МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

зав.кафедрой, д.т.н.,проф.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)

(подпись)
«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности/ специализации	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

ст. преподаватель	20.02.26	В.С. Беззатеева
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф.	20.02.26	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н.	20.02.26	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности/специализации «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

УК-2 «Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений»

ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности»

ОПК-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

ОПК-10 «Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты»

Содержание дисциплины охватывает круг вопросов, связанных с теоретическими основами информационной безопасности, правовым регулированием защиты информации, организацией защиты информации ограниченного доступа, персональных данных, коммерческой и государственной тайны, охраной результатов интеллектуальной деятельности, формированием политики информационной безопасности, разработкой локальных актов, физической защитой объекта, пропускным и внутриобъектовым режимами, контролем и аудитом мер защиты.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия и самостоятельную работу обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (8 семестр).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания дисциплины в системе подготовки по направлению подготовки 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем» является получение обучающимися знаний, умений и навыков в области правового и организационного обеспечения информационной безопасности, применения нормативных правовых актов, стандартов и методических документов, разработки локальных актов организации, выбора организационных и режимных мер защиты информации ограниченного доступа, формирования политики ИБ и управления реализацией комплекса мер защиты.

1.2. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Универсальные компетенции	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.З.2 знать действующее законодательство и правовые нормы, регулирующие профессиональную деятельность УК-2.У.2 уметь использовать нормативную и правовую документацию УК-2.В.1 владеть навыками выбора оптимального способа решения задач с учетом действующих правовых норм
Общепрофессиональные компетенции	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.З.1 знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации ОПК-5.З.2 знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации ОПК-5.З.3 знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений

		в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации ОПК-5.З.4 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-5.У.1 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав ОПК-5.У.2 умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ОПК-5.У.3 умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации ОПК-5.У.4 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.В.1 владеет навыками работы с нормативными документами, государственными и международными стандартами в области информационной безопасности и защиты информации
Общепрофессиональные компетенции	ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и	ОПК-6.З.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации ОПК-6.З.2 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях ОПК-6.З.3 знает систему организационных мер, направленных на

	методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	защиту информации ограниченного доступа ОПК-6.З.4 знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа ОПК-6.У.4 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации ОПК-6.В.1 владеет навыками применения нормативных правовых актов, нормативных и методических документов при организации системы защиты информации
Общепрофессиональные компетенции	ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.З.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- «Информационное право»,
- «Основы информационной безопасности»,

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- «Производственная практика научно исследовательская работа»,
- « Производственная преддипломная практика»,
- «Государственная итоговая аттестация».

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки		
Аудиторные занятия, всего час.	40	40
в том числе:		
лекции (Л), (час)	20	20
практические/семинарские занятия (ПЗ), (час)	20	20
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	32	32
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет,	Зачет,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий. Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 8					
Раздел 1. Теоретические и нормативные основы обеспечения информационной безопасности. Тема 1.1. Информационное общество и информационная безопасность. Тема 1.2. Система обеспечения ИБ РФ и организации. Тема 1.3. Источники правового регулирования в области информации и защиты информации. Тема 1.4. Субъекты, регуляторы и полномочия органов государственной власти.	6	6			10
Раздел 2. Правовое обеспечение защиты информации и ответственности. Тема 2.1. Правовые режимы информации ограниченного доступа. Тема 2.2. Защита персональных данных и конфиденциальной информации. Тема 2.3. Охрана РИД, электронная подпись и электронное взаимодействие. Тема 2.4. Лицензирование, сертификация и аттестация. Тема 2.5. Юридическая и дисциплинарная ответственность.	7	7			11

Раздел 3. Организационное обеспечение ИБ на объекте защиты. Тема 3.1. Политика ИБ и локальное нормативное регулирование. Тема 3.2. Организационные меры защиты информации ограниченного доступа. Тема 3.3. Физическая защита объекта, пропускной и внутриобъектовый режимы. Тема 3.4. Управление персоналом, контроль, аудит и корректирующие мероприятия.	7	7			11
Итого в семестре:	20	20	0	0	32
Итого	20	20	0	0	32

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
Раздел 1.	Раздел 1. Теоретические и нормативные основы обеспечения информационной безопасности: введение в понятийный аппарат дисциплины, раскрытие связи между информационным обществом и информационной безопасностью, формирование представления о системе правового регулирования и о роли регуляторов. Тема 1.1. Информационное общество и информационная безопасность. Понятие информационного общества. Содержание информационной сферы. Значение информационной безопасности для личности, общества и государства. Информация как стратегический ресурс. Понятия угрозы, уязвимости и защиты. Конфиденциальность, целостность и доступность как базовые свойства информации. Лекция-беседа с разбором примеров угроз. Тема 1.2. Система обеспечения ИБ РФ и организации. Строение системы обеспечения ИБ. Уровни управления безопасностью. Место организации в государственной системе защиты информации. Силы и средства обеспечения ИБ. Государственный, отраслевой и объектовый уровни. Функции руководства, службы ИБ, ИТ, юриста и кадровой службы. Документы, координирующие защиту информации. Тема 1.3. Источники правового регулирования в области информации и защиты информации. Иерархии источников права. Конституция РФ и федеральные законы, подзаконные акты, стандарты и методические документы. Соотношение общих и

Номер раздела	Название и содержание разделов и тем лекционных занятий
	специальных норм. Локальные акты организации. Тема 1.4. Субъекты, регуляторы и полномочия органов государственной власти. Система регуляторов: пределы их компетенции, взаимодействие публичных субъектов и организаций. Полномочия Президента РФ и Правительства РФ. Компетенция ФСТЭК России, ФСБ России, Роскомнадзора. Обладатель информации, оператор персональных данных, владелец информационной системы. Контроль и надзор.
Раздел 2.	Раздел 2. Правовое обеспечение защиты информации и ответственности: Специальные правовые режимы информации ограниченного доступа, требования к персональным данным, РИД и электронному документообороту, процедуры лицензирования, сертификации, аттестации и виды ответственности. Тема 2.1. Правовые режимы информации ограниченного доступа. Правовые режимы сведений ограниченного доступа. Различия в мерах защиты для разных категорий сведений. Государственная тайна, коммерческая тайна, служебная и профессиональная тайны. Доступ, хранение, передача и уничтожение носителей. Тема 2.2. Защита персональных данных и конфиденциальной информации. Обязанности оператора, требования к законной обработке и защите персональных данных. Понятие персональных данных. Принципы и основания обработки, согласие субъекта, права субъектов и обязанности оператора, организационные меры и внутренний контроль. Лекция-дискуссия по анализу разновидностей персональных данных и рисков, связанных с их обработкой в организации. Тема 2.3. Охрана РИД, электронная подпись и электронное взаимодействие. Правовые инструменты защиты результатов интеллектуальной деятельности. Условия юридически значимого электронного взаимодействия. Результаты интеллектуальной деятельности и ноу-хау. Электронный документ и его юридическая сила. Виды электронной подписи. Удостоверяющие центры. Доказательственная сила электронных документов. Тема 2.4. Лицензирование, сертификация и аттестация. Смысл разрешительных и подтверждающих процедур, место этих процедур в жизненном цикле объекта защиты. Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации. Аттестация объектов информатизации. Цели процедур и комплект документов. Тема 2.5. Юридическая и дисциплинарная ответственность. Квалификация нарушений требований защиты информации, правовые последствия инцидентов. Дисциплинарная, гражданско-правовая, административная

Номер раздела	Название и содержание разделов и тем лекционных занятий
	и уголовная ответственность. Нарушение режима конфиденциальности. Неправомерный доступ к информации. Служебное расследование.
Раздел 3.	Раздел 3. Организационное обеспечение ИБ на объекте защиты: практическая организация защиты информации на объекте информатизации. Разработка локальных регламентов и режимных мер. Увязка физической защиты, кадровой безопасности, контроля и аудита в единую систему. Тема 3.1. Политика ИБ и локальное нормативное регулирование. проектирование базового комплекта локальных документов. Юридическая и управленческая роль политики ИБ. Политика ИБ. Положения, инструкции и регламенты. Разграничение доступа. Обращение с носителями. Реагирование на инциденты. Связь локальных актов с требованиями регуляторов. Тема 3.2. Организационные меры защиты информации ограниченного доступа. Организационные меры защиты, их применение на уровне процессов и рабочих мест. Классификация информации. Разграничение прав доступа. Учет носителей. Журналирование действий. Резервное копирование. Инвентаризация активов. Инструктаж и регистрация инцидентов. Лекция с разбором конкретного инцидента: построение организационно-правовой системы для защиты информации ограниченного доступа. Тема 3.3. Физическая защита объекта, пропускной и внутриобъектовый режимы. Физическая безопасность как элемент комплексной защиты информации. Режимные меры и правовой режим защищаемых сведений. Зонирование помещений, пропускной режим, сопровождение посетителей. Хранение бумажных и электронных носителей. Защита переговорных. Чистое рабочее место. Контроль печати и копирования. Тема 3.4. Управление персоналом, контроль, аудит и корректирующие мероприятия. Роли кадровой безопасности. Значение внутреннего контроля, аудита и корректирующих мер. Кадровые риски. Допуск и обязательства о неразглашении. Обучение и повышение осведомленности. Увольнение и отзыв прав доступа. Внутренний контроль. Аудит соответствия. Корректирующие и предупреждающие мероприятия. Лекция с разбором конкретных ситуаций по выявлению нарушений режима внутреннего контроля и ацдита.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 8					
1	Нормативные основы обеспечения информационной безопасности	Комментированное чтение нормативных актов, групповая дискуссия, решение ситуационных задач, построение схемы регуляторов.	4	4	1
2	Правовые режимы информации ограниченного доступа	Кейс-анализ, разработка перечня сведений ограниченного доступа, подготовка фрагмента локального акта.	4	4	2
3	Лицензирование, сертификация, аттестация, электронная подпись	Решение практических задач, сопоставление процедур, подготовка схемы документального сопровождения.	4	4	2
4	Политика ИБ и локальные акты организации	Игровое проектирование, разработка структуры политики ИБ, проекта приказа и регламента доступа.	4	4	3
5	Физическая защита, пропускной режим, контроль и аудит	Моделирование реальных условий, анализ схемы объекта, подготовка корректирующих мероприятий.	4	4	3
Всего			20	20	20

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				

Всего			

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 8, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	12	12
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	6	6
Домашнее задание (ДЗ)	8	8
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	6	6
Всего:	32	32

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
https://urait.ru/bcode/584372	Организационное и правовое обеспечение информационной безопасности : учебник / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — ISBN 978-5-534-19107-3.	
https://urait.ru/bcode/588741	Зенков, А. В. Информационная	

	безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9.	
https://urait.ru/bcode/590417	Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 190 с. — (Высшее образование). — ISBN 978-5-534-17864-7.	
https://urait.ru/bcode/588515	Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3.	
https://urait.ru/bcode/589232	Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебник для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 50 с. — (Высшее образование). — ISBN 978-5-534-19364-0.	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
https://urait.ru/	Образовательная платформа Юрайт
https://znanium.ru/	Электронно-библиотечная система Znanium
https://e.lanbook.com/	Электронно-библиотечная система «Лань»
https://fstec.ru/	Официальный сайт ФСТЭК России
https://fsb.ru/	Официальный сайт ФСБ России
https://rkn.gov.ru/	Официальный сайт Роскомнадзора
http://www.edou.ru/enc/docs/detail.php?ID=2489&PAGEN_1=3	Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления
http://www.cntd.ru/	Портал центра нормативно-технической документации
http://www.gostedu.ru/	Портал стандартов

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория — укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации.	
2	Мультимедийная лекционная аудитория — укомплектована электронными средствами обучения, обеспечивающими демонстрацию презентаций, учебных фильмов и иных материалов.	
3	Компьютерный класс для проведения практических занятий — укомплектован специализированной (учебной) мебелью, компьютерной техникой, программным обеспечением, возможностью подключения к сети «Интернет» и доступом к ЭИОС ГУАП.	
4	Помещение для самостоятельной работы — укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду организации.	
5	Аудитория для промежуточной аттестации — укомплектована специализированной (учебной) мебелью и техническими средствами обучения.	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты;

	Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий**.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий**.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора

	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1.	Назовите основные нормативные правовые акты и правовые нормы, регулирующие профессиональную деятельность специалиста в области организационного и правового обеспечения информационной безопасности.	УК-2.З.2
2.	Раскройте значение действующего законодательства при определении задач по обеспечению информационной безопасности организации.	УК-2.З.2
3.	Охарактеризуйте роль правовых норм при выборе организационных, технических и режимных мер защиты информации ограниченного доступа.	УК-2.З.2
4.	Перечислите основные правовые ограничения, которые необходимо учитывать при обработке персональных данных, коммерческой тайны, служебной информации и иных сведений ограниченного доступа.	УК-2.З.2
5.	Установите соответствие между правовой нормой или нормативным актом и сферой его применения: 1) Федеральный закон «Об информации, информационных технологиях и о защите информации»; 2) Федеральный закон «О персональных данных»; 3) Федеральный закон «О коммерческой тайне»; 4) Закон Российской Федерации «О государственной тайне»; 5) Федеральный закон «Об электронной подписи». А. Регулирование применения электронной подписи в электронном взаимодействии. Б. Установление режима коммерческой тайны в организации. В. Общие требования к информации, информационным технологиям и защите информации. Г. Правовой режим сведений, составляющих государственную тайну. Д. Требования к обработке и защите персональных данных. Запишите соответствующую последовательность букв.	УК-2.З.2
6.	Составьте пример перечня нормативных и правовых документов, которые необходимо использовать при решении задачи по организации защиты информации ограниченного доступа в организации.	УК-2.У.2
7.	Сформулируйте запрос в юридическое подразделение организации о предоставлении актуальных нормативных правовых актов, необходимых для разработки локального регламента по защите информации.	УК-2.У.2
8.	Опишите порядок использования нормативной и правовой документации при подготовке политики информационной безопасности организации.	УК-2.У.2
9.	Покажите, как использовать нормативные правовые акты и	УК-2.У.2

	методические документы при выборе мер защиты персональных данных в информационной системе организации.	
10.	Решите практическую задачу. Организация планирует внедрить систему электронного документооборота, в которой будут обрабатываться персональные данные работников и сведения ограниченного доступа. Определите, какие нормативные и правовые документы необходимо использовать, какие правовые ограничения учесть и какие локальные документы подготовить.	УК-2.У.2
11.	Продемонстрируйте навыки выбора оптимального способа решения задачи по защите информации ограниченного доступа с учетом действующих правовых норм, ресурсов организации и имеющихся ограничений.	УК-2.В.1
12.	Разработайте вариант решения задачи по организации доступа работников к сведениям ограниченного доступа, учитывая требования законодательства, должностные обязанности работников и принцип минимально необходимого доступа.	УК-2.В.1
13.	Смоделируйте ситуацию выбора между несколькими способами защиты информации в организации и обоснуйте оптимальный вариант с учетом действующих правовых норм, ресурсов и ограничений.	УК-2.В.1
14.	Оцените правомерность выбранного организацией способа защиты информации, если доступ к сведениям ограниченного доступа предоставляется всем работникам подразделения без анализа их должностных обязанностей и без оформления локальных документов.	УК-2.В.1
15.	Установите верную последовательность действий при выборе оптимального способа решения задачи в области информационной безопасности: А. Выявить правовые нормы и ограничения, применимые к задаче. Б. Определить цель и круг задач по обеспечению информационной безопасности. В. Оценить имеющиеся ресурсы организации. Г. Сравнить возможные способы решения задачи. Д. Выбрать оптимальный способ решения с учетом правовых норм, ресурсов и ограничений. Е. Оформить принятое решение в локальном документе или служебном предложении. Запишите соответствующую последовательность букв.	УК-2.В.1
16.	Назовите основные элементы российской правовой системы, которые необходимо учитывать при организационном и правовом обеспечении информационной безопасности организации.	ОПК-5.З.1
17.	Раскройте значение Конституции Российской Федерации, федеральных законов, подзаконных актов и локальных нормативных актов в регулировании профессиональной деятельности специалиста по информационной безопасности.	ОПК-5.З.1
18.	Охарактеризуйте правовой статус личности при обработке	ОПК-5.З.1

	и защите информации: основные права, свободы, обязанности и гарантии защиты прав субъектов информационных отношений.	
19.	Перечислите органы государственной власти Российской Федерации, участвующие в регулировании информационной безопасности, защиты информации, персональных данных и сведений ограниченного доступа.	ОПК-5.3.1
20.	Установите соответствие между субъектом правового регулирования и его ролью в сфере информационной безопасности: 1) Президент Российской Федерации; 2) Правительство Российской Федерации; 3) ФСТЭК России; 4) ФСБ России; 5) Роскомнадзор. А) организация контроля и надзора за соблюдением законодательства о персональных данных; Б) определение основных направлений государственной политики в сфере безопасности; В) нормативное и методическое регулирование технической защиты информации; Г) обеспечение реализации государственной политики и координация деятельности федеральных органов исполнительной власти; Д) регулирование вопросов криптографической защиты информации в пределах компетенции. Запишите соответствующую последовательность букв.	ОПК-5.3.1
21.	Назовите основные отрасли российского права, нормы которых применяются в профессиональной деятельности организации при обеспечении информационной безопасности.	ОПК-5.3.2
22.	Раскройте значение административного, гражданского, трудового и уголовного права при организации защиты информации и привлечении нарушителей к ответственности.	ОПК-5.3.2
23.	Охарактеризуйте основные понятия информационного права, используемые при обеспечении информационной безопасности: информация, информационная система, обладатель информации, доступ к информации, защита информации.	ОПК-5.3.2
24.	Перечислите правовые режимы информации, которые могут использоваться в профессиональной деятельности организации: общедоступная информация, конфиденциальная информация, персональные данные, коммерческая тайна, государственная тайна.	ОПК-5.3.2
25.	Установите соответствие между отраслью права и сферой ее применения в деятельности организации: 1) трудовое право; 2) гражданское право; 3) административное право; 4) уголовное право; 5) информационное право.	ОПК-5.3.2

	А) ответственность за неправомерный доступ к компьютерной информации; Б) оформление обязанностей работника по неразглашению защищаемой информации; В) регулирование отношений, связанных с информацией, информационными технологиями и защитой информации; Г) защита исключительных прав и договорное регулирование передачи прав; Д) административная ответственность за нарушение требований защиты информации. Запишите соответствующую последовательность букв.	
26.	Назовите основные нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации.	ОПК-5.3.3
27.	Раскройте правовые основы организации защиты государственной тайны, конфиденциальной информации и информации ограниченного доступа в организации.	ОПК-5.3.3
28.	Охарактеризуйте правовую характеристику преступлений в сфере компьютерной информации и их значение для организации защиты автоматизированных информационных систем.	ОПК-5.3.3
29.	Перечислите меры правовой и дисциплинарной ответственности за разглашение защищаемой информации, нарушение режима конфиденциальности и неправомерный доступ к информации.	ОПК-5.3.3
30.	Установите соответствие между видом нарушения и возможной мерой ответственности: 1) разглашение коммерческой тайны работником; 2) неправомерный доступ к компьютерной информации; 3) нарушение требований обработки персональных данных; 4) несоблюдение локальной инструкции по защите информации; 5) разглашение сведений, составляющих государственную тайну. А) дисциплинарная ответственность; Б) административная ответственность в сфере персональных данных; В) уголовная ответственность за компьютерное преступление; Г) ответственность за нарушение режима коммерческой тайны; Д) ответственность за разглашение государственной тайны. Запишите соответствующую последовательность букв.	ОПК-5.3.3
31.	Назовите правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности в организации.	ОПК-5.3.4
32.	Раскройте обязанности оператора персональных данных при их обработке, хранении, передаче, уничтожении и обеспечении безопасности.	ОПК-5.3.4
33.	Охарактеризуйте правовой режим результатов	ОПК-5.3.4

	интеллектуальной деятельности, служебных произведений, программ для ЭВМ, баз данных и ноу-хау в деятельности организации.	
34.	Перечислите локальные документы, необходимые для организации защиты персональных данных и охраны результатов интеллектуальной деятельности в организации.	ОПК-5.З.4
35.	Установите соответствие между правовым объектом и его содержанием: 1) персональные данные; 2) оператор персональных данных; 3) результат интеллектуальной деятельности; 4) коммерческая тайна; 5) ноу-хау. А) сведения, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности третьим лицам; Б) информация, относящаяся к прямо или косвенно определенному физическому лицу; В) лицо, организующее и осуществляющее обработку персональных данных; Г) охраняемый результат творческой деятельности; Д) сведения любого характера, охраняемые как секрет производства при соблюдении режима конфиденциальности. Запишите соответствующую последовательность букв.	ОПК-5.З.4
36.	Составьте пример обоснования управленческого решения о введении режима коммерческой тайны в организации с учетом правовых норм и должностных обязанностей работников.	ОПК-5.У.1
37.	Сформулируйте запрос в юридическое подразделение организации о правовой оценке мер по защите персональных данных и восстановлению нарушенных прав субъекта персональных данных.	ОПК-5.У.1
38.	Опишите порядок действий специалиста по информационной безопасности при выявлении нарушения режима защиты конфиденциальной информации в пределах его должностных обязанностей.	ОПК-5.У.1
39.	Покажите, как использовать правовые нормы при подготовке служебного предложения о восстановлении нарушенных прав организации после утечки сведений ограниченного доступа.	ОПК-5.У.1
40.	Решите практическую задачу. Работник организации передал файл, содержащий персональные данные клиентов и коммерческую информацию, через личную электронную почту. Обоснуйте правовую оценку ситуации, определите применимые нормы, меры реагирования и действия по восстановлению нарушенных прав.	ОПК-5.У.1
41.	Составьте пример структуры локального правового акта, регламентирующего работу по обеспечению информационной безопасности в организации.	ОПК-5.У.2
42.	Сформулируйте запрос руководителю подразделения о	ОПК-5.У.2

	предоставлении сведений, необходимых для разработки проекта инструкции по защите информации ограниченного доступа.	
43.	Опишите порядок анализа действующих локальных актов организации на соответствие требованиям законодательства, нормативных и методических документов в области защиты информации.	ОПК-5.У.2
44.	Покажите, как использовать результаты анализа рисков и требований регуляторов при разработке проекта регламента доступа к информационной системе организации.	ОПК-5.У.2
45.	Решите практическую задачу. В организации отсутствует политика информационной безопасности, инструкция по обращению с информацией ограниченного доступа и регламент реагирования на инциденты. Разработайте предложения по составу локальных актов, их структуре и порядку утверждения.	ОПК-5.У.2
46.	Составьте пример перечня исходных данных, необходимых для подготовки к лицензированию деятельности в области технической защиты конфиденциальной информации.	ОПК-5.У.3
47.	Сформулируйте запрос в ответственное подразделение о предоставлении документов, необходимых для сертификации средства защиты информации или аттестации объекта информатизации по требованиям безопасности информации.	ОПК-5.У.3
48.	Опишите порядок формулирования требований при лицензировании деятельности в области защиты информации, сертификации средств защиты и аттестации объектов информатизации.	ОПК-5.У.3
49.	Покажите, как использовать требования нормативных документов ФСТЭК России и ФСБ России при подготовке объекта информатизации к аттестации по требованиям безопасности информации.	ОПК-5.У.3
50.	Решите практическую задачу. Организация планирует выполнять работы по технической защите конфиденциальной информации и использовать сертифицированные средства защиты. Определите основные требования к лицензированию, сертификации, аттестации и комплекту подтверждающих документов.	ОПК-5.У.3
51.	Составьте пример перечня требований по защите конфиденциальной информации, персональных данных и результатов интеллектуальной деятельности в организации.	ОПК-5.У.4
52.	Сформулируйте запрос в кадровую службу о предоставлении информации, необходимой для определения мер защиты персональных данных работников.	ОПК-5.У.4
53.	Опишите порядок формулирования требований к защите персональных данных при их обработке в информационной системе организации.	ОПК-5.У.4
54.	Проанализируйте ситуацию, при которой служебная	ОПК-5.У.4

	разработка хранится в общей сетевой папке без разграничения доступа, и предложите требования по охране результатов интеллектуальной деятельности и защите конфиденциальной информации.	
55.	Решите практическую задачу. Организация обрабатывает персональные данные клиентов, ведет реестр коммерчески ценных сведений и разрабатывает программный продукт. Сформулируйте требования по защите персональных данных, конфиденциальной информации и охране результатов интеллектуальной деятельности.	ОПК-5.У.4
56.	Продемонстрируйте навыки поиска, отбора и применения нормативных документов, государственных и международных стандартов при решении задачи по организации защиты информации.	ОПК-5.В.1
57.	Разработайте фрагмент перечня нормативных документов и стандартов, применимых при формировании политики информационной безопасности организации.	ОПК-5.В.1
58.	Смоделируйте порядок работы специалиста с нормативной базой при подготовке проекта локального регламента защиты информации ограниченного доступа.	ОПК-5.В.1
59.	Оцените корректность применения нормативных документов, если организация при защите информационной системы учитывает только внутренние инструкции и не применяет федеральные законы, документы регуляторов и стандарты информационной безопасности.	ОПК-5.В.1
60.	Установите верную последовательность действий при работе с нормативными документами и стандартами в области информационной безопасности: А) определить объект защиты и вид обрабатываемой информации; Б) выявить применимые федеральные законы и подзаконные акты; В) определить применимые нормативные и методические документы регуляторов; Г) выбрать государственные и международные стандарты; Д) сформировать перечень требований к системе защиты информации; Е) отразить требования в локальной, проектной и эксплуатационной документации. Запишите соответствующую последовательность букв.	ОПК-5.В.1
61.	Назовите основные нормативные правовые акты и стандарты, регулирующие лицензирование деятельности в области защиты государственной тайны, технической защиты конфиденциальной информации, аттестацию объектов информатизации и сертификацию средств защиты информации.	ОПК-6.З.1
62.	Раскройте назначение процедур лицензирования, аттестации объектов информатизации и сертификации средств защиты информации в системе организационного и правового обеспечения информационной безопасности.	ОПК-6.З.1
63.	Охарактеризуйте роль стандартов и нормативных	ОПК-6.З.1

	документов при подтверждении соответствия средств защиты информации и объектов информатизации требованиям безопасности информации.	
64.	Перечислите основные этапы подготовки организации к лицензированию деятельности в области защиты информации и к аттестации объекта информатизации по требованиям безопасности информации.	ОПК-6.3.1
65.	Установите соответствие между процедурой и ее содержанием: 1) лицензирование деятельности по защите информации; 2) аттестация объекта информатизации; 3) сертификация средства защиты информации; 4) техническая защита конфиденциальной информации; 5) защита государственной тайны. А. Подтверждение соответствия объекта установленным требованиям безопасности информации. Б. Получение права на осуществление определенного вида деятельности при соблюдении установленных требований. В. Комплекс мер по предотвращению утечки, несанкционированного доступа и иных воздействий на защищаемую информацию. Г. Подтверждение соответствия средства защиты установленным требованиям. Д. Система правовых, организационных и режимных мер по защите сведений, составляющих государственную тайну. Запишите соответствующую последовательность букв.	ОПК-6.3.1
66.	Назовите основные задачи органов защиты государственной тайны и служб защиты информации на предприятиях и в организациях.	ОПК-6.3.2
67.	Раскройте содержание деятельности службы защиты информации организации при обеспечении режима защиты сведений ограниченного доступа.	ОПК-6.3.2
68.	Охарактеризуйте взаимодействие руководителя организации, службы защиты информации, юридического подразделения, кадровой службы и подразделения информационных технологий при организации защиты информации.	ОПК-6.3.2
69.	Перечислите основные функции служб защиты информации на предприятии: планирование мер защиты, разработка локальных актов, контроль доступа, учет носителей, обучение работников, внутренний контроль и реагирование на инциденты.	ОПК-6.3.2
70.	Установите соответствие между субъектом системы защиты информации и его задачей: 1) руководитель организации; 2) служба защиты информации; 3) кадровая служба; 4) юридическое подразделение; 5) подразделение информационных технологий. А. Организация технической эксплуатации информационных систем и учет учетных записей.	ОПК-6.3.2

	Б. Проверка правовых оснований локальных актов и договорных обязательств. В. Принятие управленческих решений и утверждение локальных документов по защите информации. Г. Организация допуска, обучение работников, контроль соблюдения режима защиты информации. Д. Оформление приема, перевода, увольнения работников и документов о неразглашении. Запишите соответствующую последовательность букв.	
71.	Назовите основные организационные меры, направленные на защиту информации ограниченного доступа в организации.	ОПК-6.3.3
72.	Раскройте содержание разрешительной системы доступа как организационной меры защиты информации ограниченного доступа.	ОПК-6.3.3
73.	Охарактеризуйте значение учета носителей, разграничения прав доступа, журналирования действий пользователей и внутреннего контроля при защите сведений ограниченного доступа.	ОПК-6.3.3
74.	Перечислите организационные меры защиты информации ограниченного доступа, применяемые при работе с бумажными документами, электронными файлами, информационными системами и съемными носителями.	ОПК-6.3.3
75.	Установите соответствие между организационной мерой и ее назначением: 1) матрица прав доступа; 2) журнал учета носителей; 3) инструкция по защите информации; 4) резервное копирование; 5) внутренний аудит. А. Закрепление правил обращения с защищаемой информацией. Б. Определение разрешенных действий пользователей с информационными ресурсами. В. Проверка выполнения установленных требований и выявление нарушений. Г. Обеспечение возможности восстановления информации при сбое или утрате данных. Д. Фиксация движения материальных носителей защищаемой информации. Запишите соответствующую последовательность букв.	ОПК-6.3.3
76.	Назовите нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти, применяемые при защите информации ограниченного доступа.	ОПК-6.3.4
77.	Раскройте назначение документов ФСТЭК России при организации технической защиты конфиденциальной информации и защиты информации в информационных системах.	ОПК-6.3.4
78.	Охарактеризуйте роль документов ФСБ России при организации криптографической защиты информации, использовании средств криптографической защиты и	ОПК-6.3.4

	электронной подписи.	
79.	Перечислите виды документов, применяемых при организации защиты информации ограниченного доступа: федеральные законы, постановления Правительства РФ, приказы регуляторов, требования, руководящие и методические документы, национальные стандарты и локальные акты организации.	ОПК-6.З.4
80.	Установите соответствие между документом или органом и сферой применения: 1) ФСТЭК России; 2) ФСБ России; 3) Роскомнадзор; 4) национальный стандарт; 5) локальный нормативный акт организации. А. Установление внутренних правил защиты информации и ответственности работников. Б. Контроль и надзор в сфере обработки персональных данных. В. Техническая защита информации и требования к защите от несанкционированного доступа. Г. Общие требования, терминология и подходы к обеспечению информационной безопасности. Д. Криптографическая защита информации и применение средств криптографической защиты в пределах компетенции. Запишите соответствующую последовательность букв.	ОПК-6.З.4
81.	Составьте пример перечня требований к физической защите объекта, на котором обрабатывается информация ограниченного доступа.	ОПК-6.У.4
82.	Сформулируйте запрос руководителю подразделения о предоставлении сведений, необходимых для разработки пропускного режима: перечень помещений, категории работников, состав посетителей, режим работы и используемые материальные носители информации.	ОПК-6.У.4
83.	Опишите порядок формулирования требований к пропускному и внутриобъектовому режимам в организации, включая идентификацию работников и посетителей, порядок выдачи пропусков, сопровождение посетителей и контроль перемещения носителей информации.	ОПК-6.У.4
84.	Покажите, как использовать требования нормативных и локальных документов при определении режимных зон, порядка допуска в помещения и правил хранения носителей информации ограниченного доступа.	ОПК-6.У.4
85.	Решите практическую задачу. В организации имеется помещение, где обрабатываются персональные данные и конфиденциальная информация. Необходимо сформулировать требования к физической защите объекта и пропускному режиму: определить категории доступа, порядок прохода работников и посетителей, меры контроля, правила хранения носителей и порядок реагирования на нарушение режима.	ОПК-6.У.4

86.	Продемонстрируйте навыки применения нормативных правовых актов, нормативных и методических документов при выборе мер защиты информации для объекта информатизации организации.	ОПК-6.В.1
87.	Разработайте фрагмент локального регламента организации системы защиты информации, включив порядок классификации информации, разграничения доступа, учета носителей, контроля исполнения требований и реагирования на инциденты.	ОПК-6.В.1
88.	Смоделируйте процесс организации системы защиты информации на предприятии: от анализа состава защищаемой информации и применимых требований до разработки локальных актов, внедрения мер защиты и проведения внутреннего контроля.	ОПК-6.В.1
89.	Оцените достаточность системы защиты информации, если в организации утверждена политика информационной безопасности, но отсутствуют матрица доступа, порядок учета носителей, регламент резервного копирования и план внутреннего контроля.	ОПК-6.В.1
90.	Установите верную последовательность действий при применении нормативных правовых актов и методических документов для организации системы защиты информации: А. Определить состав защищаемой информации и объект защиты. Б. Выявить применимые нормативные правовые акты, стандарты и методические документы. В. Сформировать перечень требований к системе защиты информации. Г. Разработать локальные организационно-распорядительные документы. Д. Внедрить организационные, технические и режимные меры защиты. Е. Назначить ответственных лиц и организовать обучение работников. Ж. Провести контроль, аудит и актуализацию системы защиты информации. Запишите последовательность букв.	ОПК-6.В.1
91.	Назовите основные нормативные правовые акты, регулирующие защиту персональных данных и охрану результатов интеллектуальной деятельности в Российской Федерации.	ОПК-10.З.2
92.	Раскройте правовые основы обработки и защиты персональных данных в организации, включая обязанности оператора, права субъекта персональных данных и требования к локальным документам.	ОПК-10.З.2
93.	Охарактеризуйте правовой режим результатов интеллектуальной деятельности, служебных произведений, программ для ЭВМ, баз данных и ноу-хау в деятельности организации.	ОПК-10.З.2
94.	Перечислите основные локальные документы организации, необходимые для защиты персональных данных и охраны	ОПК-10.З.2

	результатов интеллектуальной деятельности: политика обработки персональных данных, положение о защите персональных данных, перечень лиц с доступом, соглашения о неразглашении, регламент учета и использования результатов интеллектуальной деятельности.	
95.	Установите соответствие между правовым объектом и способом его защиты: 1) персональные данные работника; 2) база данных организации; 3) программа для ЭВМ; 4) ноу-хау; 5) служебное произведение. А. Закрепление прав работодателя и автора на результат, созданный в рамках трудовых обязанностей. Б. Введение режима коммерческой тайны и ограничение доступа. В. Соблюдение требований к обработке, хранению и передаче сведений о физическом лице. Г. Правовая охрана как объекта авторского права и учет прав на использование. Д. Правовая охрана структуры и содержания базы данных, установление правил доступа и использования. Запишите соответствующую последовательность букв.	ОПК-10.З.2

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1.	Прочитайте текст и выберите один правильный ответ. Какой нормативный правовой акт закрепляет общие принципы правового регулирования отношений в области информации, информационных технологий и защиты информации? А. Федеральный закон «Об информации, информационных технологиях и о защите информации». Б. Федеральный закон «О бухгалтерском учете». В. Федеральный закон «О рекламе». Г. Федеральный закон «О несостоятельности (банкротстве)».	УК-2.З.2
2.	Прочитайте текст и выберите один правильный ответ. Что относится к правовым нормам, регулирующим профессиональную деятельность специалиста по информационной безопасности? А. Только устные распоряжения работников подразделения. Б. Федеральные законы, подзаконные акты, нормативные документы	УК-2.З.2

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	регуляторов и локальные акты организации. В. Только рекламные материалы поставщиков средств защиты информации. Г. Только технические характеристики компьютеров.	
3.	Прочитайте текст и выберите один правильный ответ. Какое требование должно учитываться при обработке персональных данных в профессиональной деятельности организации? А. Обработка данных без определения цели. Б. Свободная передача данных любым лицам. В. Обработка данных на законном основании, с соблюдением установленных целей и мер защиты. Г. Отказ от информирования работников о правилах обработки данных.	УК-2.З.2
4.	Прочитайте текст и установите соответствие между нормативным актом и сферой его применения: 1. Федеральный закон «О персональных данных». 2. Федеральный закон «О коммерческой тайне». 3. Федеральный закон «Об электронной подписи». 4. Закон Российской Федерации «О государственной тайне». А. Установление режима коммерческой тайны. Б. Защита сведений, составляющих государственную тайну. В. Правила обработки и защиты персональных данных. Г. Правовое регулирование применения электронной подписи. Запишите соответствующую последовательность букв.	УК-2.З.2
5.	Прочитайте текст и выберите правильные варианты ответа. Какие правовые источники необходимо учитывать при решении профессиональной задачи по обеспечению информационной безопасности? А. Федеральные законы. Б. Нормативные и методические документы ФСТЭК России и ФСБ России. В. Локальные нормативные акты организации. Г. Неофициальные советы из открытых форумов как единственное основание решения. Д. Государственные и международные стандарты в области информационной безопасности. Запишите выбранные буквы.	УК-2.З.2
6.	Прочитайте текст и выберите один правильный ответ. Какое действие демонстрирует умение использовать нормативную и правовую документацию при подготовке локального акта по информационной безопасности? А. Подготовка текста без проверки действующего законодательства. Б. Использование актуальных федеральных законов, документов регуляторов и внутренних регламентов организации. В. Замена требований законодательства личным мнением работника. Г. Исключение ссылок на применимые нормативные документы.	УК-2.У.2
7.	Прочитайте текст и выберите один правильный ответ. Что следует сделать перед применением нормативного документа при решении задачи по защите информации? А. Проверить актуальность документа, сферу его действия и	УК-2.У.2

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	применимость к объекту защиты. Б. Использовать документ независимо от даты и предмета регулирования. В. Применять только документы, найденные в случайных источниках. Г. Исключить анализ объекта защиты.	
8.	Прочитайте текст и установите последовательность использования нормативной документации при подготовке политики информационной безопасности: А. Определить объект регулирования и вид защищаемой информации. Б. Найти применимые федеральные законы, подзаконные акты, стандарты и документы регуляторов. В. Проверить актуальность и применимость документов. Г. Сформулировать требования для локального документа. Д. Согласовать и утвердить проект политики. Запишите соответствующую последовательность букв.	УК-2.У.2
9.	Прочитайте текст и выберите правильные варианты ответа. Какие сведения целесообразно запросить у подразделений для правильного применения нормативной документации? А. Состав обрабатываемой информации. Б. Перечень информационных систем и пользователей. В. Сведения о правовых основаниях обработки информации. Г. Личные предпочтения пользователей без связи с задачей защиты. Д. Используемые каналы передачи и места хранения информации. Запишите выбранные буквы.	УК-2.У.2
10.	Прочитайте текст и выберите один правильный ответ. Организация внедряет систему электронного документооборота с персональными данными работников. Какое решение соответствует умению использовать нормативную и правовую документацию? А. Не разрабатывать локальные документы, так как система электронная. Б. Учесть требования законодательства о персональных данных, электронной подписи, защиты информации и разработать локальный регламент работы в системе. В. Предоставить доступ всем работникам без учета должностных обязанностей. Г. Хранить сведения без определения ответственных лиц.	УК-2.У.2
11.	Прочитайте текст и выберите один правильный ответ. Какой вариант отражает оптимальный способ решения задачи с учетом действующих правовых норм? А. Выбор меры защиты без анализа законодательства и ресурсов. Б. Выбор меры защиты после анализа цели, нормативных требований, ресурсов, рисков и ограничений организации. В. Полный отказ от защиты информации из-за ограниченного бюджета. Г. Предоставление доступа всем пользователям для упрощения работы.	УК-2.В.1
12.	Прочитайте текст и выберите один правильный ответ. Что необходимо учитывать при выборе способа защиты информации ограниченного доступа? А. Только удобство пользователей. Б. Только стоимость оборудования.	УК-2.В.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	В. Действующие правовые нормы, ресурсы, ограничения, категорию информации и уровень риска. Г. Только мнение одного работника.	
13.	Прочитайте текст и установите последовательность выбора оптимального способа решения задачи по защите информации: А. Определить цель и содержание задачи. Б. Выявить применимые правовые нормы и ограничения. В. Оценить доступные ресурсы и возможные риски. Г. Сравнить допустимые варианты решения. Д. Выбрать и оформить оптимальное решение. Запишите соответствующую последовательность букв.	УК-2.В.1
14.	Прочитайте текст и выберите правильные варианты ответа. Какие действия подтверждают владение навыками выбора оптимального решения в сфере информационной безопасности? А. Обоснование выбора меры защиты ссылкой на нормативные требования. Б. Оценка ресурсов и ограничений организации. В. Сравнение нескольких допустимых способов решения. Г. Игнорирование требований законодательства. Д. Документирование выбранного решения. Запишите выбранные буквы.	УК-2.В.1
15.	Прочитайте текст и выберите один правильный ответ. В организации нужно ограничить доступ к сведениям коммерческой тайны. Какой вариант решения является правомерным и оптимальным? А. Утвердить перечень сведений, определить круг допущенных лиц, оформить обязательства о неразглашении и установить порядок учета доступа. Б. Объявить устно, что все сведения являются тайной, без документов. В. Запретить работу с любыми документами организации. Г. Разрешить доступ всем работникам при наличии служебного компьютера.	УК-2.В.1
16.	Прочитайте текст и выберите один правильный ответ. Что является основой российской правовой системы? А. Конституция Российской Федерации. Б. Локальная инструкция отдела кадров. В. Переписка работников. Г. Коммерческое предложение поставщика.	ОПК-5.З.1
17.	Прочитайте текст и выберите один правильный ответ. Какой принцип означает, что органы государственной власти и организации должны действовать в пределах установленных полномочий и требований закона? А. Принцип случайности. Б. Принцип законности. В. Принцип неформального согласования. Г. Принцип произвольного доступа.	ОПК-5.З.1
18.	Прочитайте текст и выберите один правильный ответ. Что относится к элементам правового статуса личности в Российской Федерации? А. Только должностная инструкция. Б. Права, свободы, обязанности и гарантии их реализации.	ОПК-5.З.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	В. Только корпоративные правила внешнего вида. Г. Только технические параметры рабочего места.	
19.	Прочитайте текст и установите соответствие между понятием и содержанием: 1. Правовая система. 2. Законодательство. 3. Правовой статус личности. 4. Орган государственной власти. А. Совокупность прав, свобод, обязанностей и гарантий личности. Б. Совокупность нормативных правовых актов. В. Уполномоченный публичный субъект, осуществляющий государственные функции. Г. Совокупность правовых норм, институтов, источников и практики их применения. Запишите соответствующую последовательность букв.	ОПК-5.3.1
20.	Прочитайте текст и выберите правильные варианты ответа. Какие положения относятся к основам организации и деятельности органов государственной власти в Российской Федерации? А. Компетенция органов определяется законом. Б. Органы государственной власти действуют в пределах полномочий. В. Акты органов власти могут устанавливать обязательные требования в пределах компетенции. Г. Любая организация вправе заменять федеральные органы власти. Д. Решения органов власти могут влиять на регулирование информационной безопасности. Запишите выбранные буквы.	ОПК-5.3.1
21.	Прочитайте текст и выберите один правильный ответ. Какая отрасль права регулирует управленческие отношения с участием органов исполнительной власти и вопросы административной ответственности? А. Административное право. Б. Семейное право. В. Наследственное право. Г. Международное частное право.	ОПК-5.3.2
22.	Прочитайте текст и выберите один правильный ответ. Какая отрасль права регулирует трудовые отношения, дисциплинарную ответственность работников и обязанности работодателя? А. Уголовное право. Б. Трудовое право. В. Земельное право. Г. Финансовое право.	ОПК-5.3.2
23.	Прочитайте текст и выберите один правильный ответ. К какой отрасли права относятся нормы об ответственности за неправомерный доступ к компьютерной информации? А. Уголовное право. Б. Жилищное право. В. Семейное право. Г. Авторское право как единственная отрасль.	ОПК-5.3.2
24.	Прочитайте текст и установите соответствие между отраслью права и	ОПК-5.3.2

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	примером ее применения в профессиональной деятельности организации: 1. Гражданское право. 2. Трудовое право. 3. Административное право. 4. Уголовное право. А. Ответственность за неправомерный доступ к компьютерной информации. Б. Заключение договора на оказание услуг по защите информации. В. Дисциплинарная ответственность работника за нарушение правил безопасности. Г. Ответственность организации за нарушение обязательных требований. Запишите соответствующую последовательность букв.	
25.	Прочитайте текст и выберите правильные варианты ответа. Какие отрасли права наиболее часто применяются при организации информационной безопасности в организации? А. Конституционное право. Б. Административное право. В. Трудовое право. Г. Уголовное право. Д. Только семейное право. Запишите выбранные буквы.	ОПК-5.3.2
26.	Прочитайте текст и выберите один правильный ответ. Какой орган в пределах компетенции осуществляет нормативное регулирование в сфере технической защиты информации? А. ФСТЭК России. Б. Росстат. В. Роспотребнадзор. Г. Федеральное казначейство.	ОПК-5.3.3
27.	Прочитайте текст и выберите один правильный ответ. Какой орган связан с регулированием криптографической защиты информации и использованием средств криптографической защиты в пределах компетенции? А. ФСБ России. Б. Росархив. В. Росстат. Г. Федеральная налоговая служба.	ОПК-5.3.3
28.	Прочитайте текст и выберите один правильный ответ. Что является основанием для организации защиты государственной тайны? А. Произвольное решение любого сотрудника. Б. Законодательство о государственной тайне, перечни сведений, режим допуска и требования к защите. В. Только рекламный буклет поставщика оборудования. Г. Устная договоренность с пользователем.	ОПК-5.3.3
29.	Прочитайте текст и установите соответствие между видом ответственности и примером нарушения: 1. Дисциплинарная ответственность. 2. Административная ответственность.	ОПК-5.3.3

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	3. Уголовная ответственность. 4. Гражданско-правовая ответственность. А. Возмещение убытков, причиненных разглашением конфиденциальных сведений. Б. Замечание или выговор работнику за нарушение локальной инструкции. В. Ответственность за неправомерный доступ к компьютерной информации при наличии состава преступления. Г. Ответственность за нарушение обязательных требований законодательства о защите информации. Запишите соответствующую последовательность букв.	
30.	Прочитайте текст и выберите правильные варианты ответа. Какие вопросы входят в основы законодательства в области информационной безопасности и защиты информации? А. Защита информации ограниченного доступа. Б. Защита государственной тайны и конфиденциальной информации. В. Ответственность за разглашение защищаемой информации. Г. Правовая характеристика преступлений в сфере компьютерной информации. Д. Правила организации корпоративных праздников. Запишите выбранные буквы.	ОПК-5.З.3
31.	Прочитайте текст и выберите один правильный ответ. Что понимается под персональными данными? А. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу. Б. Только сведения о государственной тайне. В. Только технические характеристики средств защиты. Г. Любые сведения о юридическом лице без исключения.	ОПК-5.З.4
32.	Прочитайте текст и выберите один правильный ответ. Кто является оператором персональных данных? А. Лицо, организующее и осуществляющее обработку персональных данных, определяющее цели и состав такой обработки. Б. Любой посетитель сайта. В. Только субъект персональных данных. Г. Только поставщик офисной мебели.	ОПК-5.З.4
33.	Прочитайте текст и выберите один правильный ответ. Что относится к результатам интеллектуальной деятельности, подлежащим правовой охране? А. Программа для ЭВМ, база данных, произведение науки, литературы или искусства. Б. Только бумажная папка с документами. В. Только канцелярские принадлежности. Г. Любой устный разговор без признаков результата творческой деятельности.	ОПК-5.З.4
34.	Прочитайте текст и установите соответствие между термином и содержанием: 1. Персональные данные. 2. Оператор персональных данных. 3. Результат интеллектуальной деятельности. 4. Исключительное право.	ОПК-5.З.4

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	А. Право использовать охраняемый результат и распоряжаться им в установленных пределах. Б. Информация, относящаяся к определенному или определяемому физическому лицу. В. Лицо, организующее и осуществляющее обработку персональных данных. Г. Охраняемый результат творческой деятельности. Запишите соответствующую последовательность букв.	
35.	Прочитайте текст и выберите правильные варианты ответа. Какие меры относятся к правовым основам защиты персональных данных и охраны результатов интеллектуальной деятельности? А. Определение целей и правовых оснований обработки персональных данных. Б. Ограничение доступа к персональным данным. В. Учет прав на служебные результаты интеллектуальной деятельности. Г. Свободное копирование программного обеспечения без правовых оснований. Д. Закрепление порядка использования результатов интеллектуальной деятельности в локальных документах и договорах. Запишите выбранные буквы.	ОПК-5.З.4
36.	Прочитайте текст и выберите один правильный ответ. Какое действие демонстрирует умение обосновывать решение, связанное с реализацией правовых норм по защите информации? А. Выбор меры защиты со ссылкой на применимые нормы права, риски и должностные обязанности. Б. Выбор меры защиты без объяснения причин. В. Игнорирование требований локальных документов. Г. Передача решения на устное усмотрение любого работника.	ОПК-5.У.1
37.	Прочитайте текст и выберите один правильный ответ. Что должен сделать специалист при выявлении нарушения права субъекта персональных данных? А. Не фиксировать нарушение. Б. Предпринять меры по восстановлению нарушенного права в пределах должностных обязанностей и установленного порядка. В. Передать данные третьим лицам. Г. Удалить все документы без регистрации.	ОПК-5.У.1
38.	Прочитайте текст и установите последовательность действий при обосновании правового решения по защите информации: А. Выявить факт или риск нарушения. Б. Определить применимые правовые нормы и должностные полномочия. В. Сформулировать возможные варианты реагирования. Г. Обосновать выбранный вариант и оформить решение. Д. Организовать контроль исполнения решения. Запишите соответствующую последовательность букв.	ОПК-5.У.1
39.	Прочитайте текст и выберите правильные варианты ответа. Какие элементы должны быть отражены в обосновании решения по защите информации? А. Применимые правовые нормы.	ОПК-5.У.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Б. Фактические обстоятельства и риски. В. Должностные полномочия лица, принимающего решение. Г. Личные предпочтения без связи с законом. Д. Меры по восстановлению нарушенных прав при необходимости. Запишите выбранные буквы.	
40.	Прочитайте текст и выберите один правильный ответ. Работник направил персональные данные клиента неуполномоченному адресату. Какое решение соответствует реализации правовых норм по защите информации? А. Не сообщать о нарушении. Б. Зафиксировать инцидент, уведомить ответственное лицо, ограничить дальнейшее распространение, провести проверку и принять меры восстановления нарушенных прав. В. Удалить переписку и не оформлять документы. Г. Разрешить дальнейшую пересылку данных.	ОПК-5.У.1
41.	Прочитайте текст и выберите один правильный ответ. Какой локальный документ обычно закрепляет общие цели, принципы и направления обеспечения информационной безопасности организации? А. Политика информационной безопасности. Б. График отпусков. В. Табель учета рабочего времени. Г. Личное заявление работника.	ОПК-5.У.2
42.	Прочитайте текст и выберите один правильный ответ. Что должно быть учтено при разработке проекта инструкции по защите информации ограниченного доступа? А. Состав защищаемой информации, порядок доступа, обязанности работников, учет носителей и ответственность. Б. Только пожелания пользователей без анализа рисков. В. Только оформление титульного листа. Г. Исключительно список праздников организации.	ОПК-5.У.2
43.	Прочитайте текст и установите последовательность разработки локального регламента по обеспечению информационной безопасности: А. Проанализировать требования законодательства и документов регуляторов. Б. Определить процессы и сведения, подлежащие регулированию. В. Подготовить проект регламента. Г. Согласовать проект с заинтересованными подразделениями. Д. Утвердить документ и ознакомить работников. Запишите соответствующую последовательность букв.	ОПК-5.У.2
44.	Прочитайте текст и выберите правильные варианты ответа. Какие разделы целесообразно включить в локальный акт по информационной безопасности? А. Общие положения и область применения. Б. Порядок допуска и доступа. В. Порядок учета носителей и регистрации действий. Г. Правила свободной передачи защищаемых сведений любым лицам. Д. Контроль исполнения и ответственность. Запишите выбранные буквы.	ОПК-5.У.2

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
45.	Прочитайте текст и выберите один правильный ответ. Организация разрабатывает положение о коммерческой тайне. Какое требование должно быть включено в проект документа? А. Перечень сведений, режим доступа, обязанности работников, порядок маркирования, хранения, передачи и контроля. Б. Разрешение публиковать сведения без согласования. В. Отсутствие ответственности за разглашение. Г. Предоставление доступа всем пользователям без учета должностных обязанностей.	ОПК-5.У.2
46.	Прочитайте текст и выберите один правильный ответ. Что относится к лицензированию деятельности в области защиты информации? А. Получение разрешения на осуществление определенного вида деятельности при соблюдении установленных требований. Б. Покупка офисной мебели. В. Устное согласование между работниками. Г. Отказ от документов регуляторов.	ОПК-5.У.3
47.	Прочитайте текст и выберите один правильный ответ. Для чего проводится сертификация средства защиты информации? А. Для подтверждения соответствия средства защиты установленным требованиям безопасности информации. Б. Для оформления командировки. В. Для замены должностных инструкций. Г. Для отмены требований законодательства.	ОПК-5.У.3
48.	Прочитайте текст и выберите один правильный ответ. Что является целью аттестации объекта информатизации по требованиям безопасности информации? А. Подтверждение соответствия объекта установленным требованиям защиты информации. Б. Увеличение количества пользователей без ограничений. В. Отказ от контроля доступа. Г. Замена всех локальных актов устными распоряжениями.	ОПК-5.У.3
49.	Прочитайте текст и установите соответствие между процедурой и ее содержанием: 1. Лицензирование. 2. Сертификация. 3. Аттестация. 4. Контроль соответствия. А. Проверка выполнения установленных требований в процессе эксплуатации. Б. Подтверждение соответствия объекта информатизации требованиям безопасности. В. Разрешение на осуществление определенного вида деятельности. Г. Подтверждение соответствия средства защиты установленным требованиям. Запишите соответствующую последовательность букв.	ОПК-5.У.3
50.	Прочитайте текст и выберите правильные варианты ответа. Какие требования необходимо формулировать при подготовке к лицензированию, сертификации или аттестации? А. Требования к квалификации персонала.	ОПК-5.У.3

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Б. Требования к комплекту организационно-распорядительных документов. В. Требования к применяемым средствам защиты и условиям эксплуатации. Г. Разрешение работать без регламентов и учета. Д. Требования к контролю соблюдения установленных процедур. Запишите выбранные буквы.	
51.	Прочитайте текст и выберите один правильный ответ. Какое требование необходимо сформулировать для защиты конфиденциальной информации в организации? А. Определить перечень защищаемых сведений, круг лиц с доступом, правила хранения, передачи и ответственности. Б. Разрешить всем работникам свободно копировать документы. В. Отказаться от маркирования и учета носителей. Г. Хранить все сведения в открытой папке.	ОПК-5.У.4
52.	Прочитайте текст и выберите один правильный ответ. Что должно быть включено в требования по защите персональных данных работников? А. Цели обработки, категории данных, правовые основания, круг лиц с доступом, меры защиты и порядок контроля. Б. Только список дней рождения работников. В. Разрешение на передачу данных без оснований. Г. Отказ от учета действий пользователей.	ОПК-5.У.4
53.	Прочитайте текст и установите последовательность введения требований по защите конфиденциальной информации: А. Определить состав защищаемых сведений. Б. Установить правовой режим и круг лиц с доступом. В. Разработать локальные документы и правила обращения со сведениями. Г. Ознакомить работников с обязанностями. Д. Организовать контроль исполнения требований. Запишите соответствующую последовательность букв.	ОПК-5.У.4
54.	Прочитайте текст и выберите правильные варианты ответа. Какие требования относятся к охране результатов интеллектуальной деятельности в организации? А. Учет служебных результатов интеллектуальной деятельности. Б. Определение порядка использования и передачи прав. В. Фиксация авторства и правообладателя. Г. Свободное копирование программного обеспечения без разрешения. Д. Закрепление порядка хранения материалов, содержащих результаты интеллектуальной деятельности. Запишите выбранные буквы.	ОПК-5.У.4
55.	Прочитайте текст и выберите один правильный ответ. Организация хранит базу клиентов и техническую документацию новой разработки. Какой набор требований является правильным? А. Требования по защите персональных данных, конфиденциальной информации и результатов интеллектуальной деятельности, включая разграничение доступа, учет, хранение и контроль. Б. Размещение файлов в общем доступе. В. Передача документов всем контрагентам без соглашений.	ОПК-5.У.4

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Г. Отсутствие локальных документов и ответственных лиц.	
56.	Прочитайте текст и выберите один правильный ответ. Что подтверждает владение навыками работы с нормативными документами и стандартами в области информационной безопасности? А. Умение находить применимые документы, оценивать их актуальность и использовать требования при подготовке локальных решений. Б. Использование только устных советов. В. Отказ от проверки актуальности документов. Г. Игнорирование государственных и международных стандартов.	ОПК-5.В.1
57.	Прочитайте текст и выберите один правильный ответ. Какое действие является правильным при работе с международным стандартом в области информационной безопасности? А. Соотнести положения стандарта с задачами организации и применимыми российскими требованиями. Б. Применять стандарт без учета сферы деятельности и законодательства. В. Использовать только название стандарта без анализа содержания. Г. Отказаться от сопоставления с локальными документами.	ОПК-5.В.1
58.	Прочитайте текст и установите последовательность работы с нормативными документами при подготовке локального регламента: А. Определить объект защиты и вид информации. Б. Подобрать применимые нормативные правовые акты, методические документы и стандарты. В. Проверить актуальность документов. Г. Выделить обязательные и рекомендуемые требования. Д. Отразить требования в локальном регламенте. Запишите соответствующую последовательность букв.	ОПК-5.В.1
59.	Прочитайте текст и выберите правильные варианты ответа. Какие навыки необходимы для работы с нормативными документами и стандартами? А. Поиск актуальных редакций документов. Б. Определение применимости требований к объекту защиты. В. Сопоставление требований разных документов. Г. Замена требований стандартов произвольными решениями. Д. Подготовка перечня требований для локальных актов. Запишите выбранные буквы.	ОПК-5.В.1
60.	Прочитайте текст и выберите один правильный ответ. Организация использует только внутренние инструкции и не учитывает федеральные законы, документы ФСТЭК России и ФСБ России, а также стандарты. Как следует оценить такой подход? А. Подход недостаточен, поскольку система защиты должна учитывать применимые нормативные правовые акты, документы регуляторов и стандарты. Б. Подход достаточен при наличии любого внутреннего документа. В. Подход исключает необходимость контроля. Г. Подход автоматически заменяет требования законодательства.	ОПК-5.В.1
61.	Прочитайте текст и выберите один правильный ответ. Какая процедура подтверждает соответствие объекта информатизации требованиям безопасности информации?	ОПК-6.З.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	А. Аттестация объекта информатизации. Б. Оформление графика отпусков. В. Проведение корпоративного собрания. Г. Регистрация входящей корреспонденции.	
62.	Прочитайте текст и выберите один правильный ответ. Что относится к системе нормативных правовых актов и стандартов в области сертификации средств защиты информации? А. Требования и документы, устанавливающие порядок подтверждения соответствия средств защиты информации. Б. Только инструкции по эксплуатации мебели. В. Только устные рекомендации пользователей. Г. Только коммерческие предложения поставщиков.	ОПК-6.3.1
63.	Прочитайте текст и выберите один правильный ответ. Для какой сферы особенно важны требования лицензирования деятельности по технической защите конфиденциальной информации? А. Для выполнения работ и оказания услуг, связанных с технической защитой конфиденциальной информации. Б. Для оформления командировок. В. Для ведения учета канцелярских товаров. Г. Для организации корпоративных праздников.	ОПК-6.3.1
64.	Прочитайте текст и установите соответствие между процедурой и объектом регулирования: 1. Лицензирование. 2. Аттестация. 3. Сертификация. 4. Защита государственной тайны. А. Объект информатизации. Б. Деятельность в установленной области защиты информации. В. Средство защиты информации. Г. Сведения, составляющие государственную тайну, и режим их защиты. Запишите соответствующую последовательность букв.	ОПК-6.3.1
65.	Прочитайте текст и выберите правильные варианты ответа. Какие элементы относятся к системе нормативного регулирования лицензирования, аттестации и сертификации в сфере защиты информации? А. Нормативные правовые акты. Б. Требования регуляторов. В. Государственные стандарты. Г. Неформальные сообщения без правового статуса. Д. Методические документы по подтверждению соответствия и защите информации. Запишите выбранные буквы.	ОПК-6.3.1
66.	Прочитайте текст и выберите один правильный ответ. Какова основная задача органов защиты государственной тайны? А. Организация и контроль мер по защите сведений, составляющих государственную тайну. Б. Организация развлекательных мероприятий. В. Выдача отпускных удостоверений. Г. Ведение только бухгалтерской отчетности.	ОПК-6.3.2

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
67.	Прочитайте текст и выберите один правильный ответ. Какова задача службы защиты информации на предприятии? А. Организация выполнения мер по защите информации, контроль соблюдения требований и участие в разработке локальных документов. Б. Замена всех подразделений организации. В. Свободная публикация защищаемых сведений. Г. Отказ от учета инцидентов.	ОПК-6.3.2
68.	Прочитайте текст и выберите один правильный ответ. Что относится к задачам службы защиты информации при работе с персоналом? А. Инструктаж работников, контроль соблюдения режима доступа и участие в расследовании инцидентов. Б. Отказ от ознакомления работников с правилами. В. Передача паролей третьим лицам. Г. Исключение кадровых рисков из анализа.	ОПК-6.3.2
69.	Прочитайте текст и установите соответствие между субъектом и задачей: 1. Орган защиты государственной тайны. 2. Служба защиты информации предприятия. 3. Руководитель организации. 4. Работник, допущенный к защищаемым сведениям. А. Соблюдение установленного режима и обязанности неразглашения. Б. Принятие управленческих решений и утверждение локальных документов. В. Организация режима защиты сведений, составляющих государственную тайну. Г. Разработка и контроль выполнения мер защиты информации на объекте. Запишите соответствующую последовательность букв.	ОПК-6.3.2
70.	Прочитайте текст и выберите правильные варианты ответа. Какие функции могут выполнять службы защиты информации на предприятиях? А. Анализ рисков и угроз. Б. Разработка локальных актов по защите информации. В. Контроль доступа и учет инцидентов. Г. Разрешение несанкционированного копирования данных. Д. Организация обучения и инструктажа работников. Запишите выбранные буквы.	ОПК-6.3.2
71.	Прочитайте текст и выберите один правильный ответ. Что относится к организационной мере защиты информации ограниченного доступа? А. Назначение ответственных лиц и установление порядка доступа. Б. Хранение документов без учета. В. Передача паролей в открытом виде. Г. Публикация конфиденциальных документов на открытом сайте.	ОПК-6.3.3
72.	Прочитайте текст и выберите один правильный ответ. Для чего применяется матрица доступа? А. Для определения пользователей, ролей и разрешенных действий с информационными ресурсами. Б. Для учета канцелярских товаров.	ОПК-6.3.3

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	В. Для оформления графика отпусков. Г. Для замены всех нормативных документов.	
73.	Прочитайте текст и выберите один правильный ответ. Какое действие снижает риск утечки информации ограниченного доступа? А. Разграничение доступа по должностным обязанностям и принципу минимально необходимого доступа. Б. Предоставление общего доступа всем работникам. В. Отсутствие учета носителей. Г. Хранение документов на общедоступном сетевом ресурсе.	ОПК-6.3.3
74.	Прочитайте текст и установите последовательность внедрения организационных мер защиты информации ограниченного доступа: А. Определить состав защищаемой информации. Б. Установить круг пользователей и полномочия доступа. В. Разработать локальные инструкции и журналы учета. Г. Ознакомить работников с требованиями. Д. Организовать контроль и аудит соблюдения режима. Запишите соответствующую последовательность букв.	ОПК-6.3.3
75.	Прочитайте текст и выберите правильные варианты ответа. Какие меры входят в систему организационной защиты информации ограниченного доступа? А. Допуск и доступ. Б. Учет носителей и документов. В. Инструктаж работников. Г. Регистрация инцидентов. Д. Свободное копирование защищаемых сведений. Запишите выбранные буквы.	ОПК-6.3.3
76.	Прочитайте текст и выберите один правильный ответ. Какой орган издает нормативные и методические документы в области технической защиты информации в пределах своей компетенции? А. ФСТЭК России. Б. Росстат. В. Роспотребнадзор. Г. Федеральное казначейство.	ОПК-6.3.4
77.	Прочитайте текст и выберите один правильный ответ. Какой орган уполномочен в области криптографической защиты информации в пределах своей компетенции? А. ФСБ России. Б. Роспатент. В. Росстат. Г. Федеральная служба судебных приставов.	ОПК-6.3.4
78.	Прочитайте текст и выберите один правильный ответ. Что является назначением методических документов уполномоченных федеральных органов в сфере защиты информации? А. Разъяснение порядка выполнения требований и применение подходов к защите информации. Б. Установление графика отпусков работников. В. Замена всех федеральных законов. Г. Описание корпоративной символики.	ОПК-6.3.4
79.	Прочитайте текст и установите соответствие между органом или	ОПК-6.3.4

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	документом и сферой применения: 1. ФСТЭК России. 2. ФСБ России. 3. Роскомнадзор. 4. Методический документ. А. Контроль и надзор в сфере персональных данных. Б. Рекомендации и разъяснения по выполнению требований. В. Техническая защита информации. Г. Криптографическая защита информации. Запишите соответствующую последовательность букв.	
80.	Прочитайте текст и выберите правильные варианты ответа. Какие документы могут использоваться при организации защиты информации ограниченного доступа? А. Нормативные правовые акты. Б. Руководящие документы регуляторов. В. Методические документы уполномоченных органов. Г. Государственные стандарты. Д. Неформальные сообщения без указания источника как единственная основа защиты. Запишите выбранные буквы.	ОПК-6.З.4
81.	Прочитайте текст и выберите один правильный ответ. Что относится к требованиям физической защиты объекта? А. Зонирование помещений, контроль доступа, охрана, учет посетителей и защита мест хранения носителей. Б. Свободный проход всех посетителей. В. Хранение носителей без контроля. Г. Отсутствие ответственных лиц.	ОПК-6.У.4
82.	Прочитайте текст и выберите один правильный ответ. Какое требование целесообразно включить в пропускной режим организации? А. Порядок оформления, выдачи, учета и возврата пропусков. Б. Разрешение прохода без проверки личности. В. Отмена регистрации посетителей. Г. Передача пропусков третьим лицам.	ОПК-6.У.4
83.	Прочитайте текст и установите последовательность организации пропускного режима: А. Определить категории работников, посетителей и транспортных средств. Б. Установить порядок оформления и выдачи пропусков. В. Организовать регистрацию входа и выхода. Г. Определить зоны доступа и правила сопровождения посетителей. Д. Установить контроль соблюдения режима. Запишите соответствующую последовательность букв.	ОПК-6.У.4
84.	Прочитайте текст и выберите правильные варианты ответа. Какие требования относятся к физической защите объекта информатизации? А. Контроль доступа в помещения. Б. Хранение носителей в оборудованных местах. В. Защита переговорных и рабочих зон. Г. Неограниченный доступ посетителей.	ОПК-6.У.4

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Д. Учет и сопровождение посетителей. Запишите выбранные буквы.	
85.	Прочитайте текст и выберите один правильный ответ. В организации посетители проходят в помещения с защищаемой информацией без регистрации и сопровождения. Какое требование необходимо сформулировать? А. Ввести порядок регистрации посетителей, проверки оснований доступа, выдачи временных пропусков и сопровождения в режимных зонах. Б. Оставить порядок без изменений. В. Разрешить посетителям самостоятельный доступ к документам. Г. Отменить зонирование помещений.	ОПК-6.У.4
86.	Прочитайте текст и выберите один правильный ответ. Какое действие подтверждает владение навыками применения нормативных документов при организации системы защиты информации? А. Выбор мер защиты на основе применимых нормативных правовых актов, методических документов и характеристик объекта защиты. Б. Выбор мер защиты случайным образом. В. Отказ от документов регуляторов. Г. Предоставление доступа без учета категорий информации.	ОПК-6.В.1
87.	Прочитайте текст и выберите один правильный ответ. Что должно быть результатом применения нормативных документов при организации системы защиты информации? А. Комплект локальных документов, выбранные меры защиты, назначенные ответственные лица и порядок контроля. Б. Только устное поручение без учета требований. В. Отсутствие журналов учета. Г. Свободное распространение защищаемой информации.	ОПК-6.В.1
88.	Прочитайте текст и установите последовательность применения нормативных документов при организации системы защиты информации: А. Определить объект защиты и состав информации. Б. Выявить применимые нормативные правовые акты и методические документы. В. Сформировать перечень требований. Г. Разработать локальные документы и выбрать меры защиты. Д. Организовать контроль и актуализацию системы защиты. Запишите соответствующую последовательность букв.	ОПК-6.В.1
89.	Прочитайте текст и выберите правильные варианты ответа. Какие навыки необходимы при применении нормативных документов для организации системы защиты информации? А. Анализ применимости требований. Б. Сопоставление требований с объектом защиты. В. Разработка локальных регламентов. Г. Исключение контроля исполнения. Д. Оценка достаточности реализованных мер. Запишите выбранные буквы.	ОПК-6.В.1
90.	Прочитайте текст и выберите один правильный ответ. В организации есть политика информационной безопасности, но	ОПК-6.В.1

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	отсутствуют матрица доступа, порядок учета носителей и регламент реагирования на инциденты. Какой вывод является правильным? А. Система защиты требует доработки, поскольку локальные документы и процедуры должны обеспечивать практическое выполнение требований защиты информации. Б. Политики достаточно для любых случаев. В. Отсутствие регламентов снижает только объем бумаги, но не влияет на защиту. Г. Контроль доступа можно не организовывать.	
91.	Прочитайте текст и выберите один правильный ответ. Какой федеральный закон устанавливает общие требования к обработке персональных данных? А. Федеральный закон «О персональных данных». Б. Федеральный закон «О рекламе». В. Федеральный закон «О бухгалтерском учете». Г. Федеральный закон «О связи» как единственный акт по всем вопросам данных.	ОПК-10.З.2
92.	Прочитайте текст и выберите один правильный ответ. Что относится к правовым основам охраны результатов интеллектуальной деятельности? А. Закрепление прав на результаты интеллектуальной деятельности и определение порядка их использования. Б. Свободное использование любых программ без правовых оснований. В. Отказ от учета авторства. Г. Передача всех материалов третьим лицам без договоров.	ОПК-10.З.2
93.	Прочитайте текст и выберите один правильный ответ. Какое действие является обязанностью организации при обработке персональных данных? А. Определить цели обработки, правовые основания, круг лиц с доступом и меры защиты. Б. Обрабатывать любые сведения без цели. В. Передавать данные всем заинтересованным лицам. Г. Отказаться от локальных документов.	ОПК-10.З.2
94.	Прочитайте текст и установите соответствие между объектом защиты и правовым режимом: 1. Персональные данные работника. 2. Программа для ЭВМ, созданная работником. 3. База данных клиентов. 4. Служебное произведение. А. Охрана результата интеллектуальной деятельности. Б. Защита персональных данных. В. Защита персональных данных и, при наличии условий, охрана базы данных. Г. Правовой режим служебного результата интеллектуальной деятельности. Запишите соответствующую последовательность букв.	ОПК-10.З.2
95.	Прочитайте текст и выберите правильные варианты ответа. Какие меры относятся к правовым основам организации защиты персональных данных и охраны результатов интеллектуальной	ОПК-10.З.2

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	деятельности? А. Разработка политики обработки персональных данных. Б. Ограничение доступа к персональным данным. В. Учет служебных результатов интеллектуальной деятельности. Г. Оформление прав на программы для ЭВМ и базы данных. Д. Разрешение свободного копирования служебных материалов без учета прав. Запишите выбранные буквы.	

Примечание: система оценивания тестовых заданий:

Оценка тестовых заданий балльная шкала	Характеристика заданий
Полное совпадение с верным ответом оценивается 1 баллом/ неверный ответ или его отсутствие – 0 баллов.	1 тип - Задание комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора считается верным, если правильно указана цифра и приведены конкретные аргументы, используемые при выборе ответа.
Полное совпадение с верным ответом оценивается 1 баллом, если допущены ошибки или ответ отсутствует 0 баллов.	2 тип - Задание комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора считается верным, если правильно указаны цифры и приведены конкретные аргументы, используемые при выборе ответов.
«Полное совпадение с верным ответом оценивается 1баллом, неверный ответ или его отсутствие - 0 баллов»	3 тип - Задание закрытого типа на установление соответствия считается верным, если установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого столбца
«Полное совпадение с верным ответом оценивается 1баллом, если допущены ошибки или ответ отсутствует – 0 баллов.»	4 тип - Задание закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр.
«Правильный ответ за задание оценивается в 3 балла, если допущена одна ошибка \ неточность \ ответ правильный, но не полный - 1 балл, если допущено более 1 ошибки \ ответ неправильный \ ответ отсутствует – 0	5 тип - Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.

Оценка тестовых заданий балльная шкала	Характеристика заданий
баллов».	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала.

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Теоретические и нормативные основы обеспечения информационной безопасности.

- Тема 1.1. Информационное общество и информационная безопасность.

- Тема 1.2. Система обеспечения ИБ РФ и организации.

- Тема 1.3. Источники правового регулирования в области информации и защиты информации.

- Тема 1.4. Субъекты, регуляторы и полномочия органов государственной власти.

Раздел 2. Правовое обеспечение защиты информации и ответственности.

- Тема 2.1. Правовые режимы информации ограниченного доступа.
- Тема 2.2. Защита персональных данных и конфиденциальной информации.
- Тема 2.3. Охрана РИД, электронная подпись и электронное взаимодействие.
- Тема 2.4. Лицензирование, сертификация и аттестация.
- Тема 2.5. Юридическая и дисциплинарная ответственность.

Раздел 3. Организационное обеспечение ИБ на объекте защиты.

- Тема 3.1. Политика ИБ и локальное нормативное регулирование.
- Тема 3.2. Организационные меры защиты информации ограниченного доступа.
- Тема 3.3. Физическая защита объекта, пропускной и внутриобъектовый режимы.
- Тема 3.4. Управление персоналом, контроль, аудит и корректирующие мероприятия.

11.2. Методические указания для обучающихся по участию в семинарах.

Основной целью для обучающегося является систематизация и обобщение знаний по изучаемой теме, разделу, формирование умения работать с дополнительными источниками информации, сопоставлять и сравнивать точки зрения, конспектировать прочитанное, высказывать свою точку зрения и т.п. В соответствии с ведущей дидактической целью содержанием семинарских занятий являются узловые, наиболее трудные для понимания и усвоения темы, разделы дисциплины. Спецификой данной формы занятий является совместная работа преподавателя и обучающегося над решением поставленной проблемы, а поиск верного ответа строится на основе чередования индивидуальной и коллективной деятельности.

При подготовке к семинарскому занятию по теме лекции необходимо ознакомиться с планом его проведения, с литературой и научными публикациями по теме семинара.

Требования к проведению семинаров

Учебным планом не предусмотрено

11.3. Методические указания для обучающихся по прохождению практических занятий.

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

– закрепление, углубление, расширение и детализация знаний при решении конкретных задач;

– развитие познавательных способностей, самостоятельности мышления, творческой активности;

– овладение новыми методами и методиками изучения конкретной учебной дисциплины;

– выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Требования к проведению практических занятий

Решение практических задач по темам раздела призвано закрепить, углубить, расширить и детализировать знания при решении конкретных жизненных ситуаций, выработать способности логического осмысления полученных знаний для выполнения профессиональных задач, обеспечить рациональное сочетание коллективной и индивидуальной форм обучения. Условия задач в письменной форме предоставляются

преподавателем. Вопросы к условию задачи могут меняться. От студента при выполнении данного вида работ требуется знание основных положений отраслевого законодательства, текст нормативного источника, умение анализировать, толковать и правильно применять правовые нормы.

Структура и форма отчета о практической работе

Отчет о практической работе должен содержать: титульный лист, основную часть, выводы по результатам исследований.

На титульном листе должны быть указаны: название дисциплины, название практической работы, фамилия и инициалы преподавателя, фамилия и инициалы студента, номер его учебной группы и дата защиты работы.

Основная часть должна содержать задание, результаты экспериментально-практической работы, расчетно-аналитические материалы, листинг кода/скрин экрана.

Выводы по проделанной работе должны содержать основные результаты по работе.

Требования к оформлению отчета о практической работе

Титульный лист отчета должен соответствовать шаблону, приведенному в секторе нормативной документации ГУАП https://guap.ru/regdocs/docs/uch

Оформление основной части отчета должно быть оформлено в соответствии с ГОСТ 7.32-2017. Требования приведены в секторе нормативной документации ГУАП https://guap.ru/regdocs/docs/uch

При формировании списка источников студентам необходимо руководствоваться требованиями стандарта ГОСТ 7.0.100-2018. Примеры оформления списка источников приведены в секторе нормативной документации ГУАП. https://guap.ru/regdocs/docs/uch

При формировании списка источников студентам необходимо руководствоваться требованиями стандарта ГОСТ 7.0.100-2018. Примеры оформления списка источников приведены в секторе нормативной документации ГУАП. https://guap.ru/regdocs/docs/uch

11.4. Методические указания для обучающихся по выполнению лабораторных работ. (*не предусмотрено учебным планом по данной дисциплине).*

11.5. Методические указания для обучающихся по выполнению курсового проекта/ курсовой работы. *(не предусмотрено учебным планом по данной дисциплине)*.

11.6. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Существенную часть самостоятельной работы студента представляет собой подготовка докладов к практическим занятиям, которая предполагает проработку материала, его обобщение и изложение. В ходе самостоятельной работы обучающийся изучает теоретический материал, нормативные правовые акты и методические документы, готовится к практическим занятиям, текущему контролю и промежуточной аттестации, выполняет домашние задания. Самостоятельная работа включает поиск и анализ информации по теме занятия, подготовку кратких сообщений, разработку фрагментов локальных организационно-распорядительных документов, изучение примеров регламентов и инструкций, связанных с защитой информации ограниченного доступа.

Методическими материалами, направляющими самостоятельную работу обучающихся, являются: рабочая программа дисциплины, материалы лекций, перечень основной и дополнительной литературы, электронные образовательные ресурсы, нормативные правовые акты и методические документы уполномоченных федеральных органов исполнительной власти. При подготовке доклада необходимо ясно выражать свои мысли, формулировать четкие фразы. Выводы должны быть краткими, но обоснованными. Доклад может сопровождаться презентациями, которые выполняются с помощью специальных компьютерных программ, например, Microsoft office PowerPoint. Выступление докладчика начинается объявлением темы доклада (сообщения) и

завершается собственными выводами по заявленной проблематике. Темы для самостоятельной работы:
1. Информационная безопасность как объект правового и организационного обеспечения.
2. Информационное общество и угрозы информационной безопасности.
3. Система обеспечения информационной безопасности РФ.
4. Доктринальные документы в сфере ИБ.
5. Законодательство об информации и защите информации.
6. Законодательство о персональных данных.
7. Правовой режим государственной тайны.
8. Правовой режим коммерческой тайны.
9. Служебная и профессиональная тайны.
10. Конфиденциальная информация: виды и признаки.
11. Правовой статус личности в информационной сфере.
12. Правовое положение организации как обладателя информации.
13. Регуляторы в сфере ИБ.
14. Полномочия ФСТЭК России.
15. Полномочия ФСБ России.
16. Полномочия Роскомнадзора.
17. Полномочия Роспатента.
18. Преступления в сфере компьютерной информации.
19. Ответственность за нарушения требований защиты информации.
20. Защита прав субъектов информационной сферы.
21. Лицензирование деятельности в области защиты информации.
22. Сертификация средств защиты информации.
23. Аттестация объектов информатизации.
24. Политика информационной безопасности организации.
25. Локальные нормативные акты по защите информации.
26. Положение о защите информации.
27. Положение о коммерческой тайне.
28. Политика обработки персональных данных.
29. Регламент доступа к информационным ресурсам.
30. Матрица доступа.
31. Задачи службы защиты информации.
32. Распределение ролей и ответственности.
33. Допуск и доступ к информации ограниченного доступа.
34. Физическая защита объекта информатизации.
35. Пропускной режим.
36. Учет носителей информации.
37. Обучение работников вопросам ИБ.
38. Внутренний контроль требований ИБ.
39. Служебное расследование инцидентов ИБ.
40. Корректирующие мероприятия по результатам аудита.

11.7. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль успеваемости осуществляется в виде:

− устный опрос на занятиях;

− систематическая проверка выполнения индивидуальных заданий;

− тестирование по материалам лекции в среде LMS;

− контроль самостоятельных работ (в письменной или устной формах);

− контроль выполнения индивидуального задания на практику;

− иные виды, определяемые научно-педагогическим работником (далее – НПР).

В случае принятия решения о подведении итогов ТКУ, они могут проводится:

1) один раз в семестр:

− на 9 (девятой) неделе в осеннем семестре;

− на 32 (тридцать второй) неделе в весеннем семестре.

2) два раза в семестр:

− на 8 (восьмой) и 14 (четырнадцатой) неделях в осеннем семестре;

− на 31(тридцать первой) и 36 (тридцать шестой) неделях в весеннем семестре.

Ведомости для подведения итогов ТКУ выдаются работниками структурного подразделения старостам учебных групп очной и очно - заочной форм обучения. Старосты обязаны вернуть полностью заполненную ведомость в течение 14 (четырнадцати) дней с момента получения.

При подведении итогов ТКУ в ведомость обучающимся выставляются аттестационные оценки: «аттестован», «не аттестован». Система и возможные критерии оценки знаний, умений, навыков и/ или опыта деятельности, характеризующих этапы формирования компетенций.

Критерии оценки уровня успеваемости обучающихся:

«АТТЕСТОВАН»

– обучающийся выполняет все требования НПР при выполнении и сдачи всех видов работ, указанных в РПД;

– обучающийся всесторонне усвоил материал, предусмотренный РПД на момент подведения итогов ТКУ;

– уверенно, логично, последовательно и грамотно излагает материал, предусмотренный РПД на момент подведения итогов ТКУ;

– опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные знания с деятельностью по направлению подготовки (специальности);

– грамотно обосновывает и аргументирует выдвигаемые выводы и идеи по материалу, предусмотренному РПД на момент подведения итогов ТКУ;

– свободно владеет системой специализированных понятий и терминологией, связанных с направлением подготовки (специальностью).

«НЕ АТТЕСТОВАН»

– обучающийся пропустил большую часть занятий и/ или не выполняет требования НПР при выполнении и сдаче всех видов работ, указанных в РПД на момент подведения итогов ТКУ;

– обучающийся не усвоил значительной части материала, предусмотренного РПД на момент подведения итогов ТКУ;

– испытывает трудности в практическом применении знаний;

– не может аргументировать научные положения;

– не формулирует и не обосновывает выдвигаемые выводы и обобщения по материалу, предусмотренному РПД, на момент подведения итогов ТКУ;

– не владеет системой специализированных понятий и терминологией, связанных с направлением подготовки (специальностью).

В соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП» оценки текущего контроля успеваемости влияют на итоги промежуточной аттестации.

Система оценок при проведении текущего контроля осуществляется в соответствии с руководящим документом организации РДО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов,

обучающихся по образовательным программам высшего образования в ГУАП» https://docs.guap.ru/guap/2020/sto_smk-3-76.pdf.

11.8. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Критерии оценивания:

–знание категорий и понятий информационного права, его источников, содержания и этапов развития;

–умение свободно оперировать правовыми терминами и понятиями в области информационного права; толковать правовые нормы, применяя различные способы и виды толкования;

–владение навыками постановки правовых целей и задач и их эффективного достижения, учитывая интересы различных субъектов права в области информационного права.

Необходимо иметь в виду, что нормативно-правовые акты и материалы судебной практики периодически изменяются, следовательно, студентам при изучении дисциплины необходимо отслеживать все изменения и использовать только актуальную редакцию.

В течение семестра для допуска к зачету студенту необходимо сдать не менее 50% практических работ, выполнить тестирования в среде LMS не ниже оценки «удовлетворительно». Далее студент допускается к собеседованию или итоговому тестированию на зачете.

Зачет выставляется на основании выполненных в течение семестра всех практических работ и написания итогового тестирования или прохождения собеседования.

Оценка формируется в соответствии с критериями, приведенными в таблице 14.

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с руководящим документом организации РДО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов, обучающихся по образовательным программам высшего образования в ГУАП» https://docs.guap.ru/guap/2020/sto_smk-3-76.pdf.

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой

Приложение № 1
к РПД «Организационное и правовое обеспечение информационной безопасности»

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Перечень ответов для тестов

№ п/п	Перечень ответов для тестов	Код индикатора
1.	А	УК-2.З.2
2.	Б	УК-2.З.2
3.	В	УК-2.З.2
4.	1-В, 2-А, 3-Г, 4-Б	УК-2.З.2
5.	А, Б, В, Д	УК-2.З.2
6.	Б	УК-2.У.2
7.	А	УК-2.У.2
8.	А, Б, В, Г, Д	УК-2.У.2
9.	А, Б, В, Д	УК-2.У.2
10.	Б	УК-2.У.2
11.	Б	УК-2.В.1
12.	В	УК-2.В.1
13.	А, Б, В, Г, Д	УК-2.В.1
14.	А, Б, В, Д	УК-2.В.1
15.	А	УК-2.В.1
16.	А	ОПК-5.З.1
17.	Б	ОПК-5.З.1
18.	Б	ОПК-5.З.1
19.	1-Г, 2-Б, 3-А, 4-В	ОПК-5.З.1
20.	А, Б, В, Д	ОПК-5.З.1
21.	А	ОПК-5.З.2
22.	Б	ОПК-5.З.2
23.	А	ОПК-5.З.2
24.	1-Б, 2-В, 3-Г, 4-А	ОПК-5.З.2
25.	А, Б, В, Г	ОПК-5.З.2
26.	А	ОПК-5.З.3
27.	А	ОПК-5.З.3
28.	Б	ОПК-5.З.3
29.	1-Б, 2-Г, 3-В, 4-А	ОПК-5.З.3
30.	А, Б, В, Г	ОПК-5.З.3
31.	А	ОПК-5.З.4
32.	А	ОПК-5.З.4
33.	А	ОПК-5.З.4
34.	1-Б, 2-В, 3-Г, 4-А	ОПК-5.З.4
35.	А, Б, В, Д	ОПК-5.З.4
36.	А	ОПК-5.У.1
37.	Б	ОПК-5.У.1
38.	А, Б, В, Г, Д	ОПК-5.У.1
39.	А, Б, В, Д	ОПК-5.У.1
40.	Б	ОПК-5.У.1
41.	А	ОПК-5.У.2
42.	А	ОПК-5.У.2

№ п/п	Перечень ответов для тестов	Код индикатора
43.	А, Б, В, Г, Д	ОПК-5.У.2
44.	А, Б, В, Д	ОПК-5.У.2
45.	А	ОПК-5.У.2
46.	А	ОПК-5.У.3
47.	А	ОПК-5.У.3
48.	А	ОПК-5.У.3
49.	1-В, 2-Г, 3-Б, 4-А	ОПК-5.У.3
50.	А, Б, В, Д	ОПК-5.У.3
51.	А	ОПК-5.У.4
52.	А	ОПК-5.У.4
53.	А, Б, В, Г, Д	ОПК-5.У.4
54.	А, Б, В, Д	ОПК-5.У.4
55.	А	ОПК-5.У.4
56.	А	ОПК-5.В.1
57.	А	ОПК-5.В.1
58.	А, Б, В, Г, Д	ОПК-5.В.1
59.	А, Б, В, Д	ОПК-5.В.1
60.	А	ОПК-5.В.1
61.	А	ОПК-6.З.1
62.	А	ОПК-6.З.1
63.	А	ОПК-6.З.1
64.	1-Б, 2-А, 3-В, 4-Г	ОПК-6.З.1
65.	А, Б, В, Д	ОПК-6.З.1
66.	А	ОПК-6.З.2
67.	А	ОПК-6.З.2
68.	А	ОПК-6.З.2
69.	1-В, 2-Г, 3-Б, 4-А	ОПК-6.З.2
70.	А, Б, В, Д	ОПК-6.З.2
71.	А	ОПК-6.З.3
72.	А	ОПК-6.З.3
73.	А	ОПК-6.З.3
74.	А, Б, В, Г, Д	ОПК-6.З.3
75.	А, Б, В, Г	ОПК-6.З.3
76.	А	ОПК-6.З.4
77.	А	ОПК-6.З.4
78.	А	ОПК-6.З.4
79.	1-В, 2-Г, 3-А, 4-Б	ОПК-6.З.4
80.	А, Б, В, Г	ОПК-6.З.4
81.	А	ОПК-6.У.4
82.	А	ОПК-6.У.4
83.	А, Б, В, Г, Д	ОПК-6.У.4
84.	А, Б, В, Д	ОПК-6.У.4
85.	А	ОПК-6.У.4
86.	А	ОПК-6.В.1
87.	А	ОПК-6.В.1
88.	А, Б, В, Г, Д	ОПК-6.В.1
89.	А, Б, В, Д	ОПК-6.В.1
90.	А	ОПК-6.В.1

№ п/п	Перечень ответов для тестов	Код индикатора
91.	А	ОПК-10.З.2
92.	А	ОПК-10.З.2
93.	А	ОПК-10.З.2
94.	1-Б, 2-А, 3-В, 4-Г	ОПК-10.З.2
95.	А, Б, В, Г	ОПК-10.З.2