СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Утверждено
На заседании кафедры
Протокол № 1 от 29.08.2018
Зав. кафедрой

Мустафина С.А.

Рабочая программа дисциплины (модуля)

дисциплина ***Информационная безопасность в профессиональной деятельности***

Блок Б1, базовая часть, Б1.Б.30
Цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Специальность

38.05.01 ***Экономическая безопасность***
код наименование направления или специальности

Специализация №1

Экономико-правовое обеспечение экономической безопасности

Разработчик (составитель)
к.ф-м.н., доцент Викторов С.В.
к.ф-м.н., доцент Каримов Р.Х.
Ученая степень, ученое звание, ФИО — подпись — 29.08.2018г. дата

Стерлитамак 2018

Оглавление

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими виду (видам) профессиональной деятельности, на который (которые) ориентирована программа:

1. *способностью выполнять должностные обязанности по обеспечению законности и правопорядка, охране общественного порядка (ПК-7)*
2. *способностью осуществлять мероприятия, направленные на профилактику, предупреждение преступлений и иных правонарушений, на основе использования закономерностей экономической преступности и методов ее предупреждения; выявлять и устранять причины и условия, способствующие совершению преступлений, в том числе коррупционных проявлений (ПК-10)*
3. *способностью осуществлять производство по делам об административных правонарушениях (ПК-14)*
4. *способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)*
5. *способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)*

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (компетенции)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью выполнять должностные обязанности по обеспечению законности и правопорядка, охране общественного порядка (ПК-7)	1 этап: Знания	Обучающийся должен знать: - содержание понятий «обеспечение информационной безопасности», «правовой режим информационной безопасности» и «организационный режим информационной безопасности»; - предметную область правового и организационного режимов информационной безопасности; - политические причины возникновения информационного противоборства; затрагиваемые им сферы общественной жизни;
	2 этап: Умения	Обучающийся должен уметь определять основные направления установления правового режима информационной безопасности;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками определения функциональной направленности режимов обеспечения информационной безопасности, а также выявления и анализа направлений установления правового режима информационной безопасности личности, организации, государства.
способностью осуществлять мероприятия, направленные на профилактику, предупреждение преступлений и иных правонарушений, на	1 этап: Знания	Обучающийся должен знать: - основные объекты обеспечения информационной безопасности в сфере создания и функционирования общегосударственных информационно- телекоммуникационных систем; - основные цели применения профилей стандартов при

основе использования закономерностей экономической преступности и методов ее предупреждения; выявлять и устранять причины и условия, способствующие совершению преступлений, в том числе коррупционных проявлений (ПК-10)		создании и организации функционирования информационно-телекоммуникационных систем;
	2 этап: Умения	Обучающийся должен уметь: - определять содержание документов политик информационной безопасности организации (компании) в соответствии с основными положениями национальных стандартов в области управления информационной безопасностью автоматизированных систем в защищенном исполнении;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: - методикой проведения анализа нормативно- деятельности) правовых актов, регулирующих отношения в области обеспечения информационной безопасности в сети Интернет.
Способностью осуществлять производство по делам об административных правонарушениях (ПК-14)	1 этап: Знания	Обучающийся должен знать: - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;
	2 этап: Умения	Обучающийся должен уметь: выявлять обстоятельства, способствующие совершению правонарушений, планировать и осуществлять деятельность по предупреждению и профилактике административных правонарушений и фиксировать их в информационных системах
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками анализа правоприменительной и правоохранительной административной практики.
способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)	1 этап: Знания	Обучающийся должен знать: - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;
	2 этап: Умения	Обучающийся должен уметь: выявлять обстоятельства, способствующие совершению правонарушений, планировать и осуществлять деятельность по предупреждению и профилактике административных правонарушений и фиксировать их в информационных системах
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками анализа правоприменительной и правоохранительной административной практики.
способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)	1 этап: Знания	Обучающийся должен знать: - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;
	2 этап: Умения	Обучающийся должен уметь: выявлять обстоятельства, способствующие совершению правонарушений, планировать и осуществлять деятельность по предупреждению и профилактике административных правонарушений и фиксировать их в информационных системах
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками анализа правоприменительной и правоохранительной административной практики.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках *базовой* части.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Экономическая информатика и Административное право.

Дисциплина изучается на 3 курсе в 5 и 6 семестрах по заочной форме обучения.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единиц (з.е.), 144 академических часов.

Объем дисциплины	**Всего часов**
	Заочная форма обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	17.2
лекций	6
практических	10
лабораторных	
формы контактной работы (ФКР)	1.2
Учебных часов на самостоятельную работу обучающихся (СРС)	120.2
Учебных часов на контроль:	
экзамен	6.6

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

Заочная форма

№ п/п	**Наименовж-з ание раздела /темы дисциплины**	**Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)**				
		Контактная работа с преподавателем				**СРС**
		Лек	**Сем/ Пр**	**Лаб**		
1.	**Понятие, организация и основы обеспечения информационной безопасности**					
1.1.	Правовые основы защиты государственной и служебной тайны; персональных данных	1	1			20
1.2.	Система организационно-правового обеспечения информационной безопасности.	1	2			20
2.	**Правовое обеспечение информационной безопасности**					

2.1.	Правовая основа информационной безопасности	1	1			20.2
2.2.	Принципы защиты информации.	1	2			20
2.3	Правовая защита обладателей информации.	1	2			20
2.4	Содержание организационного обеспечения информационной безопасности.	1	2			20
	Итого	**6**	**10**			**120.2**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Лекционный курс

№	Наименование раздела /темы дисциплины	Содержание
1	**Понятие, организация и основы обеспечения информационной безопасности в правоохранительной сфере**	
1.1.	Правовые основы защиты государственной и служебной тайны; персональных данных	Информационное обеспечение государственной политики Российской Федерации. Сведения, составляющих государственную тайну. Законность отнесения сведений к государственной тайне. Система защиты государственной тайны. Сведения «особой важности». Сведения «совершенно секретные». Сведения «секретные». Основания для рассекречивания сведений. Допуск должностных лиц и граждан РФ к государственной тайне. Служебную тайна, ее режим. Конфиденциальная информация. Владелец и пользователь информационных ресурсов, информационных систем, технологий и средств их обеспечения.
1.2.	Система организационно-правового обеспечения информационной безопасности.	Международно-правовые акты и международные стандарты в области информационной безопасности. Международные стандарты по информационной безопасности. Информационное законодательство как основной источник правового регулирования информационной безопасности. Особенности ведомственного и корпоративного нормативного регулирования обеспечения информационной безопасности. Сущность ведомственного правового акта и его государственная регистрация. Действующие нормативные правовые акты в системе обеспечения информационной безопасности и защиты информации. Формирование корпоративных требований и спецификаций информационной безопасности. Сущность, роль и место политики информационной безопасности в деятельности современного предприятия. Структура корпоративной политики информационной безопасности. Исходные данные для формирования политики информационной безопасности предприятия и уровни документирования ее требований.
2	**Правовое обеспечение информационной безопасности**	
2.1.	Правовая основа информационной безопасности	Требования к законодательству в области информационной безопасности. Правовая основа обеспечения информационной безопасности в России. Регламентирование вопросов защиты информации в ведомственных нормативных актах. Ответственность за нарушение требований защиты информации
2.2.	Принципы защиты информации.	Принципы защиты информации : общая характеристика. Принцип обоснованности доступа. Обязательное выполнение 2-х основных условий: пользователь должен иметь достаточную "форму допуска" для получения информации требуемого им уровня конфиденциальности, и эта информация необходима ему для выполнения его производственных функций.

2.3.	Правовая защита обладателей информации.	Три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический. Фундаментальные требования, которые используются для обработки конфиденциальной информации. Похищение документов, содержащих защищаемые сведения. Незаконное получение конфиденциальной информации.
2.4.	Содержание организационного обеспечения информационной безопасности.	Принцип достаточной глубины контроля доступа. Принцип разграничения потоков информации. Принцип чистоты повторно используемых ресурсов. Принцип персональной ответственности. Принцип целостности средств защиты

Курс практических (семинарский) занятий

№	Наименование раздела /темы дисциплины	Содержание
1	**Понятие, организация и основы обеспечения информационной безопасности в правоохранительной сфере**	
1.1.	Правовые основы защиты государственной и служебной тайны; персональных данных	Понятие и защита государственной и коммерческой тайны в системе защиты информации. Действующие нормативные правовые акты, нормативно-методические и методические документы в системе защиты государственной и коммерческой тайны. Принципы защиты. Отнесение сведений к коммерческой, служебной и профессиональной тайнам. Перечень сведений, составляющих государственную тайну. Сведения, которые не могут составлять государственную и коммерческую тайну. Степени и грифы секретности. Засекречивание и рассекречивание. Основания и порядок доступа к конфиденциальной информации. Государственное лицензирование деятельности, связанное с защитой информации.
1.2.	Система организационно-правового обеспечения информационной безопасности.	Система защиты информации. Структурная и функциональная часть защиты информации. Государственная система организационно-правового обеспечения информационной безопасности. Основные категории и функции органов защиты информации. Основные формы организации работ по защите информации в правоохранительной сфере.
2	Правовое обеспечение информационной безопасности	
2.1.	Правовая основа информационной безопасности	Правовая основа обеспечения информационной безопасности в России. Регламентирование вопросов защиты информации в ведомственных нормативных актах. Правовое регулирование информационной безопасности в правоохранительной сфере. Понятие коммерческой тайны. Ответственность и ее виды за нарушение требований к защите информации.
2.2.	Принципы защиты информации.	Понятие защиты информации. Мероприятия по защите информации: правовые меры; организационные мероприятия; Правовые принципы защиты информации: принцип собственности на информацию; принцип экономической целесообразности. Организационные принципы защиты информации в правоохранительной сфере: принцип системного подхода к организации защиты информации; принцип максимального ограничения числа лиц, допускаемых к защищаемой информации; принцип персональной ответственности за

		сохранность доверенных секретов; принцип непрерывности.
2.3.	Правовая защита обладателей информации.	Информация как результат интеллектуальной деятельности, объект права собственности и правовых отношений. Интеллектуальная собственность и ее защита. Сущность, содержание, объект, виды и право интеллектуальной собственности. Институты, образующие систему правовой охраны интеллектуальной собственности. Объекты институтов права интеллектуальной собственности. Государственная регистрация интеллектуальной собственности. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Способы защиты интеллектуальных прав. Защита личных неимущественных прав и исключительных прав. Ответственность юридических лиц и индивидуальных предпринимателей за нарушения исключительных прав. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ. Программы для ЭВМ и базы данных, созданные по заказу и при выполнении работ по договору. Технические средства защиты авторских прав.
2.4.	Содержание организационного обеспечения информационной безопасности.	Политика безопасности. Требования действующих международных стандартов по вопросам менеджмента информационной безопасности Принципы организационного обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности. Функции органов управления и подразделения защиты информации в системе обеспечения информационной безопасности. Роль внешних контролирующих органов в системе обеспечения информационной безопасности. Возможности специализированных организаций по формированию требований к информационной безопасности корпорации и контролю эффективности их выполнения. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Обязанности администрации по созданию надлежащих условий персоналу для работы с конфиденциальной информацией.

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Перечень вопросов для самостоятельного изучения

1. Назначение и структура правового обеспечения информационной безопасности
2. Основы правового регулирования отношений в информационной сфере
3. Основные законодательные акты и правовые нормы в сфере обеспечения информационной безопасности
4. Правовые основы защиты тайны и персональных данных
5. История и современные направления развития информационной безопасности
6. Система организационно-правового обеспечения информационной безопасности
7. Правовая основа информационной безопасности
8. Источники угроз защищаемой информации
9. Общая характеристика способов незаконного получения защищаемой информации
10. Принципы защиты информации
11. Правовая защита обладателей информации

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1. Перечень компетенций с указанием этапов их формирования и описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.

Планируемые результаты освоения образовательной программы	**Этап**	**Показатели и критерии оценивания результатов обучения**				**Вид оценочного средства**
1.	2.	3.				
		неуд.	удовл.	хорошо	отлично	
Способностью выполнять должностные обязанности по обеспечению законности и правопорядка, охране общественного порядка (ПК-7)	1 этап: Знания	Не знает - содержание понятий «обеспечение информационной безопасности», «правовой режим информационной безопасности» и «организационный режим информационной безопасности»; - предметную область правового и организационного режимов информационной безопасности; - политические причины возникновения информационного противоборства; затрагиваемые им сферы общественной жизни;	Не в полной мере знает - содержание понятий «обеспечение информационной безопасности», «правовой режим информационной безопасности» и «организационный режим информационной безопасности»; - предметную область правового и организационного режимов информационной безопасности; - политические причины возникновения информационного противоборства; затрагиваемые им сферы общественной жизни;	Достаточно знает - содержание понятий «обеспечение информационной безопасности», «правовой режим информационно й безопасности» и «организационный режим информационной безопасности»; - предметную область правового и организационного режимов информационной безопасности; - политические причины возникновения информационного противоборства; затрагиваемые им сферы общественной	В полном объеме знает - содержание понятий «обеспечение информационной безопасности», «правовой режим информационной безопасности» и «организационный режим информационной безопасности»; - предметную область правового и организационного режимов информационной безопасности; - политические причины возникновения информационного противоборства; затрагиваемые им сферы общественной	контрольные вопросы

				жизни;	жизни;	
	2 этап: Умения	Не умеет - определять основные направления установления правового режима информационно й безопасности;	Недостаточно умеет - определять основные направления установления правового режима информационной безопасности;	В целом умеет - определять основные направления установления правового режима информационной безопасности;	В полном объеме умеет определять основные направления установления правового режима информационной безопасности;	тестирование
	3 этап: Владения (навыки / опыт деятельности)	Не владеет - навыками определения функциональной направленности режимов обеспечения информационной безопасности, а также выявления и анализа направлений установления правового режима информационной безопасности личности, организации, государства.	С трудом владеет - навыками определения функциональной направленности режимов обеспечения информационной безопасности, а также выявления и анализа направлений установления правового режима информационной безопасности личности, организации, государства.	Не в полном объеме владеет - навыками определения функциональной направленности режимов обеспечения информационной безопасности, а также выявления и анализа направлений установления правового режима информационной безопасности личности, организации, государства	В полном объеме владеет - навыками определения функциональной направленности режимов обеспечения информационной безопасности, а также выявления и анализа направлений установления правового режима информационной безопасности личности, организации, государства.	контрольные задания
способностью осуществлять мероприятия, направленные на профилактику, предупреждение преступлений и иных правонарушений, на основе использования закономерностей	1 этап: Знания	Не знает - основные объекты обеспечения информационной безопасности в сфере создания и функционирования общегосударственных информационно-телекоммуникационных систем; - основные	Не в полной мере знает - основные объекты обеспечения информационной безопасности в сфере создания и функционирования общегосударственных информационно-телекоммуникационных	Достаточно знает - основные объекты обеспечения информационной безопасности в сфере создания и функционирования общегосударственных информационно-телекоммуникационных	В полном объеме знает - основные объекты обеспечения информационной безопасности в сфере создания и функционирования общегосударственных информационно-телекоммуникационных	контрольные вопросы

экономической преступности и методов ее предупреждения; выявлять и устранять причины и условия, способствующие совершению преступлений, в том числе коррупционных проявлений (ПК-10)		цели применения профилей стандартов при создании и организации функционирования информационно-телекоммуникационных систем;	систем; - основные цели применения профилей стандартов при создании и организации функционирования информационно-телекоммуникационных систем;	систем; - основные цели применения профилей стандартов при создании и организации функционирования информационно-телекоммуникационных систем;	систем; - основные цели применения профилей стандартов при создании и организации функционирования информационно-телекоммуникационных систем;	
	2 этап: Умения	Не умеет - определять содержание документов политик информационной безопасности организации (компании) в соответствии с основными положениями национальных стандартов в области управления информационной безопасностью автоматизированных систем в защищенном исполнении;	Недостаточно умеет - определять содержание документов политик информационной безопасности организации (компании) в соответствии с основными положениями национальных стандартов в области управления информационной безопасностью автоматизированных систем в защищенном исполнении;	В целом умеет - определять содержание документов политик информационной безопасности организации (компании) в соответствии с основными положениями национальных стандартов в области управления информационной безопасностью автоматизированных систем в защищенном исполнении;	В полном объеме умеет - определять содержание документов политик информационной безопасности организации (компании) в соответствии с основными положениями национальных стандартов в области управления информационной безопасностью автоматизированных систем в защищенном исполнении;	тестирование
	3 этап: Владения (навыки / опыт деятельности)	Не владеет - методикой проведения анализа нормативно- правовых актов, регулирующих отношения в области обеспечения информационно й безопасности в сети Интернет.	С трудом владеет - методикой проведения анализа нормативно-правовых актов, регулирующих отношения в области обеспечения информационной безопасности в сети Интернет.	Не в полном объеме владеет - методикой проведения анализа нормативно- правовых актов, регулирующих отношения в области обеспечения информационной безопасности в сети Интернет.	В полном объеме владеет - методикой проведения анализа нормативно- правовых актов, регулирующих отношения в области обеспечения информационной безопасности в сети Интернет.	контрольные задания

Способностью осуществлять производство по делам об административных правонарушениях (ПК-14)	1 этап: Знания	Не знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационно й безопасности Российской Федерации;	Не в полной мере знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	Достаточно знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	В полном объеме знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	контрольные вопросы
	2 этап: Умения	Не умеет определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов;	Недостаточно умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов	В целом умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационно й безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов;	умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов;	Тестовые задания
	3 этап: Владения (навыки / опыт деятельности)	Не владеет - методикой выявления проявления угроз информационной безопасности; общественные	Не в полной мере владеет - методикой выявления проявления угроз информационной безопасности;	Достаточно владеет - методикой выявления проявления угроз информационной безопасности;	В полном объеме владеет - методикой выявления проявления угроз информационной безопасности;	контрольные задания

		отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений	общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	
способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)	1 этап: Знания	Не знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	Не в полной мере знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	Достаточно знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	В полном объеме знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	контрольные вопросы
	2 этап: Умения	Не умеет определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности;	Недостаточно умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные	В целом умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационно й безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные	умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения,	Тестовые задания

		общественные отношения, возникающие в связи с деятельностью данных субъектов;	отношения, возникающие в связи с деятельностью данных субъектов	отношения, возникающие в связи с деятельностью данных субъектов;	возникающие в связи с деятельностью данных субъектов;	
	3 этап: Владения (навыки / опыт деятельности)	Не владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	Не в полной мере владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений	Достаточно владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	В полном объеме владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	контрольные задания
способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20)	1 этап: Знания	Не знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	Не в полной мере знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	Достаточно знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	В полном объеме знает - методику определения функциональной направленности режимов обеспечения безопасности; - методику выявления угроз информационной безопасности Российской Федерации;	контрольные вопросы (в том числе по сам. раб.)
	2 этап: Умения	Не умеет определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность	Недостаточно умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную	В целом умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную	умеет - определять объект обеспечения информационной безопасности; субъект информационной безопасности; - определять функциональную направленность	Тестовые задания

		режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов;	направленность режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов	направленность режимов обеспечения информационно й безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов;	режимов обеспечения информационной безопасности человека, организации, государства; - выявлять субъекты проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов;	
	3 этап: Владения (навыки / опыт деятельности)	Не владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	Не в полной мере владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений	Достаточно владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	В полном объеме владеет - методикой выявления проявления угроз информационной безопасности; общественные отношения, возникающие в связи с противоправной деятельностью субъектов информационных отношений.	контрольные задания

6.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Перечень вопросов для оценки уровня сформированности компетенции ПК-7 на этапе «Знания»

1. Назовите современные направления защиты информации
2. Перечислите источники угроз защищаемой информации.
3. Укажите основные объективные и субъективные условия утечки информации

Перечень вопросов для оценки уровня сформированности компетенции ПК-10 на этапе «Знания»

1. Какая ответственность предусмотрена за нарушения оператором требований Федерального закона «О персональных данных»?
2. Как осуществляется сертификация и лицензирование в области защиты информации?
3. Перечислите методы обеспечения информационной безопасности Российской Федерации.

Перечень вопросов для оценки уровня сформированности компетенции ПК-14 на этапе «Знания»

1. Дайте определение информации с правовой точки зрения.
2. Перечислите категории информации по условиям доступа и распространения.
3. Раскройте смысл понятия «информационная безопасность».

Перечень вопросов для оценки уровня сформированности компетенции ОК-12 на этапе «Знания»

1. Охарактеризуйте порядок и правила определения степени секретности сведений
2. Распространяются ли требования Федерального закона «О персональных данных» на юридическое лицо иностранного государства?
3. Понятие информационной безопасности общества.

Перечень вопросов для оценки уровня сформированности компетенции ПК-20 на этапе «Знания»

1. Какими правами обладают граждане РФ в информационной сфере? Опишите механизмы их реализации.
2. Какой орган при осуществлении своей деятельности имеет право подготавливать и представлять в установленном порядке Президенту и в Правительство РФ предложения по правовому регулированию вопросов защиты государственной тайны, совершенствованию системы защиты государственной тайны?
3. Понятие безопасности в глобальном информационном пространстве.

Тестовые задания

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-7 на этапе «Умения»

1. Состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства это –

a) защищенность информационных ресурсов;
b) принцип сбалансированности интересов;
c) информационная безопасность.

2.Сведения (сообщения, данные) независимо от формы их представления:

a) информация;
b) персональные данные;
c) информационные данные.

3. Организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов называется:

a) информатизация;
b) легализация;
c) коммуникация.

4. Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию … :

a) информация на бумажном носителе;
b) документированная информация;
c) конфиденциальная информация.

5. Документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации:

a) несекретная информация;
b) информация, зафиксированная на специальном носителе;
c) конфиденциальная информация:

Перечень тестовых заданий для оценки уровня сформированности компетенции ОК-12 на этапе «Умения»

6. Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем):

a) информационные ресурсы;
b) массив документации, хранящиеся в специальных помещениях;
c) информация, хранящаяся в органах государственной власти.

7. Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства:

a) обеспечение безопасного использования информации;
b) состояние безопасного информационного обмена;
c) информационная безопасность.

8. Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы:

a) информационная система:
b) система документированной информации;
c) система информационных носителей.

9. Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность:
a) банк данных на граждан;
b) информация о гражданах (персональные данные);
c) сведения о гражданах их личной жизни.

10. Субъект, реализующий полномочия владения, пользования и распоряжения информационными объектами в объеме, устанавливаемом собственником:
a) уполномоченное лицо;
b) пользователь;
c) владелец.

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-10 на этапе «Умения»

1. Передаваемое по радио сообщение является:
a) Свободной информацией
b) Связанной информацией
c) Ни свободной ни связанной информацией

2. Право на информацию отнесено Конституцией РФ к разряду:
a) Основных
b) Неосновных
c) Не закреплено в Конституции РФ

3. Впервые предложил и обосновал необходимость создания «Информационного права» как самостоятельной отрасли права:
a) А.Б. Венгеров в 1975 г.
b) С.С. Алексеев в 1981 г.
c) М.М. Рассолов в 1999 г.

4. Информационному праву как отрасли присущ:
a) Императивный метод регулирования
b) Диспозитивный метод регулирования
c) Ни один из вышеперечисленных
d) Оба метода

5. Информационное право является
a) Профилирующей отраслью
b) Специальной отраслью
c) Комплексной отраслью

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-20 на этапе «Умения»

6. К источникам информационного права не относится:

a) Международные договоры РФ
b) Доктрина информационной безопасности РФ
c) Нормотворческие акты органов местного самоуправления

7. Важнейшим документом «большой восьмерки» в сфере формирования информационного общества является:
a) Международный пакт о гражданских и политических правах
b) Хартия глобального информационного общества
c) Конвенция об информационной безопасности

8. Информационные нормы не могут быть:
a) Материальными
b) Охранительными
c) Ни материальными, ни охранительными
d) И материальными, и охранительными

9. В информационно-правовой норме как структурная часть отсутствует:
a) гипотеза
b) Диспозиция
c) Санкция
d) Нет правильного ответа

10. Объектом информационно-правовых отношений является
a) информация
b) информационное законодательство
c) информационные правоприменительные акты
d) нет правильного ответа

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-14 на этапе «Умения»

1. Режим защиты информации не устанавливается в отношении сведений, относящихся к …
a) государственной тайне
b) деятельности государственных деятелей
c) конфиденциальной информации
d) персональным данным
2. В регистрации средства массовой информации не может быть отказано…
a) когда заявление подано не соответствующим лицом
b) по мотивам нецелесообразности
c) даже если сведения в заявлении не соответствуют действительности
d) если регистрирующий орган уже зарегистрировал другое средство массовой информации с тем же названием и формой распространения

3. Засекречиванию подлежат сведения о …
a) состоянии демографии
b) состоянии преступности
c) фактах нарушения прав и свобод человека и гражданина
d) силах и средствах гражданской обороны
4. Проверить электронно-цифровую подпись под документом может…
a) только эксперт, преобразуя электронный образец документа и открытый ключ отправителя

b) любое заинтересованное лицо, преобразуя электронный образец документа, открытый ключ отправителя и собственно значение электронно-цифровой подписи
c) только эксперт с помощью преобразований электронного образца документа, открытого ключа отправителя и собственно значения электронно-цифровой подписи
d) только отправитель электронного документа

5. Режим документированной информации – это …
a) выделенная информация по определенной цели
b) электронный документ с электронно-цифровой подписью
c) выделенная информация в любой знаковой форме
d) электронная информация, позволяющая ее идентифицировать

6. Согласие субъекта персональных данных на их обработку требуется, когда обработка.персональных данных осуществляется …
a) для доставки почтовых отправлений
b) в целях профессиональной деятельности журналиста
c) в целях профессиональной деятельности оператора
d) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно

7. Режим общественного достояния устанавливается для … .
a) любой общедоступной информации
b) сведений, которые являются уникальными, незаменимыми по своей природе
c) любой общественной организации
d) для государственных органов и муниципальных образований

8. Учредителями средства массовой информации могут выступать…
a) граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории российской Федерации
b) только юридические лица
c) граждане, достигшие 16 лет и юридические лица
d) граждане другого государства, постоянно не проживающие в Российской Федерации,
e) юридические лица и органы государственной власти
f) граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти

9. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи.
a) месяца,
b) 2. полгода
c) 1 год,
d) 3 лет

10. С точки зрения информационного права информация – это …
a) сведения о законодательстве, правовых явлениях, правоприменительной деятельности
b) данные о развитии конкретной правовой науки и ее практическом применении
c) сведения независимо от формы их представления
d) форма выражения объективных знаний

Контрольная работа

Перечень контрольных заданий для оценки уровня сформированности компетенции ПК-7 на этапе «Навыки»

Задание 1. В одной из газет появилось сообщение о том, что популярный телеведущий получил ссуду в размере 1 млн 200 тыс. рублей на строительство. Он открыл депозитный счет в одном из отделений коммерческого банка. После публикации данного материала в районный суд поступило исковое заявление от телеведущего к коммерческому банку о возмещении морального вреда и о разглашении коммерческой тайны. Проанализируйте ситуацию с позиции нарушений законодательства. Разберите ситуацию.

Перечень контрольных заданий для оценки уровня сформированности компетенции ОК-12 на этапе «Навыки»

Задание 1. В одной из газет появилось сообщение о том, что популярный телеведущий получил ссуду в размере 1 млн 200 тыс. рублей на строительство. Он открыл депозитный счет в одном из отделений коммерческого банка. После публикации данного материала в районный суд поступило исковое заявление от телеведущего к коммерческому банку о возмещении морального вреда и о разглашении коммерческой тайны. Подлежат ли ответственности банк и газета?

Перечень контрольных заданий для оценки уровня сформированности компетенции ПК-20 на этапе «Навыки»

Задание 1. В одной из газет появилось сообщение о том, что популярный телеведущий получил ссуду в размере 1 млн 200 тыс. рублей на строительство. Он открыл депозитный счет в одном из отделений коммерческого банка. После публикации данного материала в районный суд поступило исковое заявление от телеведущего к коммерческому банку о возмещении морального вреда и о разглашении коммерческой тайны. Был ли нарушен редакцией газеты закон «О средствах массовой информации», а банком ГК РФ – закон «О банках и банковской деятельности»?

Перечень контрольных заданий для оценки уровня сформированности компетенции ПК-10 на этапе «Навыки»

Задание 2. На закрытом химическом предприятии, расположенном в черте города и находящимся в близи от государственной границы, в результате аварии произошел выброс вредных веществ в атмосферу. Городская администрация приняла необходимые меры по эвакуации граждан из зараженных мест и предотвращения утечки нежелательной информации об аварии. При этом она запретила руководству предприятия передавать зарубежным СМИ и специалистам информацию о масштабах, аварии и сведения, касающиеся жизни населенных пунктов, входящих в зону досягаемости распространения вредных веществ. Одновременно администрация приняла решение о нераспространении указанных сведении, ссылаясь на закрытость производства химического предприятия. Правомерны ли действия городской администрации с точки зрения норм информационного права?

Перечень контрольных заданий для оценки уровня сформированности компетенции ПК-14 на этапе «Навыки»

Желая помочь своим коллегам, программист Сальников и адвокат Сабуров - работники нотариальной конторы «ОКС» - внесли изменения в программу «Акты и документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации недвижимости за последний год и нарушена работа ПК. Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова. Есть ли в действиях Сальникова и Сабурова состав преступления?

Перечень вопросов к экзамену

1. Понятие и виды информации. Документированная и недокументированная информация.
2. Предмет информационно-правового регулирования.
3. Информационная норма: понятие, особенности, виды.
4. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации.
5. Система и компетенция органов, обеспечивающих охрану государственной тайны.
6. Компетенция органов государственной власти по обеспечению правового режима конфиденциальной информации.
7. Понятие и виды конфиденциальной информации.
8. Режимы защиты информации.
9. Государственная тайна как предмет, изъятый из гражданского оборота.
10. Служебная и профессиональная тайн
11. Коммерческая и банковская тайны
12. Понятие и структура персональных данных
13. Понятие и виды информационных технологий.
14. Порядок создания информационных технологий.
15. Нарушения порядка применения информационных технологий: информационные войны, несанкционированный мониторинг за активностью потребителя информации
16. Понятие и виды информационных ресурсов.
17. Правовой статус печатных, электронных и телекоммуникационных СМИ.
18. Компетенция органов государственного управления в отношении СМИ.
19. Права граждан в информационной сфере.
20. Право на доступ к информации.
21. Право на защиту персонифицированной информации.
22. Понятие и виды информационно-правовых систем
23. Понятие и виды информационной безопасности.
24. Понятие информационной безопасности личности.
25. Соблюдение конституционных прав и свобод человека и гражданина в области информационных правоотношений.

6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Раздел 1				
Текущий контроль			**0**	**20**
Контрольные вопросы	1	8	0	8
Тестирование	1	5	0	4
Контрольные задания	4	2	0	8
Рубежный контроль			**0**	**15**
Тестирование		1	0	15
Раздел 2				
Текущий контроль			**0**	**20**
Контрольные вопросы (в том числе по сам. раб.)	1	5	0	5
Тестирование	5	2	0	10

Контрольные задания	1	5	0	5
Рубежный контроль			**0**	**15**
Письменная контрольная работа			0	15
Штрафные баллы за пропущенные занятия				
1. Лекционные занятия				**-6**
2. Практические занятия				**-10**
Поощрительные баллы				
Публикация статей	5	1	0	**5**
Участие в конференциях	5	1	0	**5**
Итоговый контроль				
Экзамен				**30**

Объем и уровень сформированности компетенций целиком или на различных этапах у обучающихся оцениваются по результатам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80 - 100%; «удовлетворительно» – выполнено 40 - 80%; «неудовлетворительно» – выполнено 0 - 40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

$$\text{Рейтинговый балл} = k \times \text{Максимальный балл},$$

где $k = 0{,}2$ при уровне освоения «неудовлетворительно», $k = 0{,}4$ при уровне освоения «удовлетворительно», $k = 0{,}8$ при уровне освоения «хорошо» и $k = 1$ при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов БашГУ:

На экзамене выставляется оценка:

- отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- хорошо - при накоплении от 60 до 79 рейтинговых баллов,
- удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
- неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная учебная литература:

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс]: учебное пособие. — Электрон. дан. — М.: ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578. (21.08.2018)

2. Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс]: учебник. — Электрон. дан. — М.: ДМК Пресс, 2012. — 474 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990 (22.08.2018)

Дополнительная учебная литература:

1. Лапина, М.А. Информационное право : учеб. пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / М.А. Лапина, А.Т. Ревин, В.И. Лапин ; под ред. проф. И.Ш. Килясханова. — Москва : ЮНИТИ-ДАНА ; Закон и право, 2017. — 335 с. — (Высшее профессиональное образование: Юриспруденция). - ISBN 978-5-238-00798-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025586 - Текст : электронный. - URL: http://znanium.com/catalog/product/1025586 (21.08.2018)
2. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1 - Режим доступа: http://znanium.com/catalog/product/997105 (21.08.2018)

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), необходимых для освоения дисциплины (модуля)

№	Наименование документа с указанием реквизитов	Срок действия документа
1.	Электронно-библиотечная система ZNANIUM.COM, договор с ООО «ЗНАНИУМ» № 3151эбс от 31.05.2018	До 03.06.2019
2.	Электронно-библиотечная система «Университетская библиотека online», договор с ООО «Нексмедиа» № 847 от 29.08.2017	До 01.10.2018
3.	Электронно-библиотечная система издательства «Лань», договор с ООО «Издательство «Лань» № 838 от 29.08.2017	До 01.10.2018
4.	База данных периодических изданий (на платформе East View EBSCO), договор с ООО «ИВИС» № 133-П 1650 от 03.07.2018	До 30.06.2019
5.	База данных периодических изданий на платформе Научной электронной библиотеки (eLibrary), Договор с ООО «РУНЭБ» № 1256 от 13.12.2017	До 31.12.2018
6.	Электронная база данных диссертаций РГБ, Договор с ФГБУ «РГБ» № 095/04/0220 от 6 дек. 2017 г.	До 07.12.2018
7.	Национальная электронная библиотека, Договор с ФГБУ «РГБ» № 101/НЭБ/1438 от 13 апр. 2016 г.	Бессрочный
8.	Электронно-библиотечная система «ЭБ БашГУ», договор с ООО «Открытые библиотечные системы» № 095 от 01.09.2014	Бессрочный

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Наименование программного обеспечения
Office Standard 2007 Russian OpenLicensePack NoLevel Acdmc
Консультант Плюс Юрист
Система Гарант
Windows 7

8. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид учебных занятий	Организация деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям: «обеспечение информационной безопасности», «правовой режим информационной безопасности», «организационный режим информационной безопасности».
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, изучение рекомендуемой литературы и др. Развитие навыков работы с автоматизированными информационно-справочными и информационно-поисковыми системами; работы с базами данных; навыками определения направлений и видов защиты информации с учетом характера информации и задач по ее защите.
Тест	Проводится на практических занятиях. Позволяет оценить уровень теоретических знаний обучающихся по дисциплине.
Контрольная работа	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Решение типовых задач.
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для текущего контроля и промежуточной аттестации, кабинет исполнения бюджетов бюджетной системы № 30	Учебная мебель, доска, мультимедиа-проектор, экран настенный, учебно-наглядные пособия
учебная аудитория для проведения занятий семинарского типа, кабинет информатики, лаборатория «Учебный банк» № 24	Учебная мебель, доска, персональные компьютеры
Читальный зал, помещение для самостоятельной работы № 4	Учебная мебель, персональные компьютеры, учебно-наглядные пособия
учебная аудитория для групповых и индивидуальных консультаций № 43	Учебная мебель, доска