

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 *А.С.* /А.С. Исмаилова

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

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Проверка информационной защищенности на  
соответствие нормативным документам  
Б1.В.1.ДВ.03.02

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: 2015 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 .....	7
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся).....	7
4. Фонд оценочных средств по дисциплине .....	7
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 .....	7
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.....	13
4.3. Рейтинг-план дисциплины.....	16
5. Учебно-методическое и информационное обеспечение дисциплины .....	21
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины .....	21
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины .....	22
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине .....	22

**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 правовые основы организации защиты государственной тайны и конфиденциальной информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	
	Знать критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	

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 разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	Уметь выполнять все виды работ (прием, передачу, хранение, размножение и т.п.) по конфиденциальному делопроизводству	ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	
	Уметь применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	
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	ОПК-7. Способность	

	<p>видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам</p>	<p>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</p>	
	<p>Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации</p>	<p>ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации</p>	
	<p>Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации</p>	<p>ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.</p>	
	<p><u>Владеть</u> Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов</p>	<p>ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.</p>	

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

Дисциплина «Проверка информационной защищенности на соответствие нормативным документам» относится к вариативным дисциплинам по выбору.

Дисциплина изучается на 3 курсе в 5 семестре.

Целью освоения дисциплины «Проверка информационной защищенности на соответствие нормативным документам» является усвоение теоретических знаний и практического опыта в области информационной безопасности на уровне государства и организации, овладение компетенциями по проверке информационной защищенности на соответствие нормативным документам.

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

Полученные знания, навыки и умения используются при прохождении производственной и преддипломной практик 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 (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основы российской правовой системы и законодательства, методы и средства правовой защиты интересов	Фрагментарные представления об основах российской правовой системы и законодательства, методы и средства	Неполные представления об основах российской правовой системы и законодательства, методы и средства правовой	Сформированные, но содержащие отдельные неточности об основах российской правовой системы и законодательства	Сформированные представления об основах российской правовой системы и законодательства, методы и средства

	субъектов в сфере информационной безопасности	правовой защиты интересов субъектов в сфере информационной безопасности	защиты интересов субъектов в сфере информационной безопасности	ства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	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 актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Фрагментарное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	В целом успешное, но не систематическое умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	В целом успешное, но содержащее отдельные пробелы предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Сформированное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной 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	В целом успешное, но не систематическое владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы владения 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 компетенци и	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворите льно»)	3 («Удовлетвор ительно»)	4 («Хорошо»)	5 («Отлично»)
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	В целом знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	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	Умеет использовать некоторые приемы использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Уверенно использует большинство приемов 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,	Не владеет основными навыками определения видов и форм информации, подверженной угрозам,	Владеет основными навыками определения видов и форм информации, подверженной угрозам,	Владеет основными навыками определения видов и форм информации, подверженной угрозам,	Уверенно владеет методикой определения видов и форм информации, подверженной угрозам,

	анализировать угрозы информационно-вычислительным системам	анализировать угрозы информационно-вычислительным системам	анализировать угрозы информационно-вычислительным системам, но допускает ошибки	анализировать угрозы информационно-вычислительным системам	анализировать угрозы информационно-вычислительным системам
--	--	--	---	--	--

ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации	Фрагментарно знает правовые основы организации защиты государственной тайны и конфиденциальной информации	В целом знает правовые основы организации защиты государственной тайны и конфиденциальной информации	Знает правовые основы организации защиты государственной тайны и конфиденциальной информации	Уверенно знает правовые основы организации защиты государственной тайны и конфиденциальной информации
Второй этап (уровень)	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	Не показывает сформированные умения разрабатывать организационно-распорядительные документы по вопросам защиты информации	Умеет использовать некоторые методы разработки организационно-распорядительные документы по вопросам защиты информации	Уверенно использует большинство методов разработки организационно-распорядительные документы по вопросам защиты информации	Уверенно умеет разрабатывать организационно-распорядительные документы по вопросам защиты информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет основными навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации	Владеет основными навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации	Владеет навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации	Уверенно владеет навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации

		информации	информации, но допускает значительные ошибки.		информации
--	--	------------	---	--	------------

ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Фрагментарно знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	В целом знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Уверенно знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области
Второй этап (уровень)	Уметь выполнять все виды работ (прием, передачу, хранение, размножение и т.п.) по конфиденциальному	Не показывает сформированные умения выполнять все виды работ (прием, передачу, хранение, размножение и т.п.) по	Умеет использовать некоторые приемы выполнять все виды работ (прием, передачу, хранение, размножение	Уверенно использует большинство приемов выполнять все виды работ (прием, передачу, хранение, размножение	Уверенно умеет выполнять все виды работ (прием, передачу, хранение, размножение и т.п.) по конфиденциальному

	делопроизводству	конфиденциальному делу производству	и т.п.) по конфиденциальному делу производству	и т.п.) по конфиденциальному делу производству	ьному делу производству
Третий этап (уровень)	Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации	Не владеет основными навыками сбора и анализа исходных данных для проектирования систем защиты информации	Владеет основными методами сбора и анализа исходных данных для проектирования систем защиты информации, но допускает ошибки	Владеет основными методами сбора и анализа исходных данных для проектирования систем защиты информации	Уверенно владеет методами сбора и анализа исходных данных для проектирования систем защиты информации

ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	<u>Знать</u> критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Фрагментарно знает критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	В целом знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Уверенно знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов
Второй этап (уровень)	<u>Уметь</u> применять отечественные стандарты в области компьютерной безопасности	Не показывает сформированные умения отечественные стандарты в области компьютерной безопасности	Умеет использовать некоторые приемы отечественные стандарты в области компьютерной безопасности	Уверенно использует большинство отечественных стандартов в области компьютерной безопасности	Уверенно умеет применять отечественные стандарты в области компьютерной безопасности

	для проектирования, разработки и оценки защищенности компьютерных систем	безопасности для проектирования, разработки и оценки защищенности компьютерных систем	й безопасности для проектирования, разработки и оценки защищенности компьютерных систем	й безопасности для проектирования, разработки и оценки защищенности компьютерных систем	безопасности для проектирования, разработки и оценки защищенности компьютерных систем
Третий этап (уровень)	<u>Владеть</u> методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	Не владеет основными методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	Владеет основными методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	Владеет основными методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	Уверенно владеет методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов

Критериями оценивания 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).

Шкалы оценивания:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

**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**

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
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	Лабораторная работа, Письменная контрольная работа
	Знать средства контроля	ОПК-7. Способность	Лабораторная

	контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	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	работа, Письменная контрольная работа
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Лабораторная работа, Письменная контрольная работа
	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	Лабораторная работа, Письменная контрольная работа
	Знать критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	Лабораторная работа, 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	Лабораторная работа, Письменная контрольная работа
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе	Лабораторная работа, Письменная контрольная работа

	информационную безопасность	анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Лабораторная работа, Письменная контрольная работа
	Уметь выполнять все виды работ (прием, передачу, хранение, размножение и т.п.) по конфиденциальному делопроизводству	ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	Лабораторная работа, Письменная контрольная работа
	Уметь применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	Лабораторная работа, Письменная 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	Лабораторная работа, 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	Лабораторная работа, Письменная контрольная работа
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности	Лабораторная работа, Письменная контрольная работа

		информации	
	Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации	ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	Лабораторная работа, Письменная контрольная работа
	Владеть Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов	ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	Лабораторная работа, Письменная контрольная работа

### 4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

#### Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов

Типовые экзаменационные материалы

#### Вопросы к экзамену

1. Международная нормативно-правовая база в области обеспечения информационной безопасности
2. Национальная нормативная база РФ в области информационной безопасности
3. Общие сведения о стандартизации, сертификации и метрологии
4. Организационные основы защиты информации
5. Законодательство РФ в области информационной безопасности
6. Правовые основы защиты информации, коммерческой и государственной тайны.
7. Изучение положений о государственном лицензировании деятельности в области защиты информации
8. Анализ сертификата соответствия
9. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации
10. Система сертификации средств криптографической защиты информации
11. Допуск и доступ персонала к защищаемым сведениям
12. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.
13. Основы работы с персоналом предприятия.
14. Основные этапы работы с персоналом.
15. Методы работы с персоналом и их характеристика.
16. Мотивация деятельности персонала.
17. Организация допуска и доступа персонала к конфиденциальной информации
18. Разрешительная система допуска и доступа к конфиденциальной информации.
19. Основные положения допуска должностных лиц и граждан к государственной тайне.
20. Порядок оформления и переоформления допуска к государственной тайне.



21. Формы допуска.
22. Основания для отказа лицу в допуске к государственной тайне и условия прекращения допуска.
23. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям.
24. Порядок доступа к конфиденциальной информации командированных лиц
25. Изучение основных принципов допускной работы.
26. Составление перечня внутренних организационно-распорядительных документов по защите информации на объекте.
27. Порядок назначения комиссии для аттестации помещений на пригодность их для ведения закрытых работ.
28. Определение состава информации, используемой в ходе совещания или переговоров

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Институт истории и государственного управления

---

Направление подготовки  
10.03.01 Информационная безопасность

**Проверка информационной защищенности на  
соответствие нормативным документам**

**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1**

1. *Международная нормативно-правовая база в области обеспечения информационной безопасности*

2. *Методы работы с персоналом и их характеристика.*

Зав. кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

---

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Институт истории и государственного управления

---

Направление подготовки  
10.03.01 Информационная безопасность

**Проверка информационной защищенности на  
соответствие нормативным документам**

**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2**

1. *Национальная нормативная база РФ в области информационной безопасности*

2. *Мотивация деятельности персонала.*

Зав. кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

---

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

· отлично - от 80 до 110 баллов (включая 10 поощрительных баллов);

- хорошо - от 60 до 79 баллов;
- удовлетворительно - от 45 до 59 баллов;
- неудовлетворительно - менее 45 баллов.

#### Критерии оценивания ответа на экзамене

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

**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

**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.

**1-10 баллов** выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов.. Студент не смог ответить ни на один дополнительный вопрос.

#### Комплект контрольных работ

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

##### Модуль 1.

Основы правовой защиты информации  
Письменная контрольная работа №1  
Введение режима коммерческой тайны

##### Вопросы

1. Указы Президента РФ, постановления Правительства РФ об информационной безопасности;
2. Международная нормативно-правовая база в области обеспечения информационной безопасности.
3. Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной безопасности

##### Критерии оценки

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

##### Модуль 2.

Допуск и доступ персонала к защищаемым сведениям  
Письменная контрольная работа №2  
Общие вопросы допуска персонала к защищаемым сведениям  
**Вопросы**

1. Закон о «О техническом регулировании»
2. Сертификация в области защиты информации (обязательная и добровольная).
3. Закон о «О лицензировании отдельных видов деятельности»
4. Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.

#### Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-4	15
Максимальный балл	15

### Комплект лабораторных работ

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

#### Модуль 1.

#### Основы правовой защиты информации

#### Типовая лабораторная работа 1

#### Правовые вопросы оформления допуска персонала к защищаемым сведениям

Для предприятия, выбранного согласно вашему варианту, составить список нормативных правовых актов и стандартов, которыми необходимо руководствоваться при построении комплексной системы защиты информации предприятия. К каждому документу представить комментарий, указывающий обязательный или рекомендательный характер документа, основное содержание документа, область применения документа для рассматриваемого вами предприятия.

Варианты:

1. железнодорожная станция;
6. школа;
7. библиотека;
8. юридическая фирма;
9. фирма по разработке программного обеспечения

#### Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 50%	8
Выполнены пункты 100%	14
Максимальный балл	14

#### Модуль 2.

#### Допуск и доступ персонала к защищаемым сведениям

#### Типовая лабораторная работа 2

#### Оформление допуска персонала к защищаемым сведениям

Для предприятия, выбранного согласно вашему варианту, составить список нормативных правовых актов и стандартов, которыми необходимо руководствоваться при построении

комплексной системы защиты информации предприятия. К каждому документу представить комментарий, указывающий обязательный или рекомендательный характер документа, основное содержание документа, область применения документа для рассматриваемого вами предприятия.

Варианты:

1. факультет университета;
2. филиал банка;
3. небольшое торговое предприятие;
4. поликлиника;
5. больница.

#### Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 50%	8
Выполнены пункты 100%	14
Максимальный балл	14

### 5. Учебно-методическое и информационное обеспечение дисциплины

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

а) основная учебная литература:

1. 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>
2. Организация безопасной работы информационных систем : учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ГГТУ», 2014. - 132 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=277794>

б) дополнительная литература

3. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю.И. Коваленко. - Москва : Горячая линия - Телеком, 2012. - 140 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0261-9 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253538>
4. 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>
5. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: <https://e.lanbook.com/book/97352>. — Загл. с экрана.

6. Петренко, С.А. Аудит безопасности Intranet [Электронный ресурс] : учебное пособие / С.А. Петренко, А.А. Петренко. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 386 с. — Режим доступа: <https://e.lanbook.com/book/1113>. — Загл. с экрана.

## 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/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> – 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)	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточна	<b>Аудитория № 403</b> 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	
		RPOMOUNTEST -1 шт., Ком-ер	
		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	

<p>(гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</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</p>	<p>я аттестация</p>	<p>встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей, ActivPanel 21S – 1 шт., Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт., Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт., Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.</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 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> Учебная мебель, доска, кресла секционные последующих рядов с</p>	<p>бессрочные.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованно о тестирования БашГУ (Moodle).GNU General Public License.</p>
---	---------------------	--	---

<p>аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p><b>5. 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), 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 профилактического обслуживания учебного оборудования:</b> аудитория № 523 (гуманитарный корпус).</p>		<p>попитром, 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 № 510</b> Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 608</b> 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 USBBLACK – 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-П2, 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>	
---	--	---	--



## Приложение 1

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

Содержание рабочей программы дисциплины

Проверка информационной защищенности на соответствие нормативным документам  
на 5 семестр - ОФО

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	73,2
лекций	18
практических / семинарских	36
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу	45
Учебных часов на подготовку к экзамену	25,8

Форма контроля:  
Экзамен 7 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая 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	Международная нормативно-правовая база в области обеспечения информационной безопасности Национальная нормативная база РФ в области информационной безопасности Общие сведения о стандартизации, сертификации и метрологии Организационные основы защиты информации Законодательство РФ в области информационной безопасности	2	4	-	4	1-4	Выбрать условную организацию для разработки документов службы делопроизводства (управление делами, отдел документационного обеспечения, канцелярия, секретариат, общий отдел, секретарь- референт).	Лабораторная работа, Письменная контрольная работа
2	Правовые основы защиты информации,	2	4	4	4	1-4	Разработать типовую	Лабораторная работа,

	<p>коммерческой и государственной тайны. Изучение положений о государственном лицензировании деятельности в области защиты информации</p>						<p>структуру службы делопроизводства условной организации (управление делами, отдел документационного обеспечения, канцелярия, секретариат, общий отдел, секретарь-референт).</p>	<p>Письменная контрольная работа</p>
3	<p>Анализ сертификата соответствия Изучение положений о сертификации средств защиты информации по требованиям безопасности информации</p>	2	4	-	5	1-4	<p>Оценить эффективность типовой структуры службы делопроизводства условной организации (управление делами, отдел документационного обеспечения, канцелярия, секретариат, общий отдел, секретарь-референт).</p>	<p>Лабораторная работа, Письменная контрольная работа</p>
4	<p>Система сертификации</p>	2	4	4	4	1-5	<p>Разработать</p>	<p>Лабораторная</p>

	средств криптографической защиты информации Допуск и доступ персонала к защищаемым сведениям						Положение о службе делопроизводства	работа, Письменная контрольная работа
5	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации.	2	4	-	5	1-5	Определить должностной состав службы делопроизводства условной организации.	Лабораторная работа, Письменная контрольная работа
6	Основы работы с персоналом предприятия. Основные этапы работы с персоналом. Методы работы с персоналом и их характеристика. Мотивация деятельности персонала. Организация допуска и доступа персонала к конфиденциальной информации Разрешительная система допуска и доступа к	2	4	4	5	1-6	Разработать должностные инструкции сотрудников службы делопроизводства условной организации.	Лабораторная работа, Письменная контрольная работа

	конфиденциальной информации.								
7	Основные положения допуска должностных лиц и граждан к государственной тайне. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска. Основания для отказа лицу в допуске к государственной тайне и условия прекращения допуска.	2	4	-	6	1-6	Изучить рекомендованную литературу	Лабораторная работа, Письменная контрольная работа	
8	Организация доступа персонала предприятия к сведениям, составляющим государственную тайну, и их носителям. Порядок доступа к конфиденциальной информации командированных лиц Изучение основных принципов допускной работы.	2	4	4	6	1-6	Изучить рекомендованную литературу	Лабораторная работа, Письменная контрольная работа	

	Составление перечня внутренних организационно-распорядительных документов по защите информации на объекте.							
9	Порядок назначения комиссии для аттестации помещений на пригодность их для ведения закрытых работ. Определение состава информации, используемой в ходе совещания или переговоров	2	4	2	6	1-6	Рассчитать количественный состав сотрудников службы делопроизводства условной организации.	Лабораторная работа, Письменная контрольная работа
	итого	18	36	18	45			

Приложение 2

**Рейтинг – план дисциплины**

Проверка информационной защищенности на соответствие нормативным документам

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. Основы правовой защиты информации</b>				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Лабораторная работа №1	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №1	15	1	0	15
Всего				35
<b>Модуль 2. Допуск и доступ персонала к защищаемым сведениям</b>				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Лабораторная работа №2	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №2	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			0	30