МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО Руководитель ОПОП О.В. Бесчастнова 07.05.2025	УТВЕРЖДАЮ Заведующий кафедрой ГПДиМП Т.В. Говердовская 07.05.2025

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Составитель	**Имзалиева М.Р., старший преподаватель**
Согласовано с работодателями:	**Крипакова Д.Р. судья, Камызякский районный суд Астраханской области; Яковлев Д.Ю. судья, Кировский районный суд г. Астрахани**
Направление подготовки / специальность	**40.05.04 СУДЕБНАЯ И ПРОКУРОРСКАЯ ДЕЯТЕЛЬНОСТЬ**
Направленность (профиль) ОПОП	**Судебная деятельность**
Квалификация (степень)	**юрист**
Форма обучения	**очная, заочная**
Год приема	**2025**
Курс	**2,6**
Семестры	**4 (по очной форме)/ 11 (по заочной форме)**

Астрахань 2025

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Целями освоения дисциплины (модуля) «Правовое обеспечение информационной безопасности» являются усвоение законодательно-правовых основ правового обеспечения информационной безопасности, принципов построения систем обеспечения информационной безопасности, анализа и оценки угроз информационной безопасности объектов.

1.2 Задачи освоения дисциплины (модуля): «Правовое обеспечение информационной безопасности»:

- изучить понятийный аппарат, основные понятия и категории информационного права и информационного законодательства РФ
- изучить общетеоретические основы правового регулирования в сфере обеспечения национальной безопасности в информационной сфере
- изучить правовой режим секретной и конфиденциальной информации, организацию защиты информации ограниченного доступа при размещении ее в информационной системе
- сформировать у студентов способности самостоятельно работать с различными источниками правовой информации, государственными информационными ресурсами и системами
- выработать навыки правильного толкования и применения норм информационного законодательства РФ

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Учебная дисциплина (модуль) «Правовое обеспечение информационной безопасности» относится к обязательной части и осваивается в 4 и 11 семестрах.

2.2 Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

Правовые базы данных

Информационные технологии в профессиональной деятельности

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

Знания: цели и задачи основных направлений построения информационного общества в Российской Федерации; основные признаки, понятия и цели обеспечения информационной безопасности

Умения: адекватно толковать правовые нормы, посвященные вопросам информационной безопасности; разграничивать функции участников информационных отношений; применять нормы гражданского, административного, уголовного, трудового и других отраслей права для решения конфликтных ситуаций в сфере обеспечения информационной безопасности

Навыки: навыками работы с нормативно-правовыми актами, их анализа, поиска информации по вопросам обеспечения информационной безопасности

2.3 Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

Судебное делопроизводство

3 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) обще профессиональных (ОПК):

ОПК – 5 - Способен профессионально толковать нормы права

ОПК – 9 - Способен получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований

информационной безопасности

Таблица 1 Декомпозиция результатов обучения

Код компетенции	Код и наименование индикатора компетенции[1]	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
Способен профессионально толковать нормы права ОПК-5	ОПК-5.1 Осуществляет толкование правовых актов, в том числе в ситуациях при пробелах и коллизиях правовых норм	виды и способы толкования правовых норм	определять вид и способ толкования норм права, подлежащих применению	навыками толкования права, навыками применения коллизионных правил
Способен получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований информационной безопасности ОПК – 9	ОПК-9.2. Способен анализировать юридически значимую информацию, полученную из различных источников, включая правовые базы данных для решения конкретных задач профессиональной деятельности с учетом требований информационной безопасности	основные принципы обеспечения информационной безопасности, установленные в нормах действующего законодательства.	использовать требования информационной безопасности при осуществлении профессиональной деятельности юриста.	применения методов защиты информации при осуществлении профессиональной деятельности юриста.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 2 зачетные единицы (72 часа).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной и заочной форм обучения приведена в таблице 2.1.

Таблица 2.1 Трудоемкость отдельных видов учебной работы по формам обучения

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения	для заочной формы обучения
Объем дисциплины в зачетных единицах	2		2
Объем дисциплины в академических часах	72		72
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):	26		10
- занятия лекционного типа, в том числе:	18		4
- практическая подготовка (если предусмотрена)			-
- лабораторные занятия			
- практическая подготовка (если предусмотрена)	18		6
- консультация (предэкзаменационная)	-		-
- промежуточная аттестация по дисциплине			-
Самостоятельная работа обучающихся (час.)	36		62
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	Зачет- 4 семестр		Зачет – 11 семестр

Содержание дисциплины, структурированное по темам (разделам) с указанием

[1] Указываются в соответствии с утвержденными в ОПОП ВО

отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено в таблице 2.2.

Таблица 2.2 Структура и содержание дисциплины (модуля)

для очной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации [по семестрам]
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 1 Проблемная сфера информационной безопасности и защиты информации	**3**				**3**			**6**	**12**	Устное собеседование
Тема 2 Основы информационной безопасности в информационной сфере	**3**				**3**			**6**	**12**	Практическая работа
Тема 3 Интересы личности, общества и государства в информационной сфере	**3**				**3**			**6**	**12**	Практическая работа
Тема 4 Законодательство в области информационной безопасности и защиты информации	**3**				**3**			**6**	**12**	Практическая работа
Тема 5 Понятие и виды информации, защищаемой законодательством Российской Федерации	**3**				**3**			**6**	**12**	Практическая работа
Тема 6 Методы обеспечения информационной безопасности	**3**				**3**			**6**	**12**	Практическая работа Итоговое тестирование
Консультации										
Контроль промежуточной аттестации										**зачет**
Итого за весь период	**18**				**18**			**36**	**72**	**зачет**

для заочной формы обучения

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации [по семестрам]
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 1 Проблемная сфера информационной безопасности и защиты информации	**2**							**10**	**12**	Устное собеседование
Тема 2 Основы информационной безопасности в информационной сфере					**2**			**10**	**12**	Практическая работа
Тема 3 Интересы личности, общества и государства в информационной сфере					**2**			**10**	**12**	Практическая работа
Тема 4 Законодательство в области информационной безопасности и защиты информации	**2**							**10**	**12**	Практическая работа
Тема 5 Понятие и виды информации, защищаемой законодательством Российской Федерации								**12**	**12**	Практическая работа

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации [по семестрам]
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
Тема 6 Методы обеспечения информационной безопасности					**2**			**10**	**12**	Практическая работа Итоговое тестирование
Консультации										
Контроль промежуточной аттестации										**зачет**
Итого за семестр	**4**				**6**			**62**	**72**	**зачет**

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3 Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых в них компетенций

Темы, разделы дисциплины	Кол-во часов	Компетенции		Общее количество компетенций
		ОПК 5	*ОПК-9*	
Тема 1 Проблемная сфера информационной безопасности и защиты информации	12	+	+	2
Тема 2 Основы информационной безопасности в информационной сфере	12	+	+	2
Тема 3 Интересы личности, общества и государства в информационной сфере	12	+	+	2
Тема 4 Законодательство в области информационной безопасности и защиты информации	12	+	+	2
Тема 5 Понятие и виды информации, защищаемой законодательством Российской Федерации	12	+	+	2
Тема 6 Методы обеспечения информационной безопасности	12	+	+	2
ИТОГО	**72**			

КРАТКОЕ СОДЕРЖАНИЕ КАЖДОЙ ТЕМЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Тема 1. Проблемная сфера информационной безопасности и защиты информации

Информация и право. Информатика и правовые дисциплины. Информационное право. Виды информации, подлежащей защите. Понятие информации с ограниченным доступом. Соотношение тайн и права на информацию.

Тема 2. Основы информационной безопасности в информационной сфере

Понятие и предмет информационной безопасности. Национальные интересы России в информационной сфере и угрозы информационной безопасности.

Тема 3. Интересы личности, общества и государства в информационной сфере.

Правовое обеспечение информационной безопасности личности. Правовое обеспечение защиты личности и общества от воздействия вредной информации.

Тема 4. Законодательство в области информационной безопасности и защиты информации

Правовое обеспечение информационной безопасности государства. Государственная и служебная тайна в системе обеспечения информационной безопасности государства.

Тема 5. Понятие и виды информации, защищаемой законодательством Российской Федерации.

Коммерческая, банковская и профессиональная тайна в системе обеспечения информационной безопасности. Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности. Правовое регулирование вопросов лицензирования и сертификации в области защиты информации. Юридическая ответственность за нарушение правовых норм в области информационной безопасности.

Тема 6. Методы обеспечения информационной безопасности.

Доктрина информационной безопасности. Правовые, экономические, организационно-технические методы. Разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности. Использование средств защиты информации. Контроль за действием персонала в защищаемых информационных системах.

5 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Указания по организации и проведению лекционных, практических занятий с перечнем учебно-методического обеспечения

При подготовке к лекциям, и практическим занятиям, выполнение самостоятельных работ необходимо воспользоваться системой «Электронное образование»:

https://moodle.asu.edu.ru/

Основу теоретического обучения студентов составляют лекции. Они дают систематизированные знания студентам о наиболее сложных и актуальных проблемах изучаемой дисциплины. На лекциях особое внимание уделяется не только усвоению студентами изучаемых проблем, но и стимулированию их активной познавательной деятельности, творческого мышления, развитию научного мировоззрения, профессионально-значимых свойств и качеств.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Основными видами аудиторной самостоятельной работы являются:

- выполнение практических заданий;
- работа с литературой и другими источниками информации, в том числе электронными;
- решение проблемных и ситуационных задач.

Выполнение практических работ осуществляется на практических занятиях в соответствии с графиком учебного процесса. Для обеспечения самостоятельной работы преподавателями разрабатываются методические указания по выполнению практикума.

Работа с литературой, другими источниками информации, в т.ч. электронными может реализовываться на лекционных занятиях.

Данные источники информации могут быть представлены на бумажном и/или электронном носителях, в том числе, в сети Internet. Преподаватель формулирует цель работы с данным источником информации, определяет время на проработку документа и форму отчетности.

Решение проблемных и ситуационных задач используется на лекционном и других видах занятий. Проблемная/ситуационная задача должна иметь четкую формулировку, к ней должны быть поставлены вопросы, ответы на которые необходимо найти и обосновать. Критерии оценки правильности решения проблемной/ситуационной задачи должны быть известны всем обучающимся

5.2 Указания для обучающихся по освоению дисциплины (модулю)

Самостоятельная работа студентов по дисциплине «Правовое обеспечение информационной безопасности» предполагает выполнение следующих видов деятельности:

1. Выполнение практических заданий в электронном виде, оформленном средствами Microsoft Word и Microsoft PowerPoint и отправка его на платформу портала Цифрового обучения

2. Основными формами самостоятельной (внеаудиторной) работы студентов являются: изучение специальной литературы с более подробным рассмотрением ключевых проблем дисциплины, а также чтение и конспектирование рекомендованной литературы;

Осуществляя учебные действия на занятиях, студенты должны внимательно воспринимать действия преподавателя, запоминать складывающиеся образы, мыслить, добиваться понимания изучаемого предмета, применения знаний на практике, при решении учебно-профессиональных задач. Студенты должны аккуратно вести конспект. В случае недопонимания какой-либо части предмета следует задать вопрос в установленном порядке преподавателю.

Лекционные занятия закладывают основы знаний по предмету в обобщенной форме, а практические занятия направлены на расширение и детализацию этих знаний, на выработку и закрепление навыков профессиональной деятельности. Подготовка к практическим занятиям предполагает предварительную самостоятельную работу студентов в соответствии с методическими разработками по каждой запланированной теме.

Целью самостоятельной работы студентов (СРС) является освоение фундаментальных знаний, развитие ответственности и организованности, умений самостоятельно работать с учебным материалом и приобретение навыков поиска и реферирования доступной научной информации в области информационной безопасности.

Таблица 4 Содержание самостоятельной работы обучающихся

для очной формы обучения

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Тема 1	Проблемная сфера информационной безопасности и защиты информации	6	Устное собеседование
Тема 2	Основы информационной безопасности в информационной сфере	6	Практическая работа
Тема 3	Интересы личности, общества и государства в информационной сфере	6	Практическая работа
Тема 4	Законодательство в области информационной безопасности и защиты информации	6	Практическая работа
Тема 5	Понятие и виды информации, защищаемой законодательством Российской Федерации	6	Практическая работа
Тема 6	Методы обеспечения информационной безопасности	6	Практическая работа Итоговое тестирование

для заочной формы обучения

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Тема 1	Проблемная сфера информационной безопасности и защиты информации	10	Устное собеседование
Тема 2	Основы информационной безопасности в информационной сфере	10	Практическая работа
Тема 3	Интересы личности, общества и государства в информационной сфере	10	Практическая работа
Тема 4	Законодательство в области информационной безопасности и защиты информации	10	Практическая работа
Тема 5	Понятие и виды информации, защищаемой законодательством Российской Федерации	12	Практическая работа
Тема 6	Методы обеспечения информационной безопасности	10	Практическая работа Итоговое тестирование

5.3 Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

Методические рекомендации по проведению практических работ

Выполнение практических работ осуществляется на аудиторных занятиях в соответствии с графиком учебного процесса. Для обеспечения самостоятельной работы преподавателями разрабатываются методические указания по выполнению практической работы.

Критерии оценки практического задания

- оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;
- оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.
- оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;
- оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

6 ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

6.1 Образовательные технологии

В процессе изучения курса «Правовое обеспечение информационной безопасности» большое значение имеет усвоение лекционного курса. Для этого студенты должны посещать лекции и конспектировать лекционный материал. В процессе проведения работы закрепляются основные термины и понятия, студенты могут задавать уточняющие вопросы.

Методика преподавания курса, помимо лекций предполагает:

- проведение практических работ с использованием возможностей ПК с выходом в Интернет.

В соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров в рамках изучения дисциплины «Правовое обеспечение информационной безопасности» предусмотрено использование в учебном процессе в течение одного семестра, следующих форм проведения занятий:

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

для очной формы обучения

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Проблемная сфера информационной безопасности и защиты информации	Обзорная лекция	Не предусмотрено	Устное собеседование
Основы информационной безопасности в информационной сфере	Лекция-диалог	Не предусмотрено	Практическая работа
Интересы личности, общества и государства в информационной сфере	Лекция-диалог	Не предусмотрено	Практическая работа
Законодательство в области информационной безопасности и защиты информации	Лекция-диалог	Не предусмотрено	Практическая работа

Понятие и виды информации, защищаемой законодательством Российской Федерации	Лекция-диалог	Не предусмотрено	Практическая работа
Методы обеспечения информационной безопасности	Лекция-диалог	Не предусмотрено	Практическая работа

для заочной формы обучения

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Проблемная сфера информационной безопасности и защиты информации	Лекция-диалог но	Не предусмотрено	Не предусмотрено
Основы информационной безопасности в информационной сфере	Не предусмотрено	Не предусмотрено	Практическая работа
Интересы личности, общества и государства в информационной сфере	Не предусмотрено	Не предусмотрено	Практическая работа
Законодательство в области информационной безопасности и защиты информации	Лекция-диалог	Не предусмотрено	Не предусмотрено
Понятие и виды информации, защищаемой законодательством Российской Федерации	Не предусмотрено	Не предусмотрено	Не предусмотрено
Методы обеспечения информационной безопасности	Не предусмотрено	Не предусмотрено	Практическая работа

6.2 Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров

6.3 Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
Notepad++	Текстовый редактор

OpenOffice	Пакет офисных программ
Opera	Браузер
Microsoft Security Assessment Tool. Режим доступа: http://www.microsoft.com/ru-ru/download/details.aspx?id=12273 (Free) Windows Security Risk Management Guide Tools and Templates. Режим доступа: http://www.microsoft.com/en-us/download/details.aspx?id=6232 (Free)	Программы для информационной безопасности
VLC Player	Медиапроигрыватель
Far Manager	Файловый менеджер

6.3.2. Современные профессиональные базы данных и информационные справочные системы

Наименование современных профессиональных баз данных, информационных справочных систем
Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС» http://dlib.eastview.com *Имя пользователя: AstrGU* *Пароль: AstrGU*
Электронные версии периодических изданий, размещённые на сайте информационных ресурсов www.polpred.com
Электронный каталог Научной библиотеки АГУ на базе MARKSQL НПО «Информ-систем» https://library.asu.edu.ru/catalog/
Электронный каталог «Научные журналы АГУ» https://journal.asu.edu.ru/
Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС) – сводная база данных, содержащая полную аналитическую роспись 1800 названий журналов по разным отраслям знаний. Участники проекта предоставляют друг другу электронные копии отсканированных статей изкниг, сборников, журналов, содержащихся в фондах их библиотек. http://mars.arbicon.ru
Справочная правовая система КонсультантПлюс. Содержится огромный массив справочной правовой информации, российское и региональное законодательство, судебную практику, финансовые икадровые консультации, консультации для бюджетных организаций, комментарии законодательства, формы документов, проекты нормативных правовых актов, международные правовые акты, правовые акты, технические нормы и правила. http://www.consultant.ru

7 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1 Паспорт фонда оценочных средств.

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Правовое обеспечение информационной безопасности» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 5 Соответствие изучаемых разделов, результатов обучения и оценочных средств

№ п/п	Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
1	Проблемная сфера информационной безопасности и защиты информации	ОПК-5 ОПК-9	Устное собеседование
2	Основы информационной безопасности в информационной сфере	ОПК-5 ОПК-9	Практическая работа

3	Интересы личности, общества и государства в информационной сфере	ОПК-5 ОПК-9	Практическая работа
4	Законодательство в области информационной безопасности и защиты информации	ОПК-5 ОПК-9	Практическая работа
5	Понятие и виды информации, защищаемой законодательством Российской Федерации	ОПК-5 ОПК-9	Практическая работа
6	Методы обеспечения информационной безопасности	ОПК-5 ОПК-9	Практическая работа Итоговое тестирование

7.2 Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 6

Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 7

Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1 Проблемная сфера информационной безопасности и защиты информации

Вопросы практического занятия

1. Основные понятия. Общие положения. Типы и виды информационной безопасности. Участники отношений в области информационной безопасности. Федеральные, региональные, местные законы по информационной безопасности.
2. Информационная общество, информационная сфера
3. Определение и эволюция термина «информационная безопасность». Соперничество в информационной сфере
4. Понятие информационных ресурсов. Документирование информации как обязательное условие документированных информационных ресурсов

5. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.

6. Экономическая информация как товар и объект безопасности.

Тема 2 Основы информационной безопасности в информационной сфере

Вопросы практической работы

1. Окинавская хартия глобального информационного общества от 22 июля 2000 года.
2. Принципы правового регулирования отношений в сфере регулирования. Обладатель информации.
3. Конфиденциальная информация.
4. Роль Интернета в мировом информационном пространстве. Глобальные ожидания и опасения человечества. Негативные последствия глобальной информатизации общества.
5. Информация и право. Научно-технический прогресс и условия формирования информационного общества. Информатика и правовые дисциплины. Информационное право. Виды информации, подлежащей защите. Понятие информации с ограниченным доступом. Соотношение тайн и права на информацию.

Тема 3 Интересы личности, общества и государства в информационной сфере.

Вопросы практической работы

1. Конституционные гарантии прав граждан на информацию и механизм их реализации.
2. Понятие государственной тайны, правовое регулирование.
3. Режим государственной тайны.
4. Понятие коммерческой тайны, правовое регулирование. Режим коммерческой тайны.
5. Практика правового регулирования и защиты коммерческой тайны за рубежом.

Тема 4 Законодательство в области информационной безопасности и защиты информации

Вопросы практической работы

1. Указы Президента Российской Федерации «О концепции национальной безопасности», «Перечень сведений, отнесенных к государственной тайне».
2. «Вопросы Межведомственной комиссии по защите государственной тайны».
3. Постановления Правительства Российской Федерации.
4. Нормативные документы Межведомственной комиссии по защите государственной тайны в Российской Федерации, ФСТЭК, МВД, ФСБ и др.
5. Законодательное регулирование вопросов обеспечения информационной безопасности.
6. Законы Российской Федерации «О безопасности», «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О персональных данных».
1. Правовая охрана информационных ресурсов.
2. Электронная подпись.
3. Лицензирование и сертификация в области обеспечения информационной безопасности.
4. Защита авторских и смежных прав в законодательстве Российской Федерации.

Тема 5 Понятие и виды информации, защищаемой законодательством Российской Федерации.

Вопросы практической работы

1. Классификация информации ограниченного доступа.
2. Государственная тайна.
3. Персональные данные.
4. Личная и семейная тайна.

5. Служебная тайна.
6. Коммерческая тайна.
7. Профессиональная тайна.
8. Тайна связи.
9. Тайна страхования.
10. Налоговая тайна.
11. Банковская тайна.
12. Тайна нотариальных действий.
13. Адвокатская тайна.
14. Врачебная тайна.
15. Тайна усыновления.
16. Тайна предварительного следствия и судопроизводства.

Тема 6 Методы обеспечения информационной безопасности

Практическое задание:

Составление распорядительных документов по обеспечению информационной безопасности на предприятиях различных форм собственности

Задание:

1. Разработать организационную структуру предприятия, номенклатуру должностей работников.
2. Разработать основной круг вопросов, решаемых руководством и сотрудниками предприятия по обеспечению информационной безопасности предприятия.
3. Разработать приказ по обеспечению информационной безопасности предприятия (распорядительная часть должна содержать не менее 5 пунктов мероприятий).
4. Составить указание сотрудникам предприятия по развитию и внедрению новых информационных технологий в своей отрасли.
5. Составить распоряжение о внедрении новых разработок по защите информации.
6. Составить решение о подготовке к проведению конференции по информационной безопасности.
7. Составить краткий протокол совещания по вопросам информационной безопасности.
8. Быть в готовности в роли руководителя, начальника службы безопасности решать управленческие задачи, связанные с обеспечением комплексной безопасности предприятия (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
9. Студентам письменно выполнить задание (объем 5-7 листов) и быть в готовности к его защите на практическом занятии.

Итоговое тестирование

1.В соответствии с Конституцией Российской Федерации информация и связь относятся:

а) к исключительному ведению Российской Федерации

б) к совместному ведению Российской Федерации и субъектов Российской Федерации

в) к ведению субъектов Российской Федерации

2. Согласно легальному определению, информация - это:

а) сведения о каких-либо событиях, явлениях, процессах, передаваемые от человека к человеку

б) сведения (сообщения, данные) независимо от формы их представления

в) сообщение, переданное или полученное пользователем информационно-телекоммуникационной сети

3. Лицо, самостоятельно создавшее информацию, либо получившее право разрешать или ограничивать доступ к информации, является:

а) создателем информации

б) хранителем информации

в) обладателем информации

4. Не подлежат размещению в сети «Интернет»:

а) фамилии, имена и отчества председателя суда, заместителей председателя суда, судей, руководителя аппарата суда

б) тексты судебных актов, вынесенные по делам, затрагивающим безопасность государства

в) информация о внепроцессуальных обращениях, поступивших судьям по делам, находящимся в их производстве

5.Объективная сторона информационной безопасности- это:

а) психологическое отношение граждан к вопросу правового регулирования отношений в сфере информационной безопасности

б) система норм права об информационной безопасности

в) система охранительных действий субъектов информационного права в отношении объекта охраны

6. Под киберпреступлением понимается:

а) самостоятельный вид виновно совершенного общественно опасного деяния, запрещенного нормами Уголовного кодекса Российской Федерации

б) любое преступление, совершенное в сфере информационной безопасности

в) совершение действий в системе Интернет, при которых компьютер является орудием либо предметом посягательства в кибернетическом пространстве

7. Понятие «информационная безопасность» закреплено:

а) в Законе Российской Федерации от 27 декабря 1991г. №1224-11 «О средствах массовой информации»

б) в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»

в) в Доктрине информационной безопасности

8. К числу носителей сведений, составляющих государственную тайну, не относится:

а) руководитель органа государственной власти

б) служебные документы

в) техническое устройство

9. Система защиты государственной тайны представляет собой:

а) совокупность органов защиты государственной тайны и используемых ими средств и методов защиты

б) процедуры оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений

в) порядок и способы отнесения сведений к государственной тайне и их засекречивание

10. Под засекречиванием сведений понимается:

а) взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями

б) передача сведений, составляющих государственную тайну, другим государствам или международным организациям

в) ведение ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям

11. Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых:

а) административным актом органа государственной власти, в распоряжение которого переходит эта информация

б) в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником

в) в соответствии с заявлением собственника информации

12. К сведениям, составляющим государственную тайну, без проведения проверочных мероприятий допускаются:

а) представители истца и ответчика в суде

б) действующие судьи

в) члены Правительства РФ

13. Коммерческая тайна представляет собой:

а) защищаемые юридическим лицом сведения любого характера (производственные, технические, экономические), имеющие коммерческую ценность в силу неизвестности их третьим лицам

б) режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

в) сведения, для которых установлен специальный режим сбора, хранения, обработки, распространения и использования, доступ к которым ограничен в соответствии с федеральным законом

14. Могут быть отнесены к информации, составляющей коммерческую тайну:

а) сведения о составе имущества государственного или муниципального предприятия, государственного учреждения

б) сведения о численности и составе работников, о системе оплаты труда

в) сведения, позволяющие юридическому лицу увеличить доходы и избежать неоправданных расходов

15. Обладателем секрета производства является:

а) лицо, которое использует ноу-хау в целях извлечение прибыли

б) лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании

в) любое юридическое лицо или индивидуальный предприниматель

16. По лицензионном договору:

а) одна сторона обязуется оформить в интересах другой стороны исключительное право на секрет производства

б) одна сторона передает или обязуется передать принадлежащее ей исключительное право на секрет производства в полном объеме другой стороне

в) одна сторона - обладатель исключительного права на секрет производства предоставляет или обязуется предоставить другой стороне право использования соответствующего секрета производства в установленных договором пределах

17. Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых:

а) административным актом органа государственной власти, в распоряжение которого переходит эта информация

б) в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником

в) в соответствии с заявлением собственника информации

18. Информация, относящаяся к прямо или косвенно определенному или определяемому лицу, является:

а) персональными данными субъекта

б) коммерческой тайной

в) служебной тайной

19. Правами в информационной сфере пользуются:

а) только физические лица

б) физические лица и юридические лица

в) физические лица, юридические лица, органы государственной власти, должностные лица, общественные организации

20. Не относятся к числу специальных категорий персональных данных:

а) сведения, которые характеризуют физиологические особенности человека

б) сведения, касающиеся расовой и национальной принадлежности

в) сведения о состоянии здоровья и интимной жизни человека

21. К числу прав субъекта персональных данных относится:

а) право на выбор вида обработки персональных данных автоматизированная, неавтоматизированная)

б) право на доступ к своим персональным данным

в) право контролировать деятельность оператора персональных данных

22. Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию - это:

а) ключ электронной подписи

б) сертификат ключа проверки электронной подписи

в) электронная подпись

23. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети, называется:

а) электронным сообщением

б) базой данных

в) электронной цифровой подписью

24. Удостоверяющий центр - это:

а) государственный орган, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации

б) любое юридическое или физическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации

в) юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации

25. Тайна вязи представляет собой:

а) деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений

б) нечто скрываемое от других, известное не всем; секрет

в) определенный режим доступа к информации, не подлежащей разглашению без согласия пользователя услуг, который реализуется путём принятия специальных мер организационного, правового, технического характера

26. В соответствии с Федеральным законом «О почтовой связи» в Российской Федерации действуют:

а) почтовая связь общего пользования, осуществляемая государственными унитарными предприятиями, государственными учреждениями почтовой связи, а также иными операторами почтовой связи

б) почтовая связь общего пользования; специальная связь федерального органа исполнительной власти; федеральная фельдъегерская связь; фельдъегерско-почтовая связь

в) специальная связь федерального органа исполнительной власти, осуществляющего управление деятельностью в области связи; федеральная фельдъегерская связь; фельдъегерско-почтовая связь федерального органа исполнительной власти в области обороны

27. Деятельность юридических лиц и индивидуальных предпринимателей по возмездному оказанию услуг связи:

а) не подлежит лицензированию

б) осуществляется только на основании лицензии на осуществление деятельности в области оказания услуг связи

в) подлежит лицензированию только в предусмотренных законом случаях

28. Не может выступать учредителем средства массовой информации:

а) государственный орган

б) гражданин другого государства

в) гражданин Российской Федерации, признанный судом дееспособным

29. Средство массовой информации - это:

а) результат интеллектуальной деятельности

б) печатные, аудио-, аудиовизуальные и иные сообщения и материалы; в) форма периодического распространения массовой информации

30. Деятельность средства массовой информации не может быть прекращена или приостановлена:

а) по решению учредителя

б) судом в порядке гражданского судопроизводства по иску регистрирующего органа

в) судом по требованию органа, осуществляющего цензуру

Перечень вопросов и заданий, выносимых на зачет

1.Понятие субъекта информационной безопасности. и объекты защиты.

2.Виды субъектов информационной безопасности.

3.Российская Федерация как субъект информационной безопасности.

4.Субъекты РФ и муниципальные образования как субъекты информационной безопасности.

5.Граждане и другие физические лица как субъекты информационной безопасности.

6.Несовершеннолетние как субъекты информационной безопасности.

7.Правовой статус общественных объединений и коммерческих организаций как субъектов информационной безопасности.

8.Государственное регулирование права доступа к информации.

9.Государственное регулирование охраны государственной тайны.

10.Компетенция органов государственной власти по обеспечению правового режима конфиденциальной информации.

11.Понятие и виды конфиденциальной информации.

12.Режимы защиты информации.

13.Государственная тайна как предмет, изъятый из гражданского оборота.

14.Служебная и профессиональная тайна

15.Коммерческая и банковская тайны

16.Понятие и структура персональных данных

17.Понятие и виды информационных технологий.

18.Порядок создания информационных технологий.

19.Нарушения порядка применения информационных технологий: информационные войны, несанкционированный мониторинг за активностью потребителя информации.

20.Понятие и виды информационной безопасности.

21.Понятие информационной безопасности личности.

22.Соблюдение конституционных прав и свобод человека и гражданина в области информационных правоотношений.

23.Ограничения использования информации о частной жизни.

24.Гарантии информационных прав граждан. Право на судебную защиту.

25.Правовые и этические пределы вмешательства в личную жизнь при использовании интерактивных методов работы с аудиторией.

26.Понятие безопасности в глобальном информационном пространстве.

27.Информационное обеспечение государственной политики Российской Федерации.

28.Понятие информационной безопасности общества.

29.Понятие информационной безопасности государства.

30.Обеспечение защиты информационных ресурсов от несанкционированного доступа.

31. Обеспечение безопасности информационных и телекоммуникационных систем.
32. Общая характеристика и виды ответственности за правонарушения в сфере информационной безопасности.
33. Дисциплинарная ответственность в сфере информационной безопасности.
34. Административная ответственность в сфере информационной безопасности.
35. Уголовная ответственность в сфере информационной безопасности.
36. Материальная ответственность в сфере информационной безопасности.
37. Материальная ответственность в сфере информационной безопасности.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
Код и наименование проверяемой компетенции ОПК – 5 - Способен профессионально толковать нормы права				
1	Задание закрытого типа	Понятие «информационная безопасность» закреплено: в Законе Российской Федерации от 27 декабря 1991г. №1224-11 «О средствах массовой информации» в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» в Доктрине информационной безопасности	2	2
2		К числу носителей сведений, составляющих государственную тайну, не относится: руководитель органа государственной власти служебные документы техническое устройство	1	2
3		К сведениям, составляющим государственную тайну, без проведения проверочных мероприятий допускаются: а) представители истца и ответчика в суде б) действующие судьи в) члены Правительства РФ	2	2
4		Информация, относящаяся к прямо или косвенно определенному или определяемому лицу, является: персональными данными субъекта коммерческой тайной служебной тайной	1	2
1	Задание открытого типа	Электронная подпись - это	информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию	4
2		Удостоверяющий центр - это	юридическое лицо или индивидуальный предприниматель, осуществляющие	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации	
3		Отличительные особенности юридической обработки информации	Условием превращения совокупности исходных текстов отдельных правовых актов в правовую систему является юридическая обработка документов квалифицированными специалистами. Юридическая обработка - это выявление взаимосвязей между документами и реализация, фиксирование выявленных связей с помощью определенных форм (ссылок, примечаний, справочных сведений), а также создание редакций документов при их изменении. Юридическая обработка начинается с определения его достоверности, актуальности, нормативности, после чего следует этап подготовки документа к введению в ИБ, состоящий из следующих элементов: • классификация (рубрикация) документа, подбор ключевых слов; • выявление взаимосвязей документов; • формирование перекрестных ссылок между документами; • составление примечаний, справочных сведений к документу; подготовка новой редакции документа	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			при издании официальных изменений.	
4		Тайна вязи представляет собой	определенный режим доступа к информации, не подлежащей разглашению без согласия пользователя услуг, который реализуется путём принятия специальных мер организационного, правового, технического характера	4
5		Информационная безопасность	все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.	4
1	Задание комбинированного типа	***Прочитайте текст, выберите один правильный вариант ответа и напишите аргументы, обосновывающие выбор ответа*** В соответствии с Конституцией Российской Федерации информация и связь относятся: к исключительному ведению Российской Федерации к совместному ведению Российской Федерации и субъектов Российской Федерации к ведению субъектов Российской Федерации.	Согласно Конституции Российской Федерации, вопросы информации и связи отнесены к **совместному ведению Российской Федерации и её субъектов**. Это закреплено в статье 72 Конституции РФ, где говорится о том, что «в совместном ведении Российской Федерации и субъектов Российской Федерации находятся... вопросы... информационной политики» (пункт "б" части 1 статьи 72). Таким образом, регулирование вопросов информации и связи осуществляется как на федеральном уровне, так и на уровне субъектов федерации.	4
Код и наименование проверяемой компетенции ОПК – 9 - Способен получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учетом требований информационной безопасности				
1	Задание Закрытого типа	Что понимается под данными об объектах, событиях и процессах? содержимое баз знаний	5	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		необработанные сообщения, отражающие отдельные факты, процессы, события предварительно обработанная информация сообщения, находящиеся в хранилищах данных		
2		Согласно легальному определению, информация - это: сведения о каких-либо событиях, явлениях, процессах, передаваемые от человека к человеку сведения (сообщения, данные) независимо от формы их представления сообщение, переданное или полученное пользователем информационно-телекоммуникационной сети.	2	2
3		Лицо, самостоятельно создавшее информацию, либо получившее право разрешать или ограничивать доступ к информации, является: создателем информации хранителем информации обладателем информации	3	2
4		Не подлежат размещению в сети «Интернет»: фамилии, имена и отчества председателя суда, заместителей председателя суда, судей, руководителя аппарата суда тексты судебных актов, вынесенные по делам, затрагивающим безопасность государства информация о внепроцессуальных обращениях, поступивших судьям по делам, находящимся в их производстве	2	2
1	Задание открытого типа	Коммерческая тайна представляет собой ….	режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду	4
2		Что не относятся к числу специальных категорий персональных данных	сведения, которые характеризуют физиологические особенности человека	4
3		Правами в информационной сфере пользуются ….	физические лица, юридические лица, органы государственной власти, должностные	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			лица, общественные организации*.	
4		Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в размерах, определяемых	в договоре между органом государственной власти, в распоряжение которого переходит эта информация, и ее собственником	4
5		По лицензионном договору …	одна сторона - обладатель исключительного права на секрет производства предоставляет или обязуется предоставить другой стороне право использования соответствующего секрета производства в установленных договором пределах	4
1	Задание комбинированного типа	***Прочитайте текст, выберите один правильный вариант ответа и напишите аргументы, обосновывающие выбор ответа*** Под киберпреступлением понимается: самостоятельный вид виновно совершенного общественно опасного деяния, запрещенного нормами Уголовного кодекса Российской Федерации любое преступление, совершенное в сфере информационной безопасности совершение действий в системе Интернет, при которых компьютер является орудием либо предметом посягательства в кибернетическом пространстве	Киберпреступление действительно представляет собой самостоятельный вид преступной деятельности, которая нарушает нормы уголовного права. В Уголовном кодексе Российской Федерации есть ряд статей, регулирующих ответственность за преступления в области компьютерной информации (например, статья 272 УК РФ – неправомерный доступ к компьютерной информации). Эти преступления связаны с использованием компьютеров, компьютерных сетей и других информационных технологий для совершения противоправных деяний. Киберпреступления включают такие виды преступлений, как взлом систем защиты данных, распространение вредоносных программ, мошенничество с	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			использованием электронных средств платежа и другие подобные действия.	

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Максимальное количество баллов за работу в течение 1 семестра: 100 баллов

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1	Устное собеседование	1 задание по 10 баллов	10 баллов	по расписанию
2	Практическая работа	5 заданий по 10 баллов	50 баллов	по расписанию
3	Тестирование	1 работа по 20 баллов	20 баллов	по расписанию
Всего			**80 баллов**	-
Блок бонусов				
1	Посещение занятий	0,5 баллов	2 баллов	
2	Своевременное выполнение всех заданий	0,5 баллов	3 баллов	
Всего			**5 баллов**	-
Дополнительный блок				
1	Зачет	1 билет 15 баллов	15 баллов	По расписанию
Всего			15 баллов	-
ИТОГО			**100**	-

Таблица 11 Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	2
Нарушение учебной дисциплины	10
Неготовность к занятию	1
Пропуск занятия без уважительной причины	2

Таблица 12 Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

ДИСЦИПЛИНЫ (МОДУЛЯ)

а) Основная литература

1. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: рек. УМО по образованию в области историко-архивоведения в качестве учеб. пособия для студентов вузов, обуч. по спец. «Организация и технология защиты информации», «Комплексная защита объектов информации» - М.: ФОРУМ; ИНФРА-М, 2014. - 256 с.
2. Куняев Н.Н., Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, Т.В. Кондрашова, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева - М.: Логос, 2017. - 500 с. (Новая университетская библиотека) - ISBN 978-5-98704-711-8 - Текст : электронный// ЭБС «Консультант студента» : [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785987047118.html (ЭБС «Консультант студента»).

б) Дополнительная литература

1. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф.-М.: ДМК Пресс, 2014. - http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
2. Садердинов, А.А. Информационная безопасность предприятия: учеб. пособ. / А. А. Садердинов, Трайнев, В.А., Федулов, А.А. - 2-е изд. - М.: Дашков и К, 2005. - 336 с. (37 экз.)
3. Конституция Российской Федерации // СПС КонсультантПлюс
4. Доктрина информационной безопасности РФ. Утверждена Президентом РФ 09.09.2000. № Пр-1895 // СПС КонсультантПлюс
5. Уголовный Кодекс РФ // СПС КонсультантПлюс
6. Гражданский кодекс РФ. Ч. 4 // СПС КонсультантПлюс
7. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ // СПС КонсультантПлюс
8. Закон РФ «О государственной тайне» // СПС КонсультантПлюс
9. Закон РФ «О безопасности» // СПС КонсультантПлюс
10. Закон РФ «О персональных данных» от 27.07.2006 №152-ФЗ. // СПС КонсультантПлюс
11. Закон РФ «О средствах массовой информации» // СПС КонсультантПлюс
12. Закон РФ «О связи» // СПС КонсультантПлюс
13. Закон РФ «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ //СПС КонсультантПлюс
14. Закон РФ «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ//СПС КонсультантПлюс
15. Закон РФ «О техническом регулировании» от 27.12.2002 № 184-ФЗ//СПС КонсультантПлюс
16. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // СПС КонсультантПлюс
17. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти // СПС КонсультантПлюс
18. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» // СПС КонсультантПлюс
19. Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» // СПС КонсультантПлюс

в) перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины (модуля)

Перечень электронно-библиотечных систем (ЭБС)

Наименование ЭБС

Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований.
www.studentlibrary.ru. *Регистрация с компьютеров АГУ*

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

В качестве материально-технического обеспечения дисциплины (модуля) могут быть использованы технические и электронные средства обучения и контроля знаний обучающихся (оборудование, демонстрационные приборы, мультимедийные средства, презентации, фрагменты фильмов, комплекты плакатов, наглядных пособий, контролирующих программ и демонстрационных установок, тренажёры, карты), применение которых предусмотрено методической концепцией преподавания, а также перечень аудиторий без указания на их номера (компьютерные классы, академические или специально оборудованные аудитории и лаборатории, наличие доски и т. д.)

10 ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т. д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т. д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую

помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).