


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

Актуализировано:  
на заседании кафедры  
протокол от «07» июня 2018 г. № 10  
Зав. кафедрой *И.С.* /А.С. Исмагилова

Согласовано:  
Председатель УМК института  
 /Р.А. Гильмутдинова

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Коммерческая тайна на предприятии  
ФТД.В.02 факультатив

программа бакалавриата

Направление подготовки  
10.03.01 Информационная безопасность

Профиль подготовки  
Организация и технология защиты информации

Квалификация  
бакалавр

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



/И.А. Шагапов

Для приема: 2017 г.

Уфа 2018 г.

Составитель: доцент И.А. Шагапов

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью  
Протокол № 10 от «07» июня 2018 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 планируемыми результатами освоения образовательной программы .....	4
2. Цель и место дисциплины в структуре образовательной программы .....	6
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся).....	6
4. Фонд оценочных средств по дисциплине .....	6
4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания .....	6
4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций.....	9
4.3. Рейтинг-план дисциплины.....	11
5. Учебно-методическое и информационное обеспечение дисциплины .....	14
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины .....	14
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины .....	15
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине .....	15

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	
	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Знать понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
Умения	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Уметь использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-	

	безопасности	аппаратных и технических средств защиты информации	
Владения (навыки / опыт деятельности)	Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	
	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	

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

Дисциплина «Коммерческая тайна на предприятии» относится к факультативным дисциплинам по выбору.

Дисциплина изучается на 3 курсе в 5 семестре.

Цели освоения дисциплины (модуля): дать студентам глубокие знания вопросов организации режима коммерческой тайны организации, меры ответственности за нарушение режима, экономическую целесообразность введения режима коммерческой тайны.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Документоведение», «Аппаратные средства защиты информации», «Организационное и правовое обеспечение информационной безопасности».

Полученные знания, навыки и умения используются при прохождении преддипломной практики и в ходе выполнения выпускной квалификационной работы.

## 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 с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности

Этап освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Фрагментарные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Сформированные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности
Второй этап (уровень)	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых	Фрагментарное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых	Сформированное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной

	актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	деятельности, и использовать их в своей деятельности
Третий этап (уровень)	Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Фрагментарное владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Успешное и систематическое владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности

ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	Фрагментарно знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	Уверенно знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа
Второй этап (уровень)	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Не показывает сформированные умения использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Уверенно использует базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность
Третий этап (уровень)	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать	Не владеет основными навыками определения видов и форм информации, подверженной угрозам, анализировать угрозы	Уверенно владеет методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам

	угрозы информационно-вычислительным системам	информационно-вычислительным системам	
--	--	---------------------------------------	--

ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования, политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Фрагментарно знает основные правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования.	Уверенно знает основные правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования.
Второй этап (уровень)	Уметь: подключать охранные и пожарные датчики к приемно-контрольным панелям с разным числом датчиков в шлейфе; настраивать системы видеонаблюдения с	Не показывает сформированные умения подключения, настройки и конфигурирования технических средств охраны	Уверенно использует методы подключения, настройки и конфигурирования технических средств охраны.



	<p>точки зрения угла обзора камер, реакции на события в поле зрения камер, расписания работы; создавать конфигурацию системы контроля и ограничения доступа в центральном компьютере системы; создавать списки пользователей системы с определенными ограничениями по времени доступа и прохода в разные помещения, реализовывать на практике принципы политики безопасности</p>		
Третий этап (уровень)	<p>Владеть: монтажом и настройкой технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации; профессиональной терминологией, навыками анализа, обработки и интерпретации результатов решения прикладных задач управления;</p>	<p>Не владеет основными методами монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации; профессиональной терминологией</p>	<p>Уверенно владеет основными методами монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации; профессиональной терминологией</p>

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины, для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10.  
Шкала оценивания для зачета:  
зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),  
не зачтено – от 0 до 59 рейтинговых баллов).

#### **4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы**

**формирования компетенций в процессе освоения образовательной программы.  
Методические материалы, определяющие процедуры оценивания знаний, умений,  
навыков и опыта деятельности, характеризующих этапы формирования компетенций**

<b>Этапы освоения</b>	<b>Результаты обучения</b>	<b>Компетенция</b>	<b>Оценочные средства</b>
1 этап Знания	Знать основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	Практическое задание, Письменная контрольная работа
	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Практическое задание, Письменная контрольная работа
	Знать понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Практическое задание, Письменная контрольная работа
2 этап Умения	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	Практическое задание, Письменная контрольная работа
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Практическое задание, Письменная контрольная работа
	Уметь использовать методы количественного представления информации и основные закономерности ее	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и	Практическое задание, Письменная

	преобразования в каналах при выполнении комплекса мер по информационной безопасности	эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	контрольная работа
3 этап Владения	Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	Практическое задание, Письменная контрольная работа
	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Практическое задание, Письменная контрольная работа
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Практическое задание, Письменная контрольная работа

### 4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

#### Типовые вопросы 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. Правомочия 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.
18. Регулирование отношений с сотрудниками.
19. Регулирование отношений с контрагентами.
20. Ограничение доступа к информации.
21. Контроль доступа к информации
22. Перечень организационных документов, необходимых для введения режима коммерческой тайны.
23. Существующие уязвимости современных технических средств сбора, обработки и передачи информации.
24. Возможные сценарии использования программных и аппаратных средств съема информации
25. Оценка рисков информационной безопасности предприятия.
26. Экономическая эффективность защиты сведений, составляющих коммерческую тайну.

Критерии оценки (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

### **Комплект контрольных работ**

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

#### Модуль 1.

### НОРМАТИВНАЯ БАЗА ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ

#### 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.

### МЕРЫ ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ

#### 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

#### Комплект практических заданий

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

##### Модуль 1.

#### НОРМАТИВНАЯ БАЗА ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ

##### Типовое практическое задание 1

##### Общие вопросы режима коммерческой тайны

**Задание** 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.

#### МЕРЫ ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ

##### Типовое практическое задание 2

##### Положение о коммерческой тайне

**Задание** 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

### 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. Памбухчиянц. - 2-е изд., перераб. - Москва : Издательско-торговая корпорация «Дашков и К°», 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. 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>
3. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 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>

##### Дополнительная литература

4. Шагапов, И.А. Защита коммерческой тайны на предприятии [Электронный ресурс]: учебное пособие / И.А. Шагапов; Башкирский государственный университет. — Уфа: РИЦ БашГУ, 2018. — Электрон. версия печ. публикации. — Доступ возможен через Электронную библиотеку БашГУ. — <URL:[https://elib.bashedu.ru/dl/corp/Shagapov\\_Zazchita\\_komm\\_tajny\\_na\\_predpriyatii\\_up\\_2018.pdf](https://elib.bashedu.ru/dl/corp/Shagapov_Zazchita_komm_tajny_na_predpriyatii_up_2018.pdf)>.
5. 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>
6. Плашенков, В. Обеспечение безопасности бизнеса промышленных предприятий: теория и практика : учебное пособие / В. Плашенков ; науч. ред. А.Н. Зуев ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «ЧЕРЕПОВЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Институт информационных технологий. - Череповец : Издательство ЧГУ, 2014. - 331 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-85341-634-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=434840>

## 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

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](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> – Открытый образовательный видеопортал UniverTV.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	
<b>1. учебная аудитория для проведения занятий лекционного типа:</b> 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),	Лекции, практические занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	<b>Аудитория № 403</b>	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от
		Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.	
		<b>Аудитория № 405</b>	
		Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387	
		RPOMOUNTTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDR3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. ,	

<p>аудитория № 516 (гуманитарный корпус).</p> <p><b>2. учебная аудитория для проведения занятий семинарского типа:</b></p> <p>аудитория № 403 (гуманитарный корпус),</p> <p>аудитория № 415 (гуманитарный корпус),</p> <p>аудитория № 416 (гуманитарный корпус),</p> <p>аудитория № 418 (гуманитарный корпус),</p> <p>аудитория № 419 (гуманитарный корпус),</p> <p>аудитория № 509 (гуманитарный корпус),</p> <p>аудитория № 608 (гуманитарный корпус),</p> <p>аудитория № 609 (гуманитарный корпус),</p> <p>аудитория № 610 (гуманитарный корпус).</p> <p><b>3. 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>4. учебная аудитория для текущего контроля и промежуточной аттестации:</b> аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус),</p>		<p>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><b>Аудитория № 413</b></p> <p>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></p> <p>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></p> <p>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 418</b></p> <p>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></p> <p>Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 515</b></p> <p>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 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 секционные последующих рядов с попитром.</p> <p><b>Аудитория № 516</b></p> <p>Учебная мебель, доска, кресла секционные последующих рядов с попитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p><b>Аудитория № 509</b></p> <p>Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 608</b></p>	<p>12.11.2014 г.</p> <p>Лицензии бессрочные.</p> <p>3. Система централизованно о тестирования БашГУ (Moodle).GNU General Public License..</p>
--	--	---	---



<p>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. помещения для самостоятельной работы:</b> читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p><b>6. помещение для хранения и профилактического обслуживания 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>Аудитория № 523</b> Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
---	--	--	--

## Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы дисциплины  
Коммерческая тайна на предприятии  
на 5 семестр - ОФО

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

Форма контроля  
Зачет 5 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнитель ная литература, рекомендуе мая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС			
1	2	4	5	6	7	8	9	10
1	<b>РАЗДЕЛ I. НОРМАТИВНАЯ БАЗА ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ</b> Федеральный закон «О коммерческой тайне». Сущность понятия «режим коммерческой тайны», «информация, составляющая коммерческую тайну» Сведения, которые не могут составлять коммерческую тайну. сведений, составляющих коммерческую тайну. Порядок оформления документов по введению режима коммерческой тайны.	2	2		5	1-3	Составить перечень основных вопросов, которые должны обсуждаться перед введением режима КТ	Практическое задание, Письменная контрольная работа
2	Виды ответственности	2	2		5	1-5	Расписать виды	Практическое

	за разглашение коммерческой тайны. Привлечение к ответственности действующего или бывшего сотрудника за разглашение						ответственности за разглашение коммерческой тайны для условного предприятия	задание, Письменная контрольная работа
3	Правила и ограничения предоставления сведений, составляющих коммерческую тайну сотрудникам государственных органов.	2	2		5	1-4	Составить перечень информации, составляющей коммерческую тайну условного предприятия	Практическое задание, Письменная контрольная работа
4	<b>РАЗДЕЛ II. ОСНОВЫ УСТАНОВЛЕНИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ</b> Цели установления режима коммерческой тайны. Задачи по установлению режима коммерческой тайны.	2	2		5	1-5	Расписать конкретные задачи по установлению режима коммерческой тайны для условного предприятия	Практическое задание, Письменная контрольная работа
5	Правомочия структурных подразделений. Потери организации при несоблюдении режима коммерческой	2	2		5	1-5	Оценить потери при несоблюдении режима коммерческой тайны для условного предприятия	Практическое задание, Письменная контрольная работа

	тайны.							
6	<b>РАЗДЕЛ III. МЕРЫ ПО ЗАЩИТЕ КОММЕРЧ ЕСКОЙ ТАЙНЫ</b> Источники информации ограниченного доступа на предприятии. Комплекс требуемых мер по защите коммерческой тайны. Аудит текущего состояния защиты информации на предприятии. Введение режима коммерческой тайны. Определение перечня информации, составляющей коммерческую тайну. Регулирование отношений с сотрудниками и контрагентами. Ограничение и контроль доступа к информации.	2	2		5	1-6	Попытаться провести «виртуальный» аудит для условного предприятия	Практическое задание, Письменная контрольная работа
7	Перечень организационных документов,	2	2		5	1-5	Разработать положение по коммерческой тайне	Практическое задание, Письменная

	необходимых для введения режима коммерческой тайны. Существующие уязвимости современных технических средств сбора, обработки и передачи информации. Возможные сценарии использования программных и аппаратных средств съема информации.						для условного предприятия	контрольная работа
8	<b>РАЗДЕЛ IV. ОЦЕНКИ РИСКОВ И РАСЧЕТ ЭКОНОМИЧЕСКОЙ ЦЕЛЕСООБРАЗНОС ТИ ВВЕДЕНИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ</b> Оценка рисков информационной безопасности предприятия. Экономическая эффективность защиты сведений, составляющих коммерческую тайну	2	2		4,8	1-6	Оценить экономическую эффективность введения режима коммерческой тайны	Практическое задание, Письменная контрольная работа
	<b>Всего</b>	16	16		39,8			

Приложение 2  
Рейтинг – план дисциплины

Коммерческая тайна на предприятии  
Направление подготовки 10.03.01 Информационная безопасность  
Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль 1. НОРМАТИВНАЯ БАЗА ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ</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. МЕРЫ ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ</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				