

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

Утверждено:  
на заседании кафедры  
протокол № 6 от 31 января 2022 г.  
Зав. кафедрой

 /А.С.Исмагилова

Согласовано:  
Председатель УМК института

 /Р.А. Гильмутдинова

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Дисциплина  
**Информационная безопасность организации**

Часть, формируемая участниками образовательных отношений

**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: 2022 г.

Уфа – 2022

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры управления информационной безопасностью 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 \_\_\_\_\_ / \_\_\_\_\_ Ф.И.О/

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/

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	4
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	6
5. Учебно-методическое и информационное обеспечение дисциплины	17
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	17
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	18
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	19

## 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
	ПК-2 Способен управлять защитой информации в автоматизированных системах	ПК 2.4 Знать основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия
		ПК 2.5 Уметь применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия
		ПК 2.6 Владеть основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия

## 2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность организации» относится к группе дисциплин вариативной части образовательной программы.

Дисциплина изучается на 3-4 курсе в 6-7 семестрах.

Целью учебной дисциплины «Информационная безопасность организации» является освоение методов по поддержанию режимов безопасности и конфиденциальности; определению положений, прав, обязанностей и ответственности должностных лиц по вопросам безопасности, а также по осуществлению представительских функций предприятия в данной области ее деятельности; изучение и освоение задач по обеспечению безопасности предприятия, анализ возможных мероприятий организационно-технического и правового характера, направленных на сохранность собственности, в том числе интеллектуальной; технической базы, общесистемного и прикладного программного обеспечения экономических информационных систем и технологий.

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

Содержание рабочей программы представлено в Приложении 1.

## 4. Фонд оценочных средств по дисциплине

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

**ПК-2 Способен управлять защитой информации в автоматизированных системах**

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (зачет)	
		«Незачтено»	«Зачтено»
ПК 2.4 Знать основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Не знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия
ПК 2.5 Уметь применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Не умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия
ПК 2.6 Владеть основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Не владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ПК 2.4 Знать основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Не знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает некоторые возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия, допускает ошибки	Частично знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия

ПК 2.5 Уметь применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Не умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Умеет применять некоторые методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия, допускает ошибки	Частично умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия
ПК 2.6 Владеть основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Не владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Владеет некоторыми методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия, допускает ошибки	Частично владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия

**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
ПК 2.4 Знать основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия ПК 2.5 Уметь применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия ПК 2.6 Владеть основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Знает основные возможности управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Умеет применять основные методы управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Владеет основными методами управления защитой информации в автоматизированных системах в рамках защиты коммерческой тайны предприятия	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2

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

Информационная безопасность организации

Направление подготовки 10.03.01 ИБ

Курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль 1.</b>				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	15	1	0	15
Рубежный контроль				
1. Письменная контрольная работа №1	25	1	0	25
Всего				50
<b>Модуль 2.</b>				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №2	15	1	0	15
Рубежный контроль				
1. Письменная контрольная работа №2	25	1	0	25
Всего				50
<b>Поощрительные баллы</b>				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
<b>Итоговый контроль</b>				

Зачет				
-------	--	--	--	--

### Рейтинг – план дисциплины

Информационная безопасность организации

Направление подготовки 10.03.01 ИБ

Курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль 3.</b>				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №3	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	15	1	0	10
Всего				35
<b>Модуль 4.</b>				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №4	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №4	15	1	0	15
Всего				35
<b>Поощрительные баллы</b>				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
<b>Итоговый контроль</b>				
Экзамен				30

### Комплект контрольных работ

Для контроля освоения и/или расширения знаний, умений, владений предусмотрены несколько контрольных работ.

Модуль 1.

Письменная контрольная работа №1  
Введение режима коммерческой тайны

### Вопросы

1. Цели установления режима коммерческой тайны.
2. Задачи по установлению режима коммерческой тайны.

3. Перечень организационных документов, необходимых для введения режима коммерческой тайны.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	15
Выполнены пункты 1-3	25
Максимальный балл	25

Модуль 2

Письменная контрольная работа №2  
Функционирование режима коммерческой тайны.

**Вопросы**

1. Потери организации при несоблюдении режима коммерческой тайны.
2. Регулирование отношений с сотрудниками и контрагентами.
3. Экономическая эффективность защиты сведений, составляющих коммерческую тайну.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	15
Выполнены пункты 1-3	25
Максимальный балл	25

Модуль 3.

Письменная контрольная работа №3  
Регулирование отношений

**Вопросы**

- 1 Какие документы готовятся для регулирования отношений с сотрудниками в рамках КТ?
- 2 Как организовывается регулирование отношений с контрагентами в рамках КТ?

Критерии оценки

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

Модуль 4

Письменная контрольная работа №4  
Экономическая эффективность коммерческой тайны

**Вопросы**

1. Что нужно для оценки рисков информационной безопасности для выбранного предприятия?
2. Что нужно для вычисления экономической эффективности защиты сведений, составляющих коммерческую тайну для выбранного предприятия?

**Критерии оценки**

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

**Комплект практических заданий**

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий.

**Модуль 1**

**Типовое практическое задание 1**

Составление перечня основных вопросов для обеспечения режима коммерческой тайны

1. Составить перечень основных вопросов, которые должны обсуждаться перед введением режима КТ на выбранном предприятии
2. Составить перечень информации, циркулирующей на выбранном предприятии
3. Составить перечень информации, составляющей коммерческую тайну выбранного предприятия

**Критерии оценки**

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	10
Выполнены пункты 1-3	15
Максимальный балл	15

**Модуль 2**

**Типовое практическое задание 2**

Разработка положения о коммерческой тайне предприятия.

1. Изучить и собрать сведения по произвольно выбранному (придуманному) коммерческому предприятию.
2. Проанализировать перечень информации по деятельности предприятия.
3. Разработать положение о коммерческой тайне для выбранного предприятия.

**Критерии оценки**

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	10

Выполнены пункты 1-3	15
Максимальный балл	15

**Модуль 3**  
Типовое практическое задание 3

Составление перечня основных вопросов для обеспечения режима коммерческой тайны

- 1 Для выбранного предприятия расписать полномочия структурных подразделений.
- 2 Для выбранного предприятия составить примерный перечень потерь при несоблюдении режима коммерческой тайны

**Критерии оценки**

Показатель оценки	Распределение баллов
Выполнены пункты 1	6
Выполнены пункты 1-2	10
Максимальный балл	10

**Модуль 4**  
Типовое практическое задание 4  
Экономическая эффективность коммерческой тайны предприятия

**Вопросы**

1. Для выбранного предприятия попытаться произвести оценку рисков информационной безопасности
2. Для выбранного предприятия попытаться вычислить экономическую эффективность защиты сведений, составляющих коммерческую тайну

**Критерии оценки**

Показатель оценки	Распределение баллов
Выполнены пункты 1	6
Выполнены пункты 1-2	10
Максимальный балл	10

Перечень вопросов для зачета:

1. Федеральный закон «О коммерческой тайне».
2. Сущность понятия «режим коммерческой тайны», «информация, составляющая коммерческую тайну»
3. Сведения, которые не могут составлять коммерческую тайну.
4. Виды ответственности за разглашение коммерческой тайны.
5. Привлечение к ответственности действующего или бывшего сотрудника за разглашение сведений, составляющих коммерческую тайну.
6. Порядок оформления документов по введению режима коммерческой тайны.
7. Правила и ограничения предоставления сведений, составляющих коммерческую тайну сотрудникам государственных органов.
8. Цели установления режима коммерческой тайны.
9. Задачи по установлению режима коммерческой тайны.
10. Полномочия структурных подразделений.
11. Потери организации при несоблюдении режима коммерческой тайны.
12. Источники информации ограниченного доступа на предприятии.

13. Комплекс требуемых мер по защите коммерческой тайны.
14. Аудит текущего состояния защиты информации на предприятии.
15. Введение режима коммерческой тайны.
16. Определение перечня информации, составляющей коммерческую тайну.
17. Положение о коммерческой тайне.

### **Экзаменационные билеты<sup>1</sup>**

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

Перечень вопросов для экзамена:

1. Сущность понятия «режим коммерческой тайны», «информация, составляющая коммерческую тайну»
2. Сведения, которые не могут составлять коммерческую тайну.
3. Виды ответственности за разглашение коммерческой тайны.
4. Привлечение к ответственности действующего или бывшего сотрудника за разглашение сведений, составляющих коммерческую тайну.
5. Порядок оформления документов по введению режима коммерческой тайны.
6. Правила и ограничения предоставления сведений, составляющих коммерческую тайну сотрудникам государственных органов.
7. Цели установления режима коммерческой тайны.
8. Задачи по установлению режима коммерческой тайны.
9. Правомочия структурных подразделений.
10. Потери организации при несоблюдении режима коммерческой тайны.
11. Источники информации ограниченного доступа на предприятии.
12. Комплекс требуемых мер по защите коммерческой тайны.
13. Аудит текущего состояния защиты информации на предприятии.
14. Введение режима коммерческой тайны.
15. Определение перечня информации, составляющей коммерческую тайну.
16. Положение о коммерческой тайне.
17. Регулирование отношений с сотрудниками.
18. Регулирование отношений с контрагентами.
19. Ограничение доступа к информации.
20. Контроль доступа к информации
21. Перечень организационных документов, необходимых для введения режима коммерческой тайны.
22. Существующие уязвимости современных технических средств сбора, обработки и передачи информации.
23. Возможные сценарии использования программных и аппаратных средств съема информации
24. Оценка рисков информационной безопасности предприятия.
25. Экономическая эффективность защиты сведений, составляющих коммерческую тайну.

Образец экзаменационного билета:

...

**МИНОБРНАУКИ РОССИИ**  
**ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

---

<sup>1</sup>Если итоговой формой контроля является зачет, то приводится перечень вопросов и критерии оценки для зачета (с учетом наличия/отсутствия модульно–рейтинговой системы оценок).

Направление 10.03.01 ИБ

Дисциплина: Информационная безопасность организации

**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2**

1. Сведения, которые не могут составлять коммерческую тайну.
2. Регулирование отношений с контрагентами.

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.

**План лекционных занятий (6 семестр)**

(16 часов)

**Лекция №1**

**Основные понятия по коммерческой тайне (2 часа)**

- 1.1 Федеральный закон «О коммерческой тайне».
- 1.2 Сущность понятия «режим коммерческой тайны», «информация, составляющая коммерческую тайну»

**Лекция №2**

**Документирование режима коммерческой тайны (2 часа)**

- 2.1 Сведения, которые не могут составлять коммерческую тайну. сведений, составляющих коммерческую тайну.
- 2.2 Порядок оформления документов по введению режима коммерческой тайны. отношений

**Лекция №3**

**Ответственность за разглашение коммерческой тайны (2 часа)**

3.1 Виды ответственности за разглашение коммерческой тайны.

3.2 Привлечение к ответственности действующего или бывшего сотрудника за разглашение коммерческой тайны

#### **Лекция №4**

##### **Регулирование отношений с госорганами (2 часа)**

4.1 Предоставление сведений, составляющих коммерческую тайну сотрудникам государственных органов

4.2 Правила и ограничения предоставления сведений, составляющих коммерческую тайну сотрудникам государственных органов.

#### **Лекция №5**

##### **Основы установления режима коммерческой тайны (2 часа)**

5.1 Цели установления режима коммерческой тайны.

5.2 Задачи по установлению режима коммерческой тайны.

#### **Лекция №6**

##### **Режим коммерческой тайны (2 часа)**

6.1 Правомочия структурных подразделений.

6.2 Потери организации при несоблюдении режима коммерческой тайны

#### **Лекция №7**

##### **Меры по защите коммерческой тайны (2 часа)**

7.1 Источники информации ограниченного доступа на предприятии.

7.2 Комплекс требуемых мер по защите коммерческой тайны

#### **Лекция №8**

##### **Оценка состояния защиты информации на предприятии (2 часа)**

8.1 Аудит текущего состояния защиты информации на предприятии.

8.2 Введение режима коммерческой тайны.

#### **План лекционных занятий (7 семестр)**

(18 часов)

#### **Лекция №9**

##### **Основные документы предприятия по коммерческой тайне (2 часа)**

9.1 Перечень информации, составляющей коммерческую тайну.

9.2 Положение о коммерческой тайне

#### **Лекция № 10**

##### **Регулирование отношений (2 часа)**

10.1 Регулирование отношений с сотрудниками

10.2 Регулирование отношений с контрагентами

#### **Лекция № 11**

##### **Организационные документы по коммерческой тайне (2 часа)**

11.1 Ограничение и контроль доступа к информации.

11.2 Перечень организационных документов, необходимых для введения режима коммерческой тайны.

#### **Лекция № 12**

##### **Каналы утечки информации и методы несанкционированного доступа к**

### **конфиденциальной информации**

12.1 Существующие уязвимости современных технических средств сбора, обработки и передачи информации.

12.2 Возможные сценарии использования программных и аппаратных средств съема информации.

### **Лекция № 13**

#### **Программно-технические меры защиты информации (2 часа)**

13.1 Технические меры защиты информации в режиме коммерческой тайны

13.2 Программно-аппаратные меры защиты информации в режиме коммерческой тайны

### **Лекция № 14**

#### **Экономическая эффективность коммерческой тайны (2 часа)**

14.1 Оценка рисков информационной безопасности предприятия

14.2 Экономическая эффективность защиты сведений, составляющих коммерческую тайну

### **Лекция № 15**

#### **Пример системы технической защиты коммерческой тайны на предприятии (2 часа)**

15.1 Общие положения

15.2 Назначение, цели и состав ИС

15.3 Описание СЗ «ИС ОРИОН»

### **Лекция № 16**

#### **Обеспечение безопасности ИС «ОРИОН» (2 часа)**

16.1 Решения, реализованные по обеспечению безопасности информации

16.2 Классификация информационной системы

16.3 Меры по обеспечению безопасности ИС «ОРИОН»

### **Лекция № 17**

#### **ИС «ОРИОН» (2 часа)**

17.1 Требования, предъявляемые к ИС «ОРИОН»

17.2 Решения по созданию и вводу в действие системы защиты

### **Планы семинарских занятий (6 семестр)**

(32 часа)

#### **Семинар №1**

##### **Основные понятия по коммерческой тайне (4 часа)**

1.1 Федеральный закон «О коммерческой тайне».

1.2 Сущность понятия «режим коммерческой тайны», «информация, составляющая коммерческую тайну»

#### **Семинар №2**

##### **Документирование режима коммерческой тайны (4 часа)**

2.1 Сведения, которые не могут составлять коммерческую тайну.

сведений, составляющих коммерческую тайну.

2.2 Порядок оформления документов по введению режима коммерческой тайны. отношений

### **Семинар №3**

#### **Ответственность за разглашение коммерческой тайны (4 часа)**

- 3.1 Виды ответственности за разглашение коммерческой тайны.
- 3.2 Привлечение к ответственности действующего или бывшего сотрудника за разглашение коммерческой тайны

### **Семинар №4**

#### **Регулирование отношений с госорганами (4 часа)**

- 4.1 Предоставление сведений, составляющих коммерческую тайну сотрудникам государственных органов
- 4.2 Правила и ограничения предоставления сведений, составляющих коммерческую тайну сотрудникам государственных органов.

### **Семинар №5**

#### **Основы установления режима коммерческой тайны (4 часа)**

- 5.1 Цели установления режима коммерческой тайны.
- 5.2 Задачи по установлению режима коммерческой тайны.

### **Семинар №6**

#### **Режим коммерческой тайны (4 часа)**

- 6.1 Правомочия структурных подразделений.
- 6.2 Потери организации при несоблюдении режима коммерческой тайны

### **Семинар №7**

#### **Меры по защите коммерческой тайны (4 часа)**

- 7.1 Источники информации ограниченного доступа на предприятии.
- 7.2 Комплекс требуемых мер по защите коммерческой тайны

### **Семинар №8**

#### **Оценка состояния защиты информации на предприятии (4 часа)**

- 8.1 Аудит текущего состояния защиты информации на предприятии.
- 8.2 Введение режима коммерческой тайны.

### **План семинарских занятий (7 семестр)**

(36 часов)

### **Семинар №9**

#### **Основные документы предприятия по коммерческой тайне (4 часа)**

- 9.1 Перечень информации, составляющей коммерческую тайну.
- 9.2 Положение о коммерческой тайне

### **Семинар № 10**

#### **Регулирование отношений (2 часа)**

- 10.1 Регулирование отношений с сотрудниками
- 10.2 Регулирование отношений с контрагентами

### **Семинар № 11**

#### **Организационные документы по коммерческой тайне (4 часа)**

- 11.1 Ограничение и контроль доступа к информации.
- 11.2 Перечень организационных документов, необходимых для введения режима коммерческой тайны.

## Семинар № 12

### Каналы утечки информации и методы несанкционированного доступа к конфиденциальной информации (4 часа)

12.1 Существующие уязвимости современных технических средств сбора, обработки и передачи информации.

12.2 Возможные сценарии использования программных и аппаратных средств съема информации.

## Семинар № 13

### Программно-технические меры защиты информации (4 часа)

13.1 Технические меры защиты информации в режиме коммерческой тайны

13.2 Программно-аппаратные меры защиты информации в режиме коммерческой тайны

## Семинар № 14

### Экономическая эффективность коммерческой тайны (4 часа)

14.1 Оценка рисков информационной безопасности предприятия

14.2 Экономическая эффективность защиты сведений, составляющих коммерческую тайну

## Семинар № 15

### Пример системы технической защиты коммерческой тайны на предприятии (4 часа)

15.1 Общие положения

15.2 Назначение, цели и состав ИС

15.3 Описание СЗ «ИС ОРИОН»

## Семинар № 16

### Обеспечение безопасности ИС «ОРИОН» (4 часа)

16.1 Решения, реализованные по обеспечению безопасности информации

16.2 Классификация информационной системы

16.3 Меры по обеспечению безопасности ИС «ОРИОН»

## Семинар № 17

### ИС «ОРИОН» (4 часа)

17.1 Требования, предъявляемые к ИС «ОРИОН»

17.2 Решения по созданию и вводу в действие системы защиты

**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. Дашков, Л.П. Организация и управление коммерческой деятельностью : учебник / Л.П. Дашков, О.В. Памбухчианц. - 2-е изд., перераб. - Москва : Издательско-торговая корпорация «Дашков и К<sup>о</sup>», 2018. - 400 с. : ил. - (Учебные издания для бакалавров). - ISBN 978-5-394-02531-0 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=495757>
2. 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>
3. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 170 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253577>
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. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рыгов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>
6. Лукаш, Ю.А. Контроль персонала как составляющая безопасности и развития бизнеса : учебное пособие / Ю.А. Лукаш. - 2-е изд., стер. - Москва : Издательство «Флинта», 2017. - 24 с. - ISBN 978-5-9765-1377-8 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=115078>

#### Дополнительная литература

7. Мирсанова, О.А. К ВОПРОСУ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАТРАТ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ [Электронный ресурс] // Интеллект. Инновации. Инвестиции. — Электрон. дан. — 2015. — № 3. — С. 36-44. — Режим доступа: <https://e.lanbook.com/journal/issue/300521>. — Загл. с экрана.
8. Бойченко, О.В. ПРОБЛЕМАТИКА КОМПЛЕКСНОЙ ОЦЕНКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ [Электронный ресурс] / О.В. Бойченко, Б.В. Белименко. // Ученые записки Крымского федерального университета им. В.И. Вернадского. Экономика и управление. — Электрон. дан. — 2015. — № 1. — С. 27-31. — Режим доступа: <https://e.lanbook.com/journal/issue/299849>. — Загл. с экрана.
9. ЛЯН, М. ПРАВОВАЯ ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ В КИТАЕ. [Электронный ресурс] — Электрон. дан. // Вестник Бурятского государственного университета. — 2014. — № 2. — С. 283-285. — Режим доступа: <http://e.lanbook.com/journal/issue/292818> — Загл. с экрана.
10. Инструментальный контроль и защита информации : учебное пособие / Н.А. Свиначев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ;

#### 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/catalog/>
5. [www.fstec.ru](http://www.fstec.ru) – сайт ФСТЭК России
6. [www.fsb.ru](http://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](http://www.newlibrary.ru) – Новая электронная библиотека;
10. [www.edu.ru](http://www.edu.ru) – Федеральный портал российского образования;
11. [www.elibrary.ru](http://www.elibrary.ru) – Научная электронная библиотека;
12. [www.nehudlit.ru](http://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	
<p><b>1. учебная аудитория для проведения занятий лекционного типа:</b></p> <p>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).</p>	<p>Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация</p>	<p align="center"><b>Аудитория № 403</b></p> <p>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p align="center"><b>Аудитория № 405</b></p> <p>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 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-</p>	<p>1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p>

<p><b>2. учебная аудитория для проведения лабораторных работ:</b> Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус).</p> <p><b>3. учебная аудитория для проведения занятий семинарского типа:</b> 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><b>4. учебная аудитория для проведения групповых и индивидуальных консультаций:</b> 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><b>5. учебная аудитория для текущего контроля и промежуточной</b></p>		<p>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><b>Аудитория № 413</b> Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p><b>Аудитория № 415</b> 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><b>Аудитория № 416</b> Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 418</b> 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><b>Аудитория № 419</b> Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 515</b> Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 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 SMPRO 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 секционные последующих рядов с пюпитром.</p> <p><b>Аудитория № 516</b> Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p><b>Аудитория № 509</b> Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 608</b></p>	<p>3. Система централизованно о тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.</p>
---	--	--	--

<p><b>аттестации:</b> 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><b>6. помещения для самостоятельной работы:</b> читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p><b>7.помещение для хранения и профилактики учебного оборудования:</b> аудитория № 523 (гуманитарный корпус).</p>		<p>Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 609</b> Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 610</b> 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><b>Аудитория № 613</b> Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p><b>Компьютерный класс аудитория № 420</b> Учебная мебель, моноблоки стационарные 15 шт.</p> <p><b>Компьютерный класс аудитория № 404</b> Учебная мебель, компьютеры -15 штук.</p> <p><b>Аудитория 402 читальный зал библиотеки</b> Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p><b>Лаборатория полигон технической защиты информации № 508</b> 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 провер-кам и специальным обследованиям Калейдоскоп-II2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".</p> <p><b>Аудитория № 523</b> 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 (6 семестр)

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	48,2
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)	23,8
Учебных часов на подготовку к зачету	

Форма контроля:  
Зачет 6 семестр

Содержание рабочей программы  
дисциплины (7 семестр)

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	57,2
лекций	18
практических/ семинарских	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	3,2
Учебных часов на самостоятельную работу обучающихся (СР)	23,8
Учебных часов на подготовку к экзамену	27

Форма контроля:  
Экзамен 7 семестр

## 6 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	<b>Основные понятия по коммерческой тайне</b> 1.1 Федеральный закон «О коммерческой тайне». 1.2 Сущность понятия «режим коммерческой тайны», «информация, составляющая коммерческую тайну»	2	4		3	Изучить историю информационного оружия	Письменная контрольная работа Практическое задание
2	<b>Документирование режима коммерческой тайны</b> 2.1 Сведения, которые не могут составлять коммерческую тайну. 2.2 Порядок оформления документов по введению режима коммерческой тайны.	2	4		3	Изучить историю информационных войн	Письменная контрольная работа Практическое задание
3	<b>Ответственность за разглашение коммерческой тайны</b> 1.1 Виды ответственности за разглашение коммерческой тайны <b>1.2</b> Привлечение к ответственности действующего или бывшего сотрудника за разглашение коммерческой тайны	2	4		3	Изучить историю информационных войн и оружия	Письменная контрольная работа Практическое задание
4	<b>Регулирование отношений с госорганами</b> 4.1 Предоставление сведений, составляющих коммерческую тайну сотрудникам государственных органов 4.2 Правила и ограничения предоставления сведений, составляющих коммерческую тайну сотрудникам государственных	2	4		3	Изучить современное состояние информационных войн	Письменная контрольная работа Практическое задание

	органов.						
5	<b>Основы установления режима коммерческой тайны</b> 5.1 Цели установления режима коммерческой тайны. 5.2 Задачи по установлению режима коммерческой тайны.	2	4		3	Изучить рекомендованную литературу по дисциплине	Письменная контрольная работа Практическое задание
6	<b>Режим коммерческой тайны</b> 6.1 Правомочия структурных подразделений. 6.2 Потери организации при несоблюдении режима коммерческой тайны	2	4		3	Изучить рекомендованную литературу по угрозам ИБ	Письменная контрольная работа Практическое задание
7	<b>Меры по защите коммерческой тайны</b> 7.1 Источники информации ограниченного доступа на предприятии. 7.2 Комплекс требуемых мер по защите коммерческой тайны	2	4		3	Для выбранной организации схематично построить модель безопасности ИТ	Письменная контрольная работа Практическое задание
8	<b>Оценка состояния защиты информации на предприятии</b> 8.1 Аудит текущего состояния защиты информации на предприятии. 8.2 Введение режима коммерческой тайны.	2			2,8	Для выбранной организации схематично построить модель безопасности ИТ организации	Письменная контрольная работа Практическое задание
	Итого	16	32		23,8		

7 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	<b>Основные документы предприятия по коммерческой</b>	2	4		2	Какая информация в организации подлежит защите?	Письменная контрольная работа

	<b>тайне</b> 9.1 Перечень информации, составляющей коммерческую тайну. 9.2 Положение о коммерческой тайне						Практическое задание
10	<b>Регулирование отношений</b> 10.1 Регулирование отношений с сотрудниками 10.2 Регулирование отношений с контрагентами	2	4		2	Для чего нужны различные классификации?	Письменная контрольная работа Практическое задание
11	<b>Организационные документы по коммерческой тайне</b> 11.1 Ограничение и контроль доступа к информации. 11.2 Перечень организационных документов, необходимых для введения режима коммерческой тайны.	2	4		2	Изучить угрозы безопасности организации	Письменная контрольная работа Практическое задание
12	<b>Каналы утечки информации и методы несанкционированного доступа к конфиденциальной информации</b> 12.1 Существующие уязвимости современных технических средств сбора, обработки и передачи информации. 12.2 Возможные сценарии использования программных и аппаратных средств съема информации.	2	4		2	Изучить литературу по коммерческой тайне организации	Письменная контрольная работа Практическое задание
13	<b>Программно-технические меры защиты информации</b> 13.1 Технические меры защиты информации в режиме коммерческой тайны 13.2 Программно-аппаратные меры защиты информации в режиме коммерческой тайны	2	4		2	Изучить особенности разработки режима коммерческой тайны организации	Письменная контрольная работа Практическое задание
14	<b>Экономическая эффективность коммерческой тайны</b>	2	4		2	Изучить особенности классификации защищаемой	Письменная контрольная работа

	14.1 Оценка рисков информационной безопасности предприятия 14.2 Экономическая эффективность защиты сведений, составляющих коммерческую тайну					информации	Практическое задание
15	<b>Пример системы технической защиты коммерческой тайны на предприятии</b> 15.1 Общие положения 15.2 Назначение, цели и состав ИС 15.3 Описание СЗ «ИС ОРИОН»	2	4		3	Изучить особенности классификации защищаемой информации	Письменная контрольная работа Практическое задание
16	<b>Обеспечение безопасности ИС «ОРИОН»</b> 16.1 Решения, реализованные по обеспечению безопасности информации 16.2 Классификация информационной системы 16.3 Меры по обеспечению безопасности ИС «ОРИОН»	2	4		4	Построить классификацию защищаемой информации для выбранной организации	Письменная контрольная работа Практическое задание
17	<b>ИС «ОРИОН»</b> 17.1 Требования, предъявляемые к ИС «ОРИОН» 17.2 Решения по созданию и вводу в действие системы защиты	2	4		4,8	Построить классификацию защищаемой информации для выбранной организации	Письменная контрольная работа Практическое задание
	Итого	18	36		23,8		

