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 специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности/специализации «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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

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

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 ИБ, разработкой локальных актов, организацией пропускного и внутриобъектового режима, внутреннего контроль и аудита выполнения мер защиты.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме дифференцированного зачета (7 семестр).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания дисциплины в системе подготовки по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализации «Безопасность открытых информационных 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, участия в формировании политики информационной безопасности и управлении реализацией комплекса мер защиты на объекте.

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
Общепрофессиональные компетенции	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.З.1 знать перечень основных нормативных правовых актов, стандартов и методических документов в области защиты информации и информационной безопасности ОПК-5.У.1 уметь применять нормативные акты при проектировании и разработке систем безопасности автоматизированных информационных систем и их компонентов ОПК-5.В.1 владеть 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 автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами	ОПК-6.З.1 знать методы и средства организации защиты информации ограниченного доступа ОПК-6.З.2 знать структуру и общий состав нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-6.У.1 уметь осуществлять организацию защиты информации ограниченного доступа в соответствии с регламентирующими документами ОПК-6.В.1 владеть навыками применения нормативных правовых актов, нормативных и методических

	Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	документов при организации системы защиты информации

2. Место дисциплины в структуре ОП

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

- «Информационное право»,
- «Основы информационной безопасности»,
- «Теория информационной безопасности и методы защиты информации»,
- «Стандарты информационной безопасности»,
- «Основы цифровой грамотности».

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

- «Управление информационной безопасностью»,
- «Проектирование защищенных информационных систем»,
- «Производственная проектнотехнологическая практика»,
- «Производственная практика научно исследовательская работа».

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
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки		
Аудиторные занятия, всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)	34	34
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	40	40
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Дифф. зач.,	Дифф. зач.,

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 7					
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.	11	7			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.	12	14			15
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	13			15
Итого в семестре:	34	34			40
Итого	34	34	0	0	40

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 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.

Номер раздела	Название и содержание разделов и тем лекционных занятий
	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 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.

Номер раздела	Название и содержание разделов и тем лекционных занятий
	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 7					
1	Нормативные основы обеспечения информационной безопасности	Комментированное чтение нормативных актов, групповая дискуссия, решение ситуационных задач, построение схемы регуляторов.	7	7	1
2	Правовые режимы информации ограниченного доступа	Кейс-анализ, разработка перечня сведений ограниченного доступа, подготовка фрагмента локального акта.	7	7	2
3	Лицензирование, сертификация, аттестация, электронная	Решение практических задач, сопоставление процедур,	7	7	2

	подпись	подготовка схемы документального сопровождения.			
4	Политика ИБ и локальные акты организации	Игровое проектирование, разработка структуры политики ИБ, проекта приказа и регламента доступа.	6	6	3
5	Физическая защита, пропускной режим, контроль и аудит	Моделирование реальных условий, анализ схемы объекта, подготовка корректирующих мероприятий.	7	7	3
Всего			34	34	

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 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	14	14
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	8	8
Домашнее задание (ДЗ)	10	10

Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	8	8
Всего:	40	40

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
Дифференцированный зачёт	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**.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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 Российской Федерации, регулирующие отношения в области защиты информации и информационной безопасности.	ОПК-5.3.1
2.	Раскройте назначение Федерального закона «Об информации, информационных технологиях и о защите информации» в системе правового регулирования информационной безопасности.	ОПК-5.3.1
3.	Охарактеризуйте роль нормативных и методических документов ФСТЭК России и ФСБ России при организации защиты информации в автоматизированных	ОПК-5.3.1

	информационных системах.	
4.	Перечислите основные государственные и международные стандарты, применяемые в области информационной безопасности и защиты информации.	ОПК-5.З.1
5.	Установите соответствие между нормативным документом и сферой его применения: 1) Федеральный закон «О персональных данных»; 2) Федеральный закон «Об электронной подписи»; 3) Закон Российской Федерации «О государственной тайне»; 4) Федеральный закон «О коммерческой тайне»; 5) ГОСТ или международный стандарт в области информационной безопасности. А) регулирование применения электронной подписи; Б) защита сведений, составляющих государственную тайну; В) обработка и защита персональных данных; Г) установление режима коммерческой тайны; Д) определение требований, подходов и терминологии в сфере информационной безопасности.	ОПК-5.З.1
6.	Составьте пример перечня нормативных правовых актов и стандартов, которые необходимо учитывать при проектировании системы защиты персональных данных в автоматизированной информационной системе организации.	ОПК-5.У.1
7.	Сформулируйте запрос в ответственное подразделение организации о предоставлении исходных данных, необходимых для выбора применимых нормативных требований при разработке системы безопасности автоматизированной информационной системы.	ОПК-5.У.1
8.	Опишите порядок применения нормативных актов при определении требований к защите информации на этапах проектирования, разработки, внедрения и эксплуатации автоматизированной информационной системы.	ОПК-5.У.1
9.	Покажите, как использовать требования нормативных документов ФСТЭК России при выборе организационных и технических мер защиты информации для автоматизированной информационной системы.	ОПК-5.У.1
10.	Решите практическую задачу. Организация разрабатывает автоматизированную информационную систему, в которой будут обрабатываться персональные данные работников и сведения ограниченного доступа. Определите, какие нормативные правовые акты, стандарты и методические документы необходимо применить при проектировании системы безопасности, какие требования следует включить в техническое задание и какие локальные документы необходимо подготовить.	ОПК-5.У.1
11.	Продемонстрируйте навыки поиска и отбора нормативных документов, государственных и международных стандартов, необходимых для оценки соответствия системы защиты информации установленным требованиям.	ОПК-5.В.1
12.	Разработайте фрагмент локального перечня нормативных документов, используемых в организации при обеспечении информационной безопасности и защите информации.	ОПК-5.В.1

13.	Смоделируйте порядок работы специалиста по информационной безопасности с нормативной базой при подготовке проекта политики информационной безопасности организации.	ОПК-5.В.1
14.	Оцените корректность выбора нормативных документов для защиты автоматизированной информационной системы, если организация учитывает только внутренние инструкции и не использует федеральные законы, документы регуляторов и стандарты информационной безопасности.	ОПК-5.В.1
15.	Установите верную последовательность действий специалиста при работе с нормативными документами и стандартами в области информационной безопасности: А) определить вид защищаемой информации и объект защиты; Б) выявить применимые федеральные законы и подзаконные акты; В) определить применимые нормативные и методические документы регуляторов; Г) выбрать государственные и международные стандарты, применимые к объекту защиты; Д) сформировать перечень требований к системе защиты информации; Е) отразить требования в проектной, эксплуатационной и локальной организационно-распорядительной документации.	ОПК-5.В.1
16.	Назовите основные методы организации защиты информации ограниченного доступа в автоматизированных информационных системах.	ОПК-6.З.1
17.	Раскройте содержание организационных, правовых, технических и режимных мер защиты информации ограниченного доступа.	ОПК-6.З.1
18.	Охарактеризуйте средства защиты информации, применяемые для предотвращения несанкционированного доступа, утечки, модификации и уничтожения сведений ограниченного доступа.	ОПК-6.З.1
19.	Перечислите основные элементы системы защиты информации ограниченного доступа: разграничение доступа, учет носителей, идентификация и аутентификация пользователей, регистрация событий безопасности, контроль действий пользователей.	ОПК-6.З.1
20.	Установите соответствие между методом защиты информации ограниченного доступа и его содержанием: 1) разграничение доступа; 2) идентификация и аутентификация; 3) резервное копирование; 4) регистрация событий безопасности; 5) инструктаж персонала. А) восстановление информации при сбое или утрате данных; Б) определение разрешенных действий пользователя с информационными ресурсами; В) подтверждение личности пользователя перед предоставлением доступа; Г) фиксация действий пользователей и событий в системе; Д) доведение до работников правил обращения с защищаемой информацией.	ОПК-6.З.1
21.	Назовите основные группы нормативных и методических документов Федеральной службы безопасности Российской Федерации и Федеральной службы по	ОПК-6.З.2

	техническому и экспортному контролю, применяемых в области защиты информации.	
22.	Раскройте назначение нормативных и методических документов ФСТЭК России при организации технической защиты информации ограниченного доступа.	ОПК-6.З.2
23.	Охарактеризуйте роль нормативных и методических документов ФСБ России в сфере криптографической защиты информации, применения средств криптографической защиты и электронной подписи.	ОПК-6.З.2
24.	Перечислите основные виды документов регуляторов, используемых при организации защиты информации: приказы, требования, методические документы, руководящие документы, рекомендации, положения и регламенты.	ОПК-6.З.2
25.	Установите соответствие между регулятором или видом документа и сферой применения: 1) ФСТЭК России; 2) ФСБ России; 3) методический документ; 4) руководящий документ; 5) приказ регулятора. А) устанавливает обязательные требования или порядок выполнения определенных действий; Б) применяется при технической защите информации и защите от несанкционированного доступа; В) содержит разъяснения и рекомендации по выполнению требований; Г) используется при организации криптографической защиты информации; Д) определяет подходы, правила или процедуры защиты информации в установленной сфере.	ОПК-6.З.2
26.	Составьте пример плана организационных мероприятий по защите информации ограниченного доступа в автоматизированной информационной системе организации.	ОПК-6.У.1
27.	Сформулируйте запрос руководителю подразделения о предоставлении сведений, необходимых для организации защиты информации ограниченного доступа: состава обрабатываемой информации, перечня пользователей, используемых информационных систем и каналов передачи данных.	ОПК-6.У.1
28.	Опишите порядок организации защиты информации ограниченного доступа в соответствии с регламентирующими документами: определение объекта защиты, классификация информации, выбор мер защиты, разработка локальных документов, внедрение мер и контроль их исполнения.	ОПК-6.У.1
29.	Покажите, как использовать регламентирующие документы при определении прав доступа пользователей к информационной системе, в которой обрабатываются сведения ограниченного доступа.	ОПК-6.У.1
30.	Решите практическую задачу. В организации внедряется автоматизированная информационная система, содержащая персональные данные работников и сведения ограниченного доступа. Необходимо определить порядок организации защиты информации: установить категории защищаемой информации, определить круг пользователей,	ОПК-6.У.1

	выбрать организационные и технические меры, подготовить локальные документы и определить порядок контроля соблюдения требований.	
31.	Продемонстрируйте навыки применения нормативных правовых актов, нормативных и методических документов при выборе мер защиты информации для автоматизированной информационной системы.	ОПК-6.В.1
32.	Разработайте фрагмент локального регламента организации защиты информации ограниченного доступа, включив порядок допуска пользователей, разграничение прав доступа, учет носителей и контроль соблюдения требований.	ОПК-6.В.1
33.	Смоделируйте процесс организации системы защиты информации на объекте защиты: от анализа состава обрабатываемой информации до оформления комплекта организационно-распорядительных документов.	ОПК-6.В.1
34.	Оцените достаточность системы защиты информации, если в организации утверждена политика информационной безопасности, но отсутствуют матрица доступа, журнал учета носителей, порядок резервного копирования и регламент реагирования на инциденты.	ОПК-6.В.1
35.	Установите верную последовательность действий при организации системы защиты информации ограниченного доступа: А) определить состав и категории защищаемой информации; Б) выявить применимые нормативные правовые акты и методические документы; В) определить объект защиты и границы информационной системы; Г) выбрать организационные, технические и режимные меры защиты; Д) разработать и утвердить локальные документы; Е) внедрить меры защиты и назначить ответственных лиц; Ж) организовать контроль, аудит и актуализацию системы защиты информации.	ОПК-6.В.1

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 федеральный закон устанавливает общие правовые основы регулирования отношений в сфере информации, информационных технологий и защиты информации? А. Федеральный закон «Об информации, информационных	ОПК-5.3.1

	технологиях и о защите информации». Б. Федеральный закон «О бухгалтерском учете». В. Федеральный закон «О рекламе». Г. Федеральный закон «О связи» как единственный акт в области защиты информации.	
2.	Прочитайте текст и выберите один правильный ответ. Какой документ применяется при построении системы управления информационной безопасностью организации и определяет международный подход к менеджменту информационной безопасности? А. ГОСТ Р 7.0.97-2016. Б. ISO/IEC 27001 или национальный стандарт, основанный на данном подходе. В. Номенклатура дел организации. Г. График документооборота.	ОПК-5.3.1
3.	Прочитайте текст и установите соответствие между нормативным актом или документом и сферой его применения: 1) Федеральный закон «О персональных данных»; 2) Закон Российской Федерации «О государственной тайне»; 3) Федеральный закон «О коммерческой тайне»; 4) документы ФСТЭК России; 5) документы ФСБ России. А. Организация технической защиты информации и защиты от несанкционированного доступа. Б. Регулирование обработки и защиты сведений, относящихся к определенному или определяемому физическому лицу. В. Регулирование вопросов криптографической защиты информации в пределах компетенции. Г. Установление режима сведений, имеющих коммерческую ценность в силу неизвестности третьим лицам. Д. Защита сведений, отнесенных к государственной тайне. Запишите соответствующую последовательность букв.	ОПК-5.3.1
4.	Прочитайте текст и выберите правильные варианты ответа. Какие источники относятся к нормативной и методической базе в области защиты информации и информационной безопасности? А. Федеральные законы Российской Федерации. Б. Подзаконные нормативные правовые акты. В. Нормативные и методические документы ФСТЭК России и ФСБ России. Г. Государственные и международные стандарты в области информационной безопасности. Д. Неформальные рекомендации работников, не утвержденные организацией. Запишите выбранные буквы.	ОПК-5.3.1
5.	Прочитайте текст и установите последовательность. Определите последовательность определения применимой нормативной базы при защите информации в организации:	ОПК-5.3.1

	А. Определить вид обрабатываемой информации и объект защиты. Б. Установить применимые федеральные законы и подзаконные акты. В. Определить применимые документы регуляторов и стандарты. Г. Сформировать перечень требований к защите информации. Д. Отразить требования в локальных документах организации. Запишите соответствующую последовательность букв.	
6.	Прочитайте текст и выберите один правильный ответ. Какое действие соответствует применению нормативных актов при проектировании системы безопасности автоматизированной информационной системы? А. Определение применимых требований к защите информации с учетом вида данных, назначения системы и категории пользователей. Б. Предоставление всем пользователям одинаковых прав доступа. В. Отказ от документирования требований к защите информации. Г. Использование только устных распоряжений без учета нормативной базы.	ОПК-5.У.1
7.	Прочитайте текст и выберите один правильный ответ. Что необходимо включить в техническое задание на разработку системы безопасности автоматизированной информационной системы? А. Только перечень используемых компьютеров. Б. Требования к защите информации, разграничению доступа, регистрации событий безопасности, резервному копированию и контролю выполнения мер защиты. В. Только список работников подразделения. Г. Только описание интерфейса пользователя без мер защиты.	ОПК-5.У.1
8.	Прочитайте текст и выберите правильные варианты ответа. Какие действия выполняются при применении нормативных актов к проектированию системы безопасности автоматизированной информационной системы? А. Анализ состава и категории обрабатываемой информации. Б. Определение угроз и требований к защите информации. В. Выбор организационных и технических мер защиты. Г. Игнорирование требований регуляторов для ускорения разработки. Д. Документирование требований в проектной и эксплуатационной документации. Запишите выбранные буквы.	ОПК-5.У.1
9.	Прочитайте текст и установите последовательность. Определите порядок применения нормативных актов при проектировании системы безопасности: А. Определить объект защиты и состав обрабатываемой информации. Б. Выявить применимые нормативные требования. В. Сформировать требования к подсистемам защиты информации. Г. Включить требования в проектную документацию.	ОПК-5.У.1

	Д. Проверить соответствие реализованных мер установленным требованиям. Запишите соответствующую последовательность букв.	
10.	Прочитайте текст и решите практическую задачу. Организация проектирует автоматизированную информационную систему для обработки персональных данных работников и служебной информации ограниченного доступа. Какой вариант действий является правильным? А. Определить применимые нормативные акты, установить требования к защите данных, разработать модель угроз, выбрать меры защиты, включить их в техническое задание и локальные документы. Б. Начать эксплуатацию системы без анализа состава информации. В. Предоставить полный доступ всем пользователям, чтобы упростить сопровождение системы. Г. Не оформлять требования к защите информации документально.	ОПК-5.У.1
11.	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 требования, сопоставлять их с объектом защиты и использовать при разработке локальных и проектных документов. Б. Использование только личного опыта без проверки нормативной базы. В. Отказ от стандартов при организации защиты информации. Г. Применение устаревших документов без проверки актуальности.	ОПК-5.В.1
12.	Прочитайте текст и выберите один правильный ответ. Какой результат работы специалиста показывает правильное применение государственных и международных стандартов в области информационной безопасности? А. Подготовленный перечень применимых требований и мер защиты, согласованный с целями и процессами организации. Б. Произвольная таблица без указания источников требований. В. Устное сообщение без фиксации выводов. Г. Отказ от оценки соответствия требованиям.	ОПК-5.В.1
13.	Прочитайте текст и установите соответствие между действием специалиста и результатом работы: 1) анализ нормативных документов; 2) анализ стандартов информационной безопасности; 3) подготовка локального перечня требований; 4) проверка актуальности документов; 5) применение требований в проектной документации. А. Формирование требований к системе защиты информации. Б. Определение применимых подходов, терминов и мер управления информационной безопасностью. В. Выявление обязательных правовых и методических требований. Г. Недопущение использования отмененных или устаревших	ОПК-5.В.1

	документов. Д. Закрепление требований в техническом задании, регламентах и инструкциях. Запишите соответствующую последовательность букв.	
14.	Прочитайте текст и установите последовательность. Определите порядок работы с нормативными документами и стандартами при организации защиты информации: А. Определить цель работы и объект защиты. Б. Найти нормативные правовые акты, документы регуляторов и стандарты. В. Проверить актуальность и применимость найденных документов. Г. Сформировать перечень требований и мер защиты. Д. Отразить требования в локальных, проектных и эксплуатационных документах. Е. Организовать пересмотр документов при изменении законодательства или состава системы. Запишите соответствующую последовательность букв.	ОПК-5.В.1
15.	Прочитайте текст и выберите правильные варианты ответа. Какие навыки необходимы при работе с нормативными документами, государственными и международными стандартами в области информационной безопасности? А. Поиск и отбор актуальных нормативных документов. Б. Анализ применимости требований к конкретному объекту защиты. В. Сопоставление требований стандартов с локальными процессами организации. Г. Применение устаревших документов без проверки их действия. Д. Подготовка локальных документов на основе выявленных требований. Запишите выбранные буквы.	ОПК-5.В.1
16.	Прочитайте текст и выберите один правильный ответ. Что относится к методам организации защиты информации ограниченного доступа? А. Установление разрешительной системы доступа. Б. Свободное распространение документов среди работников. В. Хранение сведений без учета носителей. Г. Передача паролей по открытым каналам связи.	ОПК-6.З.1
17.	Прочитайте текст и выберите один правильный ответ. Какое средство применяется для подтверждения личности пользователя перед предоставлением доступа к информационной системе? А. Архивная опись. Б. Средство идентификации и аутентификации. В. Номенклатура дел. Г. График отпусков.	ОПК-6.З.1
18.	Прочитайте текст и установите соответствие между методом защиты информации и его содержанием: 1) разграничение доступа; 2) резервное копирование; 3) регистрация событий безопасности; 4) физическая защита объекта.	ОПК-6.З.1

	А. Фиксация действий пользователей и событий в информационной системе. Б. Создание копий данных для восстановления информации. В. Ограничение действий пользователя в соответствии с его полномочиями. Г. Предотвращение несанкционированного физического доступа к помещениям и оборудованию. Запишите соответствующую последовательность букв.	
19.	Прочитайте текст и установите последовательность. Определите последовательность организации защиты информации ограниченного доступа: А. Выбрать организационные, технические и режимные меры защиты. Б. Определить состав и категории защищаемой информации. В. Назначить ответственных лиц и утвердить локальные документы. Г. Определить объект защиты и круг пользователей. Д. Организовать контроль соблюдения требований защиты информации. Запишите соответствующую последовательность букв.	ОПК-6.3.1
20.	Прочитайте текст и выберите правильные варианты ответа. Какие меры относятся к организационным мерам защиты информации ограниченного доступа? А. Разработка локальных инструкций. Б. Назначение ответственных лиц. В. Размещение конфиденциальных документов в открытом доступе. Г. Ознакомление работников с правилами защиты информации. Д. Проведение внутреннего контроля соблюдения режима защиты информации. Запишите выбранные буквы.	ОПК-6.3.1
21.	Прочитайте текст и выберите один правильный ответ. Какой орган осуществляет нормативное и методическое регулирование в сфере технической защиты информации в пределах своей компетенции? А. ФСТЭК России. Б. Росстат. В. Роспотребнадзор. Г. Федеральное казначейство.	ОПК-6.3.2
22.	Прочитайте текст и выберите один правильный ответ. С документами какого органа связаны вопросы криптографической защиты информации и применения средств криптографической защиты? А. Роспатент. Б. ФСБ России. В. Росстат. Г. Федеральная служба судебных приставов.	ОПК-6.3.2
23.	Прочитайте текст и выберите один правильный ответ. Что входит в общий состав нормативных и методических документов регуляторов в области защиты информации? А. Приказы, требования, руководящие документы, методические документы и рекомендации. Б. Только рекламные материалы организаций. В. Только внутренние письма работников. Г. Только документы кадрового учета.	ОПК-6.3.2

24.	Прочитайте текст и установите соответствие между органом или документом и сферой применения: 1) ФСТЭК России; 2) ФСБ России; 3) методический документ; 4) приказ регулятора. А. Устанавливает обязательные требования или порядок выполнения действий. Б. Применяется при организации технической защиты информации. В. Содержит рекомендации и разъяснения по выполнению требований. Г. Применяется при организации криптографической защиты информации. Запишите соответствующую последовательность букв.	ОПК-6.З.2
25.	Прочитайте текст и установите последовательность. Определите порядок работы с нормативными и методическими документами ФСБ России и ФСТЭК России при организации защиты информации: А. Определить объект защиты и вид обрабатываемой информации. Б. Установить, какие требования регуляторов применимы к объекту защиты. В. Изучить соответствующие нормативные и методические документы. Г. Определить необходимые меры защиты информации. Д. Отразить требования в локальных документах организации. Запишите соответствующую последовательность букв.	ОПК-6.З.2
26.	Прочитайте текст и выберите один правильный ответ. С чего следует начинать организацию защиты информации ограниченного доступа в соответствии с регламентирующими документами? А. С определения состава защищаемой информации, объекта защиты и применимых требований. Б. С предоставления доступа всем пользователям. В. С отказа от локальных нормативных актов. Г. С удаления журналов регистрации событий.	ОПК-6.У.1
27.	Прочитайте текст и выберите один правильный ответ. Какой локальный документ целесообразно разработать для установления порядка работы с информацией ограниченного доступа? А. Инструкцию по организации защиты информации ограниченного доступа. Б. График отпусков. В. Табель учета рабочего времени. Г. Положение о корпоративных мероприятиях.	ОПК-6.У.1
28.	Прочитайте текст и выберите правильные варианты ответа. Какие действия необходимо выполнить при организации защиты информации ограниченного доступа? А. Определить категории защищаемой информации. Б. Установить круг лиц, имеющих доступ. В. Разработать локальные регламенты и инструкции. Г. Разрешить передачу документов без учета и регистрации. Д. Организовать контроль выполнения требований. Запишите выбранные буквы.	ОПК-6.У.1
29.	Прочитайте текст и установите последовательность. Определите	ОПК-6.У.1

	последовательность организации доступа пользователя к сведениям ограниченного доступа: А. Проверить наличие основания для предоставления доступа. Б. Определить объем сведений, необходимых пользователю для выполнения обязанностей. В. Оформить решение о предоставлении доступа. Г. Ознакомить пользователя с обязанностью соблюдать режим защиты информации. Д. Внести сведения о доступе в установленную систему учета. Запишите соответствующую последовательность букв.	
30.	Прочитайте текст и решите практическую задачу. В организации внедряется информационная система, в которой будут обрабатываться сведения ограниченного доступа. Какой вариант действий соответствует регламентирующим документам? А. Определить объект защиты, состав информации, пользователей, меры защиты, локальные документы и порядок контроля. Б. Предоставить доступ всем работникам для ускорения работы. В. Не вести учет пользователей и действий в системе. Г. Использовать только устные распоряжения без утвержденных документов.	ОПК-6.У.1
31.	Прочитайте текст и выберите один правильный ответ. Что подтверждает владение навыками применения нормативных документов при организации системы защиты информации? А. Умение выбирать применимые нормативные требования и отражать их в локальных документах организации. Б. Игнорирование документов регуляторов. В. Замена нормативных требований личным мнением специалиста. Г. Отказ от контроля выполнения требований.	ОПК-6.В.1
32.	Прочитайте текст и выберите один правильный ответ. Какой документ является результатом применения нормативных требований при организации защиты информации в организации? А. Политика информационной безопасности или локальный регламент защиты информации. Б. Личное сообщение работника. В. Неформальная переписка в мессенджере. Г. Рекламная презентация.	ОПК-6.В.1
33.	Прочитайте текст и установите соответствие между действием специалиста и его результатом: 1) анализ нормативных требований; 2) разработка локального регламента; 3) определение прав доступа; 4) проведение внутреннего контроля. А. Выявление соответствия системы защиты установленным требованиям. Б. Закрепление порядка защиты информации в организации. В. Формирование перечня обязательных требований к системе защиты. Г. Установление разрешенных действий пользователей. Запишите соответствующую последовательность букв.	ОПК-6.В.1
34.	Прочитайте текст и установите последовательность. Определите последовательность применения нормативных правовых актов и методических документов при организации системы защиты	ОПК-6.В.1

	информации: А. Определить вид защищаемой информации и объект защиты. Б. Выявить применимые нормативные правовые акты и методические документы. В. Сформировать перечень требований к системе защиты информации. Г. Разработать локальные организационно-распорядительные документы. Д. Внедрить меры защиты и назначить ответственных лиц. Е. Провести контроль и актуализацию системы защиты информации. Запишите соответствующую последовательность букв.	
35.	Прочитайте текст и выберите правильные варианты ответа. Какие навыки необходимы специалисту при организации системы защиты информации с применением нормативных документов? А. Анализ применимых правовых и методических требований. Б. Разработка локальных актов по защите информации. В. Оценка достаточности организационных и технических мер. Г. Предоставление доступа без проверки полномочий. Д. Организация контроля выполнения требований защиты информации. Запишите выбранные буквы.	ОПК-6.В.1

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.

Оценка тестовых заданий балльная шкала	Характеристика заданий
«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 баллов».	5 тип - Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.

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:

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

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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	ОПК-5.З.1
2.	Б	ОПК-5.З.1
3.	1-Б, 2-Д, 3-Г, 4-А, 5-В	ОПК-5.З.1
4.	А, Б, В, Г	ОПК-5.З.1
5.	А, Б, В, Г, Д	ОПК-5.З.1
6.	А	ОПК-5.У.1
7.	Б	ОПК-5.У.1
8.	А, Б, В, Д	ОПК-5.У.1
9.	А, Б, В, Г, Д	ОПК-5.У.1
10.	А	ОПК-5.У.1
11.	А	ОПК-5.В.1
12.	А	ОПК-5.В.1
13.	1-В, 2-Б, 3-А, 4-Г, 5-Д	ОПК-5.В.1
14.	А, Б, В, Г, Д, Е	ОПК-5.В.1
15.	А, Б, В, Д	ОПК-5.В.1
16.	А	ОПК-6.З.1
17.	Б	ОПК-6.З.1
18.	1-В, 2-Б, 3-А, 4-Г	ОПК-6.З.1
19.	Б, Г, А, В, Д	ОПК-6.З.1
20.	А, Б, Г, Д	ОПК-6.З.1
21.	А	ОПК-6.З.2
22.	Б	ОПК-6.З.2
23.	А	ОПК-6.З.2
24.	1-Б, 2-Г, 3-В, 4-А	ОПК-6.З.2
25.	А, Б, В, Г, Д	ОПК-6.З.2
26.	А	ОПК-6.У.1
27.	А	ОПК-6.У.1
28.	А, Б, В, Д	ОПК-6.У.1
29.	А, Б, В, Г, Д	ОПК-6.У.1
30.	А	ОПК-6.У.1
31.	А	ОПК-6.В.1
32.	А	ОПК-6.В.1
33.	1-В, 2-Б, 3-Г, 4-А	ОПК-6.В.1
34.	А, Б, В, Г, Д, Е	ОПК-6.В.1
35.	А, Б, В, Д	ОПК-6.В.1