МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНБАССКАЯ АГРАРНАЯ АКАДЕМИЯ»
КАФЕДРА ЮРИСПРУДЕНЦИИ

УТВЕРЖДАЮ:
Первый проректор
_____ О.А. Удалых
(подпись) (ФИО)
«17» апреля 2025 г.
М.П.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
«Административно-правовые основы информационной безопасности РФ»
(наименование дисциплины)

Направление подготовки/специальность 40.03.01 Юриспруденция
(код и наименование направления подготовки/специальности)

Направленность (профиль) Юриспруденция
(наименование профиля/специализации подготовки, при наличии)

Квалификация выпускника: **бакалавр**
(квалификация выпускника)

Год начала подготовки: 2025

Макеевка – 2025

Фонд оценочных средств по дисциплине «Административно-правовые основы информационной безопасности РФ» является частью ОПОП ВО по направлению подготовки 40.03.01 Юриспруденция и предназначен для оценивания уровня сформированности компетенций обучающихся.

Разработчик(и) _____ Р.Н. Горбатый
(подпись) (ИОФ)

_____ _____
(подпись) (ИОФ)

_____ _____
(подпись) (ИОФ)

Фонд оценочных средств обсужден на заседании ПМК кафедры юриспруденции, протокол № 8 от «28» марта 2025 года.

Председатель ПМК _____ Е.А.Гресева
(подпись) (ИОФ)

Фонд оценочных средств утвержден на заседании кафедры юриспруденции, протокол № 8 от «28» марта 2025 года.

Заведующий кафедрой _____ И.М. Лукина
(подпись) (ИОФ)

Раздел 1. ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Административно-правовые основы информационной безопасности РФ»

1.1. Основные сведения о дисциплине

Укрупненная группа	40.00.00 Юриспруденция		
Направление подготовки / специальность	40.03.01 Юриспруденция		
Профиль	Юриспруденция		
Образовательная программа	бакалавриат		
Квалификация	бакалавр		
Дисциплина части обязательная/ формируемая участниками образовательных отношений	Обязательная часть		
Форма контроля	зачет		
Показатели трудоемкости	Форма обучения		
	очная	**заочная**	**очно-заочная**
Год обучения	4	4	4
Семестр	8	8	8
Количество зачетных единиц	2	2	2
Общее количество часов	72	72	72
Количество часов, часы:			
-лекционных	10	10	8
-практических (семинарских)	10	-	8
-лабораторных	-	-	-
-курсовая работа (проект)	-	-	-
-контактной работы на промежуточную аттестацию	2	2	2
-самостоятельной работы	50	60	54

1.2. Перечень компетенций, формируемых дисциплиной «Административно-правовые основы информационной безопасности РФ»

Код и наименование общепрофессиональной компетенции	**Код и наименование индикатора достижения общепрофессиональнойкомпетенции**	
ОПК-8. Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований	ОПК-8.2. Умеет использовать полученную информацию для решения задач профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности деятельности. ОПК-8.3. Владеет навыками систематизации и обобщения полученной информации с применением информационных технологий и с учетом требований информационной безопасности	

1.3. Перечень тем дисциплины

Шифр темы	Название темы	Кол-во часов
Т 1.1.	Информационная безопасность в системе национальной безопасности Российской Федерации	10
Т 1.2.	Законодательство в сфере информационной безопасности в Российской Федерации	10
Т 2.1.	Информация как объект правового регулирования	10
Т 2.2.	Правовое регулирование информационной безопасности в сфере интеллектуальной собственности	10
Т 2.3.	Юридическая ответственность за правонарушения в сфере информационных технологий	10
Т 3.1.	Понятие, задачи и состав системы обеспечения информационной безопасности	10
Т 3.2.	Системы лицензирования и сертификации в области обеспечения информационной безопасности	10
	Другие виды контактной работы	2,
Всего		**72**

1.4. Матрица соответствия тем дисциплины и компетенций

Шифр компетенции по ФГОС ВО	*Шифр темы*						
	Т 1.1	**Т 1.2**	**Т 2.1.**	**Т 2.2.**	**Т 2.3.**	**Т 3.1.**	**Т 3.2.**
ОПК-8	+	+	+	+	+	+	+

1.5. Соответствие тем дисциплины и контрольно-измерительных материалов

№ темы	*ТЕКУЩИЙ КОНТРОЛЬ*					
	Тестовые задания по теоретическому материалу	***Вопросы для устного опроса***	***Типовые задания практического характера***	***Задания для контрольной работы***	***Тематика рефератов, докладов, сообщений***	***Групповое творческое задание***
	Блок А Контроль знаний		**Блок Б Контроль умений, навыков**			
Тема 1.1	+	+	+	+	+	+
Тема 1.2	+	+	+	+	+	+
Тема 2.1	+	+	+	+	+	+
Тема 2.2	+	+	+	+	+	+
Тема 2.3	+	+	+	+	+	+
Тема 3.1	+	+	+	+	+	+
Тема 3.2	+	+	+	+	+	+

1.6. Описание показателей и критериев оценивания компетенций на различных этапах их формирования

Результат обучения по дисциплине	Критерии и показатели оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
I этап	**Фрагментарные знания**	**Неполные знания**	**Сформированные, но**	**Сформированные**

Знать - предмет и метод гражданско-правового регулирования общественных отношений; субъектный состав и структуру объектов гражданского правоотношения; субъективные гражданские права, порядок их реализации и защита, исполнение субъективных гражданских обязанностей. - содержание основных нормативно-правовых актов, регулирующих земельные правоотношения; знать основные базы данных и информационно-консультационные правовые системы; официальные сайты органов государственной власти и местного самоуправления; - методы, способы и средства получения, хранения, переработки криминалистически значимой информации; - содержание нормативных правовых актов, предусматривающих ответственность за	- предмет и метод гражданско-правового регулирования общественных отношений; субъектный состав и структуру объектов гражданского правоотношения; субъективные гражданские права, порядок их реализации и защита, исполнение субъективных гражданских обязанностей. - содержание основных нормативно-правовых актов, регулирующих земельные правоотношения; знать основные базы данных и информационно-консультационные правовые системы; официальные сайты органов государственной власти и местного самоуправления; - методы, способы и средства получения, хранения, переработки криминалистически значимой информации; - содержание нормативных правовых актов, предусматривающих ответственность за совершение преступлений;	- предмет и метод гражданско-правового регулирования общественных отношений; субъектный состав и структуру объектов гражданского правоотношения; субъективные гражданские права, порядок их реализации и защита, исполнение субъективных гражданских обязанностей. - содержание основных нормативно-правовых актов, регулирующих земельные правоотношения; знать основные базы данных и информационно-консультационные правовые системы; официальные сайты органов государственной власти и местного самоуправления; - методы, способы и средства получения, хранения, переработки криминалистически значимой информации; - содержание нормативных правовых актов, предусматривающих ответственность за совершение преступлений;	**содержащие отдельные пробелы знания** - предмет и метод гражданско-правового регулирования общественных отношений; субъектный состав и структуру объектов гражданского правоотношения; субъективные гражданские права, порядок их реализации и защита, исполнение субъективных гражданских обязанностей. - содержание основных нормативно-правовых актов, регулирующих земельные правоотношения; знать основные базы данных и информационно-консультационные правовые системы; официальные сайты органов государственной власти и местного самоуправления; - методы, способы и средства получения, хранения, переработки криминалистически значимой информации;	**систематические зна** - предмет и ме гражданско-правового регулирования общественных отноше субъектный состав структуру объе гражданского правоотношения; субъективные граждан права, порядок реализации и защ исполнение субъектив гражданских обязаннос - содержание основ нормативно-правовых актов, регулирую земельные правоотношения; з основные базы данны информационно-консультационные правовые систе официальные са органов государствен власти и мест самоуправления; - методы, способы средства получе хранения, перераб криминалистически значимой информации; - содержание норматив правовых ак предусматривающих ответственность

совершение преступлений; понятие и виды юридических документов, оформляющих возникновение, изменение и прекращение уголовно-правовых отношений; систему средств, правил и приемов подготовки и упорядочения юридических документов; - основные закономерности создания и функционирования информационных процессов в правовой сфере; методы и средства поиска, систематизации и обработки правовой информации; - положения нормативных правовых актов в области обеспечения информационной безопасности; понятийный аппарат в области обеспечения информационной безопасности, виды информации, подлежащей правовой охране; организационную систему обеспечения информационной безопасности	понятие и виды юридических документов, оформляющих возникновение, изменение и прекращение уголовно-правовых отношений; систему средств, правил и приемов подготовки и упорядочения юридических документов; - основные закономерности создания и функционирования информационных процессов в правовой сфере; методы и средства поиска, систематизации и обработки правовой информации; - положения нормативных правовых актов в области обеспечения информационной безопасности; понятийный аппарат в области обеспечения информационной безопасности, виды информации, подлежащей правовой охране; организационную систему обеспечения информационной безопасности	понятие и виды юридических документов, оформляющих возникновение, изменение и прекращение уголовно-правовых отношений; систему средств, правил и приемов подготовки и упорядочения юридических документов; - основные закономерности создания и функционирования информационных процессов в правовой сфере; методы и средства поиска, систематизации и обработки правовой информации; - положения нормативных правовых актов в области обеспечения информационной безопасности; понятийный аппарат в области обеспечения информационной безопасности, виды информации, подлежащей правовой охране; организационную систему обеспечения информационной безопасности	- содержание нормативных правовых актов, предусматривающих ответственность за совершение преступлений; понятие и виды юридических документов, оформляющих возникновение, изменение и прекращение уголовно-правовых отношений; систему средств, правил и приемов подготовки и упорядочения юридических документов; - основные закономерности создания и функционирования информационных процессов в правовой сфере; методы и средства поиска, систематизации и обработки правовой информации; - положения нормативных правовых актов в области обеспечения информационной безопасности; понятийный аппарат в области обеспечения информационной безопасности, виды информации, подлежащей правовой охране; организационную систему	совершение преступле понятие и в юридических докумен оформляющих возникновение, измене и прекращение уголо правовых отноше систему средств, прави приемов подготовки упорядочения юридичес документов; - основные закономерно создания функционирования информационных процессов в право сфере; методы и средс поиска, систематизаци обработки право информации; - положения норматив правовых актов в обла обеспечения информационной безопасности; понятий аппарат в обла обеспечения информационной безопасности, в информации, подлежа правовой охр организационную сист обеспечения информационной безопасности

(ОПК-8.2/ОПК-8.3)	**/Отсутствие умений**		обеспечения информационной безопасности	
II этап Уметь - различать все виды источников гражданского права и находить необходимую информацию в них; анализировать условия, обеспечивающие юридическое равенство сторон, свободу договора, неприкосновенность права собственности; - использовать основные базы данных и информационно-консультационные правовые системы, а также интернет ресурсы, в том числе официальные сайты органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений; - использовать криминалистически значимую информацию в целях раскрытия и	**Фрагментарное умение** - различать все виды источников гражданского права и находить необходимую информацию в них; анализировать условия, обеспечивающие юридическое равенство сторон, свободу договора, неприкосновенность права собственности; - использовать основные базы данных и информационно-консультационные правовые системы, а также интернет ресурсы, в том числе официальные сайты органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений; - использовать криминалистически значимую информацию в целях раскрытия и	**В целом успешное, но несистематическое умение** - различать все виды источников гражданского права и находить необходимую информацию в них; анализировать условия, обеспечивающие юридическое равенство сторон, свободу договора, неприкосновенность права собственности; - использовать основные базы данных и информационно-консультационные правовые системы, а также интернет ресурсы, в том числе официальные сайты органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений; - использовать криминалистически значимую информацию в	**В целом успешное, но содержащее отдельные пробелы умение** - различать все виды источников гражданского права и находить необходимую информацию в них; анализировать условия, обеспечивающие юридическое равенство сторон, свободу договора, неприкосновенность права собственности; - использовать основные базы данных и информационно-консультационные правовые системы, а также интернет ресурсы, в том числе официальные сайты органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений; - использовать криминалистически	**Успешное и систематическое уме** - различать все в источников гражданс права и наход необходимую информа в них; анализиро условия, обеспечиваю юридическое равен сторон, свободу догов неприкосновенность пр собственности; - использовать основ базы данных информационно-консультационные правовые системы, а та интернет ресурсы, в числе официальные са органов государствен власти и мест самоуправления вопросам регулирова земельных правоотношений; - использов криминалистически значимую информаци

расследования преступлений; - использовать знания уголовно-правовых норм в целях квалифицированной подготовки юридических документов; использовать систему средств, правил и приемов подготовки и упорядочения юридических документов; осуществлять криминологические экспертизы нормативно-правовых документов; - применять современные информационные технологии для поиска и обработки правовой информации; - применять нормы права, регулирующие сферу информационной безопасности при решении задач профессиональной деятельности с применением информационных технологий; работать с нормативно-правовым материалом, использовать и извлекать всю необходимую для решения проблемы информацию в условиях обеспечения соблюдения законодательства	расследования преступлений; - использовать знания уголовно-правовых норм в целях квалифицированной подготовки юридических документов; использовать систему средств, правил и приемов подготовки и упорядочения юридических документов; осуществлять криминологические экспертизы нормативно-правовых документов; - применять современные информационные технологии для поиска и обработки правовой информации; - применять нормы права, регулирующие сферу информационной безопасности при решении задач профессиональной деятельности с применением информационных технологий; работать с нормативно-правовым материалом, использовать и извлекать всю необходимую для решения проблемы информацию в условиях обеспечения соблюдения законодательства	целях раскрытия и расследования преступлений; - использовать знания уголовно-правовых норм в целях квалифицированной подготовки юридических документов; использовать систему средств, правил и приемов подготовки и упорядочения юридических документов; осуществлять криминологические экспертизы нормативно-правовых документов; - применять современные информационные технологии для поиска и обработки правовой информации; - применять нормы права, регулирующие сферу информационной безопасности при решении задач профессиональной деятельности с применением информационных технологий; работать с нормативно-правовым материалом, использовать и извлекать всю необходимую для решения проблемы информацию в условиях обеспечения соблюдения	значимую информацию в целях раскрытия и расследования преступлений; - использовать знания уголовно-правовых норм в целях квалифицированной подготовки юридических документов; использовать систему средств, правил и приемов подготовки и упорядочения юридических документов; осуществлять криминологические экспертизы нормативно-правовых документов; - применять современные информационные технологии для поиска и обработки правовой информации; - применять нормы права, регулирующие сферу информационной безопасности при решении задач профессиональной деятельности с применением информационных технологий; работать с нормативно-правовым материалом, использовать и извлекать всю необходимую для решения проблемы информацию в условиях обеспечения	целях раскрытия расследования преступлений; - использовать зна уголовно-правовых нор целях квалифицирован подготовки юридичес документов; использо систему средств, прави приемов подготовки упорядочения юридичес документов; осуществл криминологические экспертизы нормати правовых документов; - применять современ информационные технологии для поиск обработки право информации; - применять нормы пр регулирующие сф информационной безопасности при реше задач профессиональ деятельности применением информационных технологий; работать нормативно-правовым материалом, использова извлекать необходимую для реше проблемы информацию условиях обеспече соблюдения

Российской Федерации субъектами права. **(ОПК-8.2/ОПК-8.3)**	Российской Федерации субъектами права. **/Отсутствие умений**	законодательства Российской Федерации субъектами права.	соблюдения законодательства Российской Федерации субъектами права.	законодательства Российской Федера субъектами права.
III этап Иметь навыки - с информационными правовыми базами, содержащими юридически значимую информацию в сфере гражданского права и иными ресурсами с учетом требований информационной безопасности; решения профессиональных задач в сфере гражданского права с использованием юридически значимой информации; - работы с основными базами данных и информационно-консультационными правовыми системами, официальными сайтами органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений; - работы с компьютером	**Фрагментарное применение навыков** - с информационными правовыми базами, содержащими юридически значимую информацию в сфере гражданского права и иными ресурсами с учетом требований информационной безопасности; решения профессиональных задач в сфере гражданского права с использованием юридически значимой информации; - работы с основными базами данных и информационно-консультационными правовыми системами, официальными сайтами органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений; - работы с компьютером	**В целом успешное, но несистематическое применение навыков** - с информационными правовыми базами, содержащими юридически значимую информацию в сфере гражданского права и иными ресурсами с учетом требований информационной безопасности; решения профессиональных задач в сфере гражданского права с использованием юридически значимой информации; - работы с основными базами данных и информационно-консультационными правовыми системами, официальными сайтами органов государственной власти и местного самоуправления по вопросам регулирования земельных правоотношений;	**В целом успешное, но сопровождающееся отдельными ошибками применение навыков** - с информационными правовыми базами, содержащими юридически значимую информацию в сфере гражданского права и иными ресурсами с учетом требований информационной безопасности; решения профессиональных задач в сфере гражданского права с использованием юридически значимой информации; - работы с основными базами данных и информационно-консультационными правовыми системами, официальными сайтами органов государственной власти и местного самоуправления по вопросам регулирования земельных	**Успешное и систематическое применение навыко** - с информационны правовыми базам содержащими юридичес значимую информацию сфере гражданского прав иными ресурсами с учет требований информационной безопасности; решен профессиональных задач сфере гражданского прав использованием юридически значим информации; - работы с основны базами данных информационно-консультационными правовыми система официальными сайта органов государственн власти и местно самоуправления вопросам регулирован земельных правоотношений;

как средством управления информацией; - использования системы средств, правил и приемов подготовки и упорядочения юридических документов; - использования информационных технологий для оформления юридических документов; владения приемами и инструментами защиты информации; - соблюдения требований нормативных правовых актов, регламентирующих вопросы обеспечения информационной безопасности, соблюдения законодательства РФ в области оборота информации, подлежащей правовой защите при решении задач профессиональной деятельности с применением информационных технологий. **(ОПК-8.2/ОПК-8.3)**	как средством управления информацией; - использования системы средств, правил и приемов подготовки и упорядочения юридических документов; - использования информационных технологий для оформления юридических документов; владения приемами и инструментами защиты информации; - соблюдения требований нормативных правовых актов, регламентирующих вопросы обеспечения информационной безопасности, соблюдения законодательства РФ в области оборота информации, подлежащей правовой защите при решении задач профессиональной деятельности с применением информационных технологий. **/Отсутствие навыков**	- работы с компьютером как средством управления информацией; - использования системы средств, правил и приемов подготовки и упорядочения юридических документов; - использования информационных технологий для оформления юридических документов; владения приемами и инструментами защиты информации; - соблюдения требований нормативных правовых актов, регламентирующих вопросы обеспечения информационной безопасности, соблюдения законодательства РФ в области оборота информации, подлежащей правовой защите при решении задач профессиональной деятельности с применением информационных технологий.	правоотношений; - работы с компьютером как средством управления информацией; - использования системы средств, правил и приемов подготовки и упорядочения юридических документов; - использования информационных технологий для оформления юридических документов; владения приемами и инструментами защиты информации; - соблюдения требований нормативных правовых актов, регламентирующих вопросы обеспечения информационной безопасности, соблюдения законодательства РФ в области оборота информации, подлежащей правовой защите при решении задач профессиональной деятельности с применением информационных технологий.	- работы с компьютер как средством управлен информацией; - использования систе средств, правил и прием подготовки и упорядочен юридических документов - использован информационных технологий д оформления юридическ документов; владен приемами и инструмента защиты информации; - соблюдения требован нормативных правов актов, регламентирующ вопросы обеспечен информационной безопасности, соблюден законодательства РФ области оборо информации, подлежащ правовой защите п решении зад профессиональной деятельности применением информационных технологий.

Раздел 2. ОЦЕНОЧНЫЕ СРЕДСТВА

Блок А
ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ ОБУЧАЮЩИХСЯ

Фонд тестовых заданий по дисциплине

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

Критерии и шкалы оценивания тестов

Критерии оценивания при текущем контроле
процент правильных ответов менее 40 (по 5 бальной системе контроля – оценка «неудовлетворительно»);
процент правильных ответов 40 – 59 (по 5 бальной системе контроля – оценка «удовлетворительно»)
процент правильных ответов 60 – 79 (по 5 бальной системе контроля – оценка «хорошо»)
процент правильных ответов 80-100 (по 5 бальной системе контроля – оценка «отлично»)

Вопросы для устного опроса

ТЕМА 1.1.

1. Дайте понятие, структура и содержание информационной безопасности.
2. В чем заключается понятие и сущность комплексной защиты информации?
3. Опишите угрозу информационной безопасности личности, обществу и государству.
4. Охарактеризуйте направления государственной политики РФ в сфере информационной безопасности личности, общества, государства, современных автоматизированных и телекоммуникационных систем.
5. Концептуальные документы в области обеспечения информационной безопасности РФ.

ТЕМА 1.2.

1. Дайте понятие и содержание правового обеспечения информационной безопасности.
2. Опишите классификацию и структуру нормативных правовых актов в сфере обеспечения защиты информации.
3. Что предусматривает Конституция о правах и обязанностях граждан России в сфере обеспечения информационной безопасности?
4. Что представляет собой международно-правовой опыт защиты информации?
5. Опишите содержание основных законодательных актов сфере информационной безопасности.
6. Основные положения Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

ТЕМА 2.1.

1. Охарактеризуйте информацию как объект правоотношений в сфере обеспечения информационной безопасности.
2. Что такое информация и информационные системы?
3. Дайте понятие и виды защищаемой информации.
4. В чем заключается государственная тайна как особый вид защищаемой информации.
5. Перечислите виды «тайны».
6. Что такое персональные данные как вид защищаемой конфиденциальной информации?

ТЕМА 2.2.

1. Дайте характеристику интеллектуальной собственности в системе правового регулирования информационной безопасности.
2. Опишите основы авторского права.
3. В чем заключается правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.
4. Что такое защита объектов промышленной собственности на основе патентов?
5. Перечислите основные положения патентного права.

ТЕМА 2.3.

1. Дайте понятие юридической ответственности за нарушение правовых норм в области информационной безопасности.
2. Опишите виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
3. Характеристика уголовной ответственности за нарушение правовых норм в сфере защиты информации.
4. Характеристика административная ответственность за нарушения правовых норм в сфере защиты информации.
5. Особенности юридической ответственности за нарушения норм защиты информации в области трудовых и гражданско-правовых отношений.

6. Уголовно-правовая ответственность за противоправные действия в сфере защиты информации.

ТЕМА 3.1.

1. Опишите понятие и задачи государственной системы обеспечения информационной безопасности в РФ.
2. В чем заключается структура государственной системы информационной безопасности в РФ?
3. Опишите организационную основу системы информационной безопасности РФ.
4. Какие полномочия органов государственной власти Российской Федерации в области обеспечения информационной безопасности.

ТЕМА 3.2.

1. Опишите основные понятия и положения системы государственного лицензирования. Организационная структура системы государственного лицензирования.
2. Назовите основные понятия и система сертификации продукции и услуг.
3. В чем заключается особенности сертификации средств защиты информации?
3. Опишите ответственность за правонарушения в сфере лицензирования и сертификации.
4. Какие особенности лицензирования и сертификации в области защиты информации?
5. Перечислите организационные аспекты получения лицензии на занятие деятельностью в сфере обеспечения информационной безопасности.
6. Опишите организационные аспекты получения сертификата соответствия на средства защиты информации.

Критерии и шкалы оценивания устного опроса

Критерии оценки при текущем контроле	Оценка
Студент отсутствовал на занятии или не принимал участия. Неверные и ошибочные ответы по вопросам, разбираемым на семинаре	«неудовлетворительно»
Студент принимает участие в обсуждении некоторых проблем, даёт расплывчатые ответы на вопросы. Описывая тему, путается и теряет суть вопроса. Верность суждений, полнота и правильность ответов – 40-59 %	«удовлетворительно»
Студент принимает участие в обсуждении некоторых проблем, даёт ответы на некоторые вопросы, то есть не проявляет достаточно высокой активности. Верность суждений студента, полнота и правильность ответов 60-79%	«хорошо»
Студент демонстрирует знание материала по разделу, основанные на знакомстве с обязательной литературой и современными публикациями; дает логичные, аргументированные ответы на поставленные вопросы. Высока активность студента при ответах на вопросы преподавателя, активное участие в проводимых дискуссиях. Правильность ответов и полнота их раскрытия должны составлять более 80%	«отлично»

Блок Б
ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УМЕНИЙ, НАВЫКОВ ОБУЧАЮЩИХСЯ

Типовые задания для практических занятий

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
- Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики

безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций.

Критерии и шкалы оценивания решения практических заданий

Критерии оценки при текущем контроле	Оценка
Задача не решена или решена неправильно	«неудовлетворительно»
Задание понято правильно; в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задача решена не полностью или в общем виде	«удовлетворительно»
Составлен правильный алгоритм решения задачи; в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задача решена нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ	«хорошо»
Составлен правильный алгоритм решения задачи; в логическом рассуждении, в выборе формул и решении нет ошибок; получен верный ответ; задача решена рациональным способом	«отлично»

Задания для контрольной работы (заочная форма обучения)

1. Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.
2. Основы авторского права.
3. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.
4. Защита объектов промышленной собственности на основе патентов.
5. Основные положения патентного права.
6. Организационно-правовая система обеспечения защиты объектов промышленной собственности на основе патентов.
7. Юридическая ответственность за нарушение правовых норм защиты информации.
8. Понятие юридической ответственности за нарушение правовых норм в области информационной безопасности.
9. Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
10. Характеристика отдельных видов юридической ответственности в сфере защиты информации.
11. Уголовная ответственность за нарушение правовых норм в сфере защиты информации.
12. Административная ответственность за нарушения правовых норм в сфере защиты информации.
13. Особенности юридической ответственности за нарушения норм защиты информации в области трудовых и гражданско-правовых отношений.
14. Уголовно-правовая ответственность за противоправные действия в сфере защиты информации.
15. Понятие и задачи государственной системы обеспечения информационной безопасности в РФ.
16. Структура государственной системы информационной безопасности в РФ.
17. Организационная основа системы информационной безопасности РФ.
18. Полномочия органов государственной власти Российской Федерации в области обеспечения информационной безопасности.
19. Система лицензирования в области защиты информации.

20. Основные понятия и положения системы государственного лицензирования.
21. Организационная структура системы государственного лицензирования.
22. Система сертификации в области защиты информации.
23. Основные понятия и система сертификации продукции и услуг.
24. Особенности сертификации средств защиты информации.
25. Ответственность за правонарушения в сфере лицензирования и сертификации.
26. Особенности лицензирования и сертификации в области защиты информации.
27. Организационные аспекты получения лицензии на занятие деятельностью в сфере обеспечения информационной безопасности.
28. Организационные аспекты получения сертификата соответствия на средства защиты информации.

Образец варианта контрольной работы

Вариант 1
1. Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
2. Основные положения патентного права.

Критерии и шкалы оценивания контрольной работы

Критерии оценивания	Оценка
Ответ не был дан или не соответствует минимальным критериям	«неудовлетворительно»
Ответ со значительным количеством неточностей, но соответствует минимальным критериям	«удовлетворительно»
Ответ был верным с незначительным количеством неточностей	«хорошо»
Ответ полный с незначительным количеством неточностей	«отлично»

Темы для подготовки реферата (доклада, сообщения, презентации)

1. Место информационной безопасности в системе национальной безопасности РФ. Понятие, структура и содержание информационной безопасности.
2. Понятие и сущность комплексной защиты информации. Угрозы информационной безопасности личности, обществу и государству.
3. Направления государственной политики РФ в сфере информационной безопасности личности, общества, государства, современных автоматизированных и телекоммуникационных систем.
4. Концептуальные документы в области обеспечения информационной безопасности РФ.
5. Понятие и содержание правового обеспечения информационной безопасности. Классификация и структура нормативных правовых актов в сфере обеспечения защиты информации.
6. Конституция о правах и обязанностях граждан России в сфере обеспечения информационной безопасности. Международно-правовой опыт защиты информации.
7. Международно-правовые нормы в области защиты информации. Содержание основных законодательных актов сфере информационной безопасности.
8. Основные положения Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Информация как объект правоотношений в сфере обеспечения информационной безопасности. Информация и информационные системы – объекты правоотношений в сфере обеспечения информационной безопасности.

10. Понятие и виды защищаемой информации. Государственная тайна как особый вид защищаемой информации. Правовая основа обеспечения защиты коммерческой тайны. Правовое обеспечение защиты служебной тайны.

11. Персональные данные как вид защищаемой конфиденциальной информации.

12. Правовая основа защиты профессиональных тайн. Банковская тайна как вид защищаемой информации.

13. Врачебная тайна как вид защищаемой информации.

14. Адвокатская тайна как вид защищаемой информации. Нотариальная тайна как вид защищаемой информации.

Критерии и шкалы оценивания рефератов (докладов)

Оценка	Профессиональные компетенции	Отчетность
«отлично»	Работа выполнена на высоком профессиональном уровне. Полностью соответствует поставленным в задании целям и задачам. Представленный материал в основном верен, допускаются мелкие неточности. Студент свободно отвечает на вопросы, связанные с докладом. Выражена способность к профессиональной адаптации, интерпретации знаний из междисциплинарных областей	Письменно оформленный доклад (реферат) представлен в срок. Полностью оформлен в соответствии с требованиями
«хорошо»	Работа выполнена на достаточно высоком профессиональном уровне, допущены несколько существенных ошибок, не влияющих на результат. Студент отвечает на вопросы, связанные с докладом, но недостаточно полно. Уровень недостаточно высок. Допущены существенные ошибки, не существенно влияющие на конечное восприятие материала. Студент может ответить лишь на некоторые из заданных вопросов, связанных с докладом	Письменно оформленный доклад (реферат) представлен в срок, но с некоторыми недоработками
«удовлетворительно»	Уровень недостаточно высок. Допущены существенные ошибки, не существенно влияющие на конечное восприятие материала. Студент может ответить лишь на некоторые из заданных вопросов, связанных с докладом	Письменно оформленный доклад (реферат) представлен со значительным опозданием (более недели). Имеются отдельные недочеты в оформлении
«неудовлетворительно»	Работа выполнена на низком уровне. Допущены грубые ошибки. Ответы на связанные с докладом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале доклада	Письменно оформленный доклад (реферат) представлен со значительным опозданием (более недели). Имеются существенные недочеты в оформлении.

Критерии и шкалы оценивания презентации

Дескрипторы	Минимальный ответ «неудовлетвори-тельно»	Изложенный, раскрытый ответ «удовлетвори-тельно»	Законченный, полный ответ «хорошо»	Образцовый ответ «отлично»
Раскрытие проблемы	Проблема не раскрыта.	Проблема раскрыта не полностью.	Проблема раскрыта. Проведен анализ	Проблема раскрыта полностью. Проведен

	Отсутствуют выводы.	Выводы не сделаны и/или выводы не обоснованы.	проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы.	анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы.
Представление	Представляемая информация логически не связана. Не использованы профессиональные термины.	Представляемая информация не систематизирована и/или не последовательна. Использован 1-2 профессиональных термина.	Представляемая информация систематизирована и последовательна. Использовано более 2 профессиональных терминов.	Представляемая информация систематизирована, последовательна и логически связана. Использовано более 5 профессиональных терминов.
Оформление	Не использованы информационные технологии (PowerPoint). Больше 4 ошибок в представляемой информации.	Использованы информационные технологии (PowerPoint) частично. 3-4 ошибки в представляемой информации.	Использованы информационные технологии (PowerPoint). Не более 2 ошибок в представляемой информации.	Широко использованы информационные технологии (PowerPoint). Отсутствуют ошибки в представляемой информации.
Ответы на вопросы	Нет ответов на вопросы.	Только ответы на элементарные вопросы.	Ответы на вопросы полные и/или частично полные.	Ответы на вопросы полные с привидением примеров.

Индивидуальное творческое задание

Подготовить презентацию в Microsoft PowerPoint (от 15 до 30 слайдов) на тему из списка (согласно журналу):

1. Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.
2. Основы авторского права.
3. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.
4. Защита объектов промышленной собственности на основе патентов.
5. Основные положения патентного права.
6. Организационно-правовая система обеспечения защиты объектов промышленной собственности на основе патентов.
7. Юридическая ответственность за нарушение правовых норм защиты информации.
8. Понятие юридической ответственности за нарушение правовых норм в области информационной безопасности.
9. Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
10. Характеристика отдельных видов юридической ответственности в сфере защиты информации.
11. Уголовная ответственность за нарушение правовых норм в сфере защиты информации.
12. Административная ответственность за нарушения правовых норм в сфере защиты информации.
13. Особенности юридической ответственности за нарушения норм защиты информации в области трудовых и гражданско-правовых отношений.
14. Уголовно-правовая ответственность за противоправные действия в сфере защиты информации.
15. Понятие и задачи государственной системы обеспечения информационной безопасности в РФ.

16. Структура государственной системы информационной безопасности в РФ.
17. Организационная основа системы информационной безопасности РФ.
18. Полномочия органов государственной власти Российской Федерации в области обеспечения информационной безопасности.
19. Система лицензирования в области защиты информации.
20. Основные понятия и положения системы государственного лицензирования.
21. Организационная структура системы государственного лицензирования.
22. Система сертификации в области защиты информации.
23. Основные понятия и система сертификации продукции и услуг.
24. Особенности сертификации средств защиты информации.
25. Ответственность за правонарушения в сфере лицензирования и сертификации.
26. Особенности лицензирования и сертификации в области защиты информации.
27. Организационные аспекты получения лицензии на занятие деятельностью в сфере обеспечения информационной безопасности.
28. Организационные аспекты получения сертификата соответствия на средства защиты информации.

Критерии и шкалы оценивания индивидуального задания

Критерии оценивания	Оценка
Задание не выполнено или допущены существенные неточности	«неудовлетворительно»
Задание выполнено не в полном объеме или полученные результаты недостаточно аргументированы, нарушена логика и последовательность изложения результатов	«удовлетворительно»
Задание выполнено в полном объеме, полученные результаты логичны, последовательны, но аргументированы недостаточно четко	«хорошо»
Задание выполнено в полном объеме, полученные результаты аргументированы, логичны, последовательны	«отлично»

Блок В
ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Перечень вопросов для подготовки к зачету

1. Что такое информационная безопасность?
2. Что относится к основным принципам обеспечения безопасности?
3. Что относится к национальным интересам в информационной сфере?
4. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?
5. Что такое правовое обеспечение информационной безопасности?
6. Дайте определение информационным правоотношениям.
7. Перечислите основные концептуальные документы в области информационной безопасности.
8. Каково содержание Конституции Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности?
9. Что понимается под информационной сферой как сферой правового регулирования?
10. Приведите известные Вам понятия «информация».
11. Что такое защищаемая информация и каковы ее отличительные признаки?
12. Перечислите известные Вам критерии классификации защищаемой информации.
13. К какой информации не может быть ограничен доступ?
14. Какие сведения относятся к информации с ограниченным доступом?
15. Что понимается под термином «государственная тайна»?
16. Что понимается под информационной сферой как сферой правового регулирования?
17. Приведите известные Вам понятия «информация».
18. Что такое защищаемая информация и каковы ее отличительные признаки?
19. Перечислите известные Вам критерии классификации защищаемой информации.
20. К какой информации не может быть ограничен доступ?
21. Какие сведения относятся к информации с ограниченным доступом?
22. Что понимается под термином «государственная тайна»?
23. Перечислите социальные гарантии, установленные для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе.
24. Перечислите основания для отказа гражданину в допуске государственной тайне.
25. Перечислите основания прекращения допуска к государственной тайне.
26. Что понимается под термином «персональные данные»?
27. Какими нормативными документами регулируются вопросы защиты персональных данных?
28. Раскройте содержание основных категорий персональных данных?
29. Что понимается под термином «информация, составляющая служебную тайну»?
30. Какими нормативными документами регулируются вопросы защиты служебной тайны?
31. Что понимается под термином «информация, составляющая коммерческую тайну»?
32. Какими нормативными правовыми документами регулируются вопросы защиты коммерческой тайны?
33. Какая информация относится к категории профессиональная тайна?
34. Каковы особенности защиты программ для ЭВМ и баз данных институтом авторского права?

35. Перечислите объекты патентного права.

36. Приведите составы преступлений в области информационной безопасности, предусмотренные УК РФ.

37. Приведите составы правонарушений, предусмотренные КоАП РФ.

38. Дайте определение системы обеспечения информационной безопасности.

39. Перечислите задачи государственных органов в рамках деятельности по обеспечению информационной безопасности.

40. Что составляет организационную основу системы обеспечения информационной безопасности?

41. Перечислите полномочия Совета Федерации Федерального Собрания Российской Федерации в сфере обеспечения информационной безопасности.

42. Перечислите полномочия Государственной Думы Федерального Собрания Российской Федерации в сфере обеспечения информационной безопасности.

43. Перечислите полномочия Совета безопасности Российской Федерации в сфере обеспечения информационной безопасности.

44. Назовите функции Правительства Российской Федерации в области информационной безопасности.

45. Охарактеризуйте состав Межведомственной Комиссия по защите государственной тайны.

46. Полномочия Федеральной службы по техническому и экспортному контролю в сфере обеспечения информационной безопасности Российской Федерации.

47. Полномочия Роскомнадзора в сфере обеспечения информационной безопасности Российской Федерации.

Шкала оценивания

Экзамен	**Критерии оценивания**
«Отлично»	Сформированные и систематические знания; успешные и систематические умения; успешное и систематическое применение навыков
«Хорошо»	Сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие пробелы умения; в целом успешное, но сопровождающееся отдельными ошибками применение навыка
«Удовлетворительно»	Неполные знания; в целом успешное, но несистематическое умение; в целом успешное, но несистематическое применение навыков
«Неудовлетворительно»	Фрагментарные знания, умения и навыки / отсутствуют знания, умения и навыки

Приложение 1

Лист визирования фонда оценочных средств
на очередной учебный год

Фонд оценочных средств по дисциплине «Административно-правовые основы информационной безопасности РФ» проанализирован и признан актуальным для использования на 20__- 20__ учебный год.

Протокол заседания кафедры юриспруденции от «__» _____ 20__ г. № __

Заведующий кафедрой юриспруденции _____ _____
«____» _____20__ г.

Фонд оценочных средств по дисциплине «Административно-правовые основы информационной безопасности РФ» проанализирован и признан актуальным для использования на 20__- 20__ учебный год.

Протокол заседания кафедры юриспруденции от «__» _____ 20__ г. № __

Заведующий кафедрой юриспруденции _____ _____
«____» _____20__ г.

КОМПЛЕКТ ИТОГОВЫХ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

ОПК-8. Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований

ОПК-8.2. Умеет использовать полученную информацию для решения задач профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности деятельности.
ОПК-8.3. Владеет навыками систематизации и обобщения полученной информации с применением информационных технологий и с учетом требований информационной безопасности

Задание закрытого типа

1 (ОПК-8.2.)

Прочитайте текст, установите соответствие и запишите аргументы, обосновывающие выбор ответа

Установите соответствие между терминами и их определениями в области административно-правового регулирования информационной безопасности

К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца:

Термины	**Определения**
1) информационная безопасность 2) административное регулирование 3) угрозы информационной безопасности 4) нормативные акты в сфере информационной безопасности	А) правовые документы, устанавливающие требования и правила в области защиты информации. Б) комплекс мер, направленных на защиту информации от несанкционированного доступа, разрушения или изменения. В) действия или события, способные нанести ущерб информационным системам и данным. Г) процесс управления и контроля за соблюдением норм и правил в области информационной безопасности.

Запишите выбранные цифры под соответствующими буквами:

А	***Б***	***В***	***Г***

Ответ:1234

Обоснование: перечень сведений, отнесённых к государственной тайне, указан в специальном перечне, утверждённом законом РФ от 21.07.1993

	Закон РФ "О государственной тайне"
2 (ОПК-8.3.)	*Прочитайте текст и выберите один правильный вариант ответа* *Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа* **Какой закон регулирует информационные отношения?** 1) Федеральный закон «Об информационных технологиях и о защите информации» 2) Федеральный закон «Об информации, информационных технологиях и о защите информации» 3) Федеральный закон «Об информации и о защите информации» 4) Федеральный закон «О защите информации» *Ответ:2* *Обоснование: Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 регулирует информационные отношения в Российской Федерации*
3 (ОПК-8.3.)	*Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа* ***Информационно-телекоммуникационная сеть это*** *1) технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники* *2) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов* *3) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам* *4) информация, переданная или полученная пользователем информационно-телекоммуникационной сети* *Ответ:1* *Обоснование: на основании ст.2 Федерального закона «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть это - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники*
4 (ОПК-8.2.)	*Прочитайте текст и установите последовательность* **При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую из?** 1) механизмы генерации новых решений 2) реагировать на угрозы информационной безопасности 3) предвидеть новые угрозы 4) уметь им противостоять

Ответ:1234

5 (ОПК-8.2.)

Прочитайте текст и установите последовательность

Установите правильную последовательность этапов административно-пра информационной безопасности.

1) оценка рисков и уязвимостей информационных систем
2) разработка и внедрение мер по обеспечению информационной безопасности
3) проведение аудита и мониторинга соблюдения мер безопасности
4) формирование и утверждение нормативных актов и стандартов в области инф

Ответ:4231

6 (ОПК-8.3)

Прочитайте текст и установите соответствие

Установите соответствие между понятием и содержанием, с которыми они связаны

К каждой позиции, данной в первом столбце, подберите соответствующую позицию из второго столбца

Понятие	Содержание
1) Обеспечение доступности информации 2) Обеспечение целостности информации 3) Обеспечение конфиденциальности информации 4) Физическая защита информации	А) одна из базовых составляющих информационной безопасности, гарантирует, что информация существует в своём исходном виде, то есть при её хранении или передаче не было произведено несанкционированных изменений Б) это защита информации от её несанкционированного раскрытия, использования или изменения третьими лицами без согласия её владельца В) включает в себя контроль доступа к серверам, хранилищам и другим информационным ресурсам, а также контроль целостности оборудования Г) это одна из составляющих информационной безопасности, которая заключается в гарантии получения требуемой информации или информационной услуги пользователем за определённое время

Запишите выбранные цифры за соответствующими буквами (без пробелов)

А	Б	В	Г

Ответ:2341

Задание открытого типа

7 *Прочитайте текст, установите последовательность и запишите*

(ОПК-8.2.)	*аргументы, обосновывающие выбор ответа* **Установите последовательность этапов процесса административно-правового регулирования информационной безопасности** 1) оценка рисков информационной безопасности 2) разработка нормативных актов 3) внедрение мер по защите информации 4) мониторинг и контроль за соблюдением норм 5) обучение сотрудников *Ответ:12345*
8 (ОПК-8.2.)	*Дайте ответ на вопрос в свободной форме* ***Компьютерная безопасность зависит?*** *Ответ: зависит от системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающего персонала.* *Обоснование: согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал*
9 (ОПК-8.3.)	*Дайте правильный ответ и запишите аргументы, обосновывающие выбор ответа* **Верно ли утверждение, что документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности – это «Оранжевая книга»**? *Ответ: да, верно.* *Обоснование: Потому что «Оранжевая книга» поясняет понятие безопасной системы, которая «управляет доступом к информации так, что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию».*
10 (ОПК-8.3.)	*Вставьте в текст пропущенные слова* **Федеральный закон «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении _____ _____, обеспечении защиты информации** *Ответ: информационных технологий*
11 (ОПК-	*Прочитайте текст и дополните предложение* **Аутентификация и контроль доступа для обеспечения безопасности конфи в информационной системе организации, необходимо организоват пользователей и управлять доступом к ней.**

8.3.)	*Ответ: аутентификацию*
12 (ОПК-8.2.)	*Дополните предложение* **_____ информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации** **Информационная безопасность автоматизированной системы – это состояние автоматизированной системы,** *Ответ: Общедоступная*
13 (ОПК-8.2)	*Дайте ответ на вопрос в свободной форме* **Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)** *Ответ: МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения*
14 (ОПК-8.2.)	*Дайте правильный ответ и запишите аргументы, обосновывающие выбор ответа* ***Верно ли утверждение, что*** **разделы современной криптографии – это симметричные криптосистемы; криптосистемы с открытым ключом; системы электронной подписи; управление ключами?** *Ответ: да, верно.* *Обоснование: Потому, что криптография — это уникальная и незаменимая область знаний, которая играет важную роль в современном мире. Ее основными задачами являются защита информации, обеспечение безопасности в онлайн-пространстве и коммуникациях. Исследования в этой области позволяют создавать надежные алгоритмы шифрования, которые защищают данные от несанкционированного доступа.*
15 (ОПК-8.3.)	*Дайте краткий ответ на вопрос в свободной форме* **Основные угрозы доступности информации:** *Правильный ответ: непреднамеренные ошибки пользователей; отказ программного и аппаратно обеспечения; разрушение или повреждение помещений*
16 (ОПК-8.3.)	*Дайте ответ на вопрос в свободной форме* **Методы повышения достоверности входных данных** *Правильный ответ: Замена процесса ввода значения процессом выбора значения из предлагаемого множества; использование вместо ввода значения его считывание с машиночитаемого носителя; введение избыточности в документ первоисточник*

17 (ОПК-8.2.)	*Дайте ответ на вопрос в свободной форме* **Назовите сервисы безопасности:** *Правильный ответ: идентификация и аутентификация; шифрование; контроль целостности; экранирование; обеспечение безопасного восстановления*
18 (ОПК-8.2.)	*Дайте ответ на вопрос в свободной форме* **Причины возникновения ошибки в данных** *Правильный ответ: погрешность измерений; ошибка при записи результатов измерений в промежуточный документ; ошибки при переносе данных с промежуточного документа в компьютер; преднамеренное искажение данных; ошибки при идентификации объекта или субъекта хозяйственной деятельности*
19 (ОПК-8.2.)	*Дайте правильный ответ и запишите аргументы, обосновывающие выбор ответа* **Верно ли утверждение, что документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности – это «Оранжевая книга»** *Правильный ответ: да, верно.* *Обоснование: Потому что «Оранжевая книга» поясняет понятие безопасной системы, которая «управляет доступом к информации так, что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию».*
20 (ОПК-8.2.)	*Дайте правильный ответ и запишите аргументы, обосновывающие выбор ответа* **Верно ли утверждение, что разделы современной криптографии – это симметричные криптосистемы; криптосистемы с открытым ключом; системы электронной подписи; управление ключами** *Правильный ответ: да, верно.* *Обоснование: Потому, что криптография — это уникальная и незаменимая область знаний, которая играет важную роль в современном мире. Ее основными задачами являются защита информации, обеспечение безопасности в онлайн-пространстве и коммуникациях. Исследования в этой области позволяют создавать*

	надежные алгоритмы шифрования, которые защищают данные от несанкционированного доступа.