиотека онлайн» – <https://biblioclub.ru>.
3. Электронная библиотечная система издательства «Лань» – <https://e.lanbook.com/>
4. Электронный каталог Библиотеки БашГУ – <http://www.bashlib.ru/catalogi/>
5. www.fstec.ru – сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. <http://univertv.ru/video/matematika/> – Открытый образовательный видеопортал Uni-verTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www.edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), ауди-	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации,	Аудитория № 403 Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition.
		Аудитория № 405 Учебная мебель, доска, вокальные	

<p>тория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</p> <p>2. учебная аудитория для проведения лабораторных работ: Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус).</p> <p>3. учебная аудитория для проведения занятий семинарского типа: 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).</p> <p>4. 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 аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p>	<p>текущий контроль, промежуточная аттестация</p>	<p>радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром Promethean ActivBoard 387 RPOMOUNT EST -1 шт., Ком-ер встраиваемый в кафедру INTEL-Corei3-4150/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.</p> <p>Аудитория № 413 Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>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.</p> <p>Аудитория № 416 Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 418 Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p>Аудитория № 419 Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 515 Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профессиональный 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/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла</p>	<p>Договор №104 от 17.06.2013 г. Лицензии бессрочные.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.</p>
---	---	--	---

<p>5. 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).</p> <p>6. помещения для самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p>7.помещение для хранения и профилактического обслуживания учебного оборудования: аудитория № 523 (гуманитарный корпус).</p>		<p>секционные последующих рядов с пюпитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>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.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p>Лаборатория полигон технической защиты информации № 508 Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект 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".</p> <p>Аудитория № 523 Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
---	--	---	--

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

Содержание рабочей программы
дисциплины (4 семестр)

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	32,2
лекций	16
практических/ семинарских	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	39,8
Учебных часов на подготовку к зачету	

Форма контроля:
Зачет 4 семестр

Содержание рабочей программы
дисциплины (5 семестр)

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	37,2
лекций	18
практических/ семинарских	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	79,8
Учебных часов на подготовку к экзамену	27

Форма контроля:
Экзамен 5 семестр

4 семестр

№	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	СРС		
1	2	3	4	5	6	7	8
1	Основы организационной защиты информации Концептуальные основы информационной безопасности Организационные основы защиты информации	2	2		5	Изучить литературу по организации допуска персонала к конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
2	Отнесение сведений к конфиденциальной информации.	2	2		5	Изучить нормативно-правовую базу по организации допуска персонала к конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
3	Засекречивание и рассекречивание сведений	2	2		5	Изучить нормативно-правовую базу по засекречиванию и рассекречиванию сведений	Письменная контрольная работа Практическое задание Лабораторная работа
4	Организация допуска и доступа персонала к конфиденциальной информации	2	2		5	Изучить нормативно-правовую базу по организации допуска персонала к конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
5	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	2	2		5	Изучить нормативно-правовую базу по организации допуска персонала к конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
6	Организация защиты информации на предприятии Организация внутриобъектового и пропускного режимов на предприятии Организация охраны предприятий	2	2		5	Собрать информацию для Положения о конфиденциальной информации для выбранного предприятия.	Письменная контрольная работа Практическое задание Лабораторная работа
7	Организация защиты информа-	2	2		5	Анализ собранной информации	Письменная контрольная рабо-

	ции при проведении совещаний, в ходе издательской и рекламной деятельности					для Положения о конфиденциальной информации для выбранного предприятия.	та Практическое задание Лабораторная работа
8	Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу	2	2		4,8	Разработать структуру Положения о конфиденциальной информации для выбранного предприятия.	Письменная контрольная работа Практическое задание Лабораторная работа
	Итого	16	16		39,8		

5 семестр

№	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	СРС		
1	2	3	4	5	6	7	8
9	Допуск предприятий к проведению работ с конфиденциальной информацией	2	2		9	Разработать Положение о конфиденциальной информации для выбранного предприятия	Письменная контрольная работа Практическое задание Лабораторная работа
10	Организация аналитической работы по защите конфиденциальной информации Организация аналитической работы по защите конфиденциальной информации	2	2		9	Изучить организационные аспекты аналитической работы по защите конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
11	Организация контроля состояния защиты конфиденциальной информации	2	2		9	Особенности аналитической работы по защите конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
12	Организация служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений	2	2		9	Эффективность аналитической работы по защите конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа

13	Проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений	2	2		9	Изучить уголовно-правовую защиту в области персональных данных	Письменная контрольная работа Практическое задание Лабораторная работа
14	Правовая защита конфиденциальной информации Уголовно-правовая защита сведений, составляющих коммерческую тайну. Уголовно-правовая защита в сфере компьютерной информации Уголовно-правовая защита сведений, составляющих государственную тайну	2	2		9	Изучить гражданско-правовую защиту в области персональных данных	Письменная контрольная работа Практическое задание Лабораторная работа
15	Административно-правовая защита информации с ограниченным доступом Гражданско-правовая защита служебной и коммерческой тайны	2	2		9	Изучить дисциплинарную ответственность за разглашение и (или) утрату конфиденциальных сведений в области персональных данных	Письменная контрольная работа Практическое задание Лабораторная работа
16	Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений	2	2		9	Изучить материальную ответственность за разглашение и (или) утрату конфиденциальных сведений в области персональных данных	Письменная контрольная работа Практическое задание Лабораторная работа
17	Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений	2	2		7,8	Изучить правовые аспекты аналитической работы по защите конфиденциальной информации	Письменная контрольная работа Практическое задание Лабораторная работа
	Итого	18	18		79,8		

