

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Иркутский государственный университет путей сообщения»  
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА  
приказом ректора  
от «08» мая 2020 г. № 266-1

## **Б1.Б.15 Организационное и правовое обеспечение информационной безопасности рабочая программа дисциплины**

Направление подготовки – 10.03.01 Информационная безопасность  
Профиль подготовки – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Программа подготовки – академический бакалавриат

Квалификация выпускника – бакалавр

Форма обучения – очная

Нормативный срок обучения – 4 года

Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 6

Формы промежуточной аттестации в семестрах:

Часов по учебному плану – 216

экзамен 4, курсовая работа 4

### **Распределение часов дисциплины по семестрам**

Семестр	4	<b>Итого</b>
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	Часов по учебному плану
<b>Аудиторная контактная работа по видам учебных занятий</b>	<b>90</b>	<b>90</b>
– лекции	54	54
– практические (семинарские)	36	36
<b>Самостоятельная работа</b>	<b>90</b>	<b>90</b>
<b>Экзамен</b>	<b>36</b>	<b>36</b>
<b>Итого</b>	<b>216</b>	<b>216</b>

ИРКУТСК

<b>1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ</b>	
<b>1.1 Цели освоения дисциплины</b>	
1	изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационно - правового обеспечения информационной безопасности и защиты информации
<b>1.2 Задачи освоения дисциплины</b>	
1	раскрытие места информационной безопасности и защиты информации в системе информационных отношений;
2	раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации
3	раскрытие взаимосвязи между информационной безопасностью и удовлетворением информационных потребностей субъектов информационных отношений;
4	раскрытие значения обеспечения информационной безопасности для предотвращения негативного информационного воздействия на субъекты информационных отношений;
5	определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны.
<b>1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины</b>	
Научно-образовательное воспитание обучающихся	
Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.	
Цель достигается по мере решения в единстве следующих задач:	
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;	
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;	
– популяризация научных знаний среди обучающихся;	
– содействие повышению привлекательности науки, поддержка научно-технического творчества;	
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;	
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.	
Цель достигается по мере решения в единстве следующих задач:	
– формирование сознательного отношения к выбранной профессии;	
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;	
– формирование психологи профессионала;	
– формирование профессиональной культуры, этики профессионального общения;	
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

<b>2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП</b>	
<b>2.1 Требования к предварительной подготовке обучающегося</b>	
1	Б1.Б.11 Основы информационной безопасности
2	Б1.Б.22 Документоведение
3	Б2.В.01(У) Учебная практика - ознакомительная
<b>2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее</b>	
1	Б1.В.05 Комплексная защита в информационных системах персональных данных
2	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем
3	Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов
4	Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков

**3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ,  
СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ  
ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

<b>ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности</b>	
<b>Минимальный уровень освоения компетенции</b>	
Знать	Нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты
Уметь	Использовать технологии автоматизированного проектирования и структурных подход при проектировании информационных систем
Владеть	Навыками разработки политики безопасности ИС
<b>Базовый уровень освоения компетенции</b>	
Знать	Принципы построения объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных
Уметь	Определять ресурсы, необходимые для безопасности ИС
Владеть	Навыками проектирования ИС
<b>Высокий уровень освоения компетенции</b>	
Знать	Требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования
Уметь	Использовать методы и средства определения технологической безопасности функционирования ИС
Владеть	Навыками управления базами данных, методами снижения угроз ИС

**ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты**

<b>Минимальный уровень освоения компетенции</b>	
Знать	Терминологию, основные руководящие и регламентирующие документы в области информационной безопасности
Уметь	Проводить анализ угроз безопасности информационных систем
Владеть	Профессиональной терминологией в области ИБ
<b>Базовый уровень освоения компетенции</b>	
Знать	Основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ
Уметь	Реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ
Владеть	Навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации
<b>Высокий уровень освоения компетенции</b>	
Знать	Организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации
Уметь	Разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Владеть	Навыками работы с нормативно-правовыми актами

**ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**

<b>Минимальный уровень освоения компетенции</b>	
Знать	Основные средства и способы обеспечения информационной безопасности
Уметь	Определять комплекс мер и мероприятий для обеспечения информационной безопасности АС
Владеть	Профессиональной терминологией в области управления ИБ
<b>Базовый уровень освоения компетенции</b>	
Знать	Основные методы управления информационной безопасностью
Уметь	Разрабатывать предложения по совершенствованию системы управления ИБ АС
Владеть	Методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации
<b>Высокий уровень освоения компетенции</b>	
Знать	Основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России)
Уметь	Методы аттестации уровней защищенности АС
Владеть	Методиками модернизации, унификации систем, средств и технологий обеспечения

	информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России
--	--

**В результате освоения дисциплины обучающийся должен**

<b>Знать</b>	
1	Основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации
2	Правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях
3	Организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
<b>Уметь</b>	
1	Применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
2	Разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
<b>Владеть</b>	
1	Навыками работы с нормативными правовыми актами
2	Навыками организации и обеспечения режима секретности
3	Методами организации и управления деятельностью служб защиты информации на предприятии
4	Методами формирования требований по защите информации

**4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	<b>Раздел 1. Правовое обеспечение информационной безопасности</b>				
1.1	Правовое обеспечение информационной безопасности и пути его совершенствования /Лек/	4	4	ОПК-5	Л1.1, Л3.1, Э1 Э2
1.2	Подготовка к практической работе на тему «Задачи и функции правовой защиты информации» /Ср/	4	4	ОПК-5	Л1.1 Л3.1, Э1 Э2
1.3	Задачи и функции правовой защиты информации /Пр/	4	4	ОПК-5	Л1.2, Л1.3, , Э1
1.4	Институт правовой защиты государственной тайны /Лек/	4	4	ПК-4	Л1.1, Л2.2, Э1 Э2
1.5	Подготовка к практической работе на тему «Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)» /Ср/	4	6	ПК-4	Л1.2, Л1.3, Л2.1, Л2.3, Э1
1.6	Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ) /Пр/	4	4	ПК-4	Л1.2, Л1.3, Л2.1, Л2.3, Э1
1.7	Институт правовой защиты коммерческой тайны /Лек/	4	3	ПК-15	Л1.2, Л1.3, Э1
1.8	Подготовка к практической работе на тему «Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны» /Ср/	4	4	ПК-15	Л1.2, Л1.3, Л2.1, Л2.3, Э1
1.9	Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны /Пр/	4	4	ПК-15	Л1.1, Л1.2, Л3.1, Э2
1.10	Институт правовой защиты профессиональной тайны /Лек/	4	4	ПК-4, ПК-15	Л1.1, Л1.2, Л3.1, Э2
1.11	Подготовка к практической работе на тему «Банковская информация и обеспечение банковской тайны» /Ср/	4	4	ПК-4, ПК-15	Л1.1, Л1.2, Л3.1, Э2

1.12	Банковская информация и обеспечение банковской тайны /Пр/	4	4	ПК-4, ПК-15	Л1.1, Л1.2, Л3.1, Э2
1.13	Институт правовой защиты информации персонального характера (персональные данные) /Лек/	4	4	ОПК-5	Л1.3, Л2.1, Л3.1, Э1 Э2
1.14	Подготовка к практической работе на тему «Международные и российские документы, касающиеся использования персональных данных и их правовой защиты» /Ср/	4	4	ОПК-5	Л1.3, Л2.1, Л3.1, Э1 Э2
1.15	Международные и российские документы, касающиеся использования персональных данных и их правовой защиты /Пр/	4	4	ОПК-5	Л1.3, Л2.1, Л3.1, Э1 Э2
1.16	Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности /Лек/	4	3	ОПК-5	Л1.3, Л2.1, Л3.1, Э1 Э2
1.17	Подготовка к практической работе на тему «Авторский договор» /Ср/	4	4	ОПК-5	Л1.1, Л.2.2, Л3.1
1.18	Авторский договор /Пр/	4	4	ОПК-5	Л1.1, Л.2.2,
	<b>Раздел 2. Организационное обеспечение информационной безопасности</b>				
2.1	Сущность организационного обеспечения информационной безопасности и его место в комплексном обеспечении информационной безопасности и системы защиты информации /Лек/	4	4	ОПК-5 ПК-15	Л1.1, Л1.2, Л2.1, Л2.3, Л3.1, Э1 Э2
2.2	Подготовка к практической работе на тему «Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации» /Ср/	4	6	ОПК-5 ПК-15	Л1.1, Л1.3, Л2.1, Л.2.2, Л2.3, Л3.1, Э1 Э2
2.3	Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации /Пр/	4	4	ОПК-5 ПК-15	Л1.2, Л1.3, Л2.1, Л.2.2, Л2.3, Л3.1, Э1 Э2
2.4	Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну /Лек/	4	4	ПК-4	Л1.1, Л1.2, Л1.3, Л.2.2, Л2.3, Л3.1, Э1 Э2
2.5	Подготовка к практической работе на тему «Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну» /Ср/	4	6	ПК-4	Л1.1, Л1.3, Л2.1, Л.2.2, Л3.1, Э1
2.6	Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну /Пр/	4	2	ПК-4	Л1.1, Л1.2, , Л2.1, Л.2.2, Л3.1, Э2
2.7	Оформление допуска сотрудников к конфиденциальной информации /Лек/	4	4	ОПК-5	Л1.2, Л1.3, Л3.1, Э1 Э2
2.8	Подготовка к практической работе на тему «Оформление допуска сотрудников к конфиденциальной информации» /Ср/	4	6	ОПК-5	Л1.1, Л1.3, Л.2.2, Л2.3, Л3.1, Э1
2.9	Оформление допуска сотрудников к конфиденциальной информации /Пр/	4	4	ОПК-5	Л1.1, Л.2.2, Л2.3, Э2
2.10	Организация разрешительной системы доступа к конфиденциальной информации /Лек/	4	4	ОПК-5	Л1.1, Л1.3, Л2.1, Л2.3, Л3.1, Э1
2.11	Подготовка к практической работе на тему «Организация разрешительной системы доступа к конфиденциальной информации» /Ср/	4	6	ОПК-5	Л1.1, Л1.3, Л2.1, Л.2.2, Л3.1, Э1 Э2

2.12	Организация разрешительной системы доступа к конфиденциальной информации /Пр/	4	4	ОПК-5	Л1.1, Л1.2, Л2.2, Э1 Э2
2.13	Организация физической охраны предприятия /Лек/	4	4	ОПК-5, ПК-4, ПК-15	Л1.1, Л1.2, Л2.2, Л2.3
2.14	Подготовка к практической работе на тему «Организация физической охраны предприятия» /Ср/	4	6	ПК-15	Л1.1, Л1.2, Л2.2, Л2.3, Л3.1, Э1 Э2
2.15	Организация физической охраны предприятия /Пр/	4	2	ПК-15	Л1.1, Л1.2, Л3.1, Э1 Э2
2.16	Организация пропускного и внутриобъектового режимов /Лек/	4	4	ПК-15	Л1.3, Л2.1, Л3.1, Э1
2.17	Подготовка к практической работе на тему «Организация пропускного и внутриобъектового режимов» /Ср/	4	6	ПК-15	Л1.1, Л1.3, Л2.1, Э2
2.18	Организация пропускного и внутриобъектового режимов /Пр/	4	2	ПК-15	Л1.2, Л1.3, Л2.1, Э1 Э2
2.19	Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями /Лек/	4	4	ПК-4	Л1.3, Л2.1, Л2.3, Э1 Э2
2.20	Подготовка к практической работе на тему «Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями» /Ср/	4	6	ПК-4	Л1.1, Л1.2, Л2.2, Л2.3, Э2
2.21	Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями /Пр/	4	2	ПК-4	Л1.2, Л1.3, Л2.1, Э2
2.22	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Лек/	4	4	ПК-4	Л1.3, Л2.1, Э2
2.23	Подготовка к практической работе на тему «Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам» /Ср/	4	6	ПК-4	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Э1 Э2
2.24	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Пр/	4	4	ПК-4	Л1.3, Л2.1, Л2.3, Э1 Э2
2.25	Проработка теоретической части курсовой работы /Ср/	4	8	ОПК-5, ПК-4, ПК-15	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Э2
2.26	Разработка практической части курсовой работы /Ср/	4	8	ОПК-5, ПК-4, ПК-15	Л1.1, Л2.2, Л3.1, Э1 Э2
2.27	Защита курсовой работы /Пр/	4	6	ОПК-5, ПК-4, ПК-15	Л1.1, Л1.2, Л2.2, Л2.3, Л3.1, Э1 Э2
	<b>Раздел 3. Контроль знаний</b>				
3.1	Экзамен/	4	36	ОПК-5, ПК-4, ПК-15	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3, Л3.1, Э1 Э2

### **5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины и размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

<b>6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ</b>				
<b>6.1 Учебная литература</b>				
<b>6.1.1 Основная литература</b>				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л1.1	Ю. М. Краковский	Информационная безопасность и защита информации: учебное пособие	Иркутск: ИрГУПС, 2016	50
Л1.2	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% Онлайн
Л1.3	М.А. Лапина, А.Г. Ревин, В.И. Лапин	Информационное право : учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% Онлайн
<b>6.1.2 Дополнительная литература</b>				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Н.С. Кармановский, О.В. Михайличенко, С.В. Савков	Организационно-правовое и методическое обеспечение информационной безопасности: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/43579	СПб. : НИУ ИТМО, 2013	100% онлайн
Л2.2	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% онлайн
Л2.3	Коваленко, Ю.И	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/5163	М. : Горячая линия-Телеком, 2012	100% Онлайн
<b>6.1.3 Методические разработки</b>				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	- Иркутск: ИрГУПС, 2013	55
<b>6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине</b>				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Глухов Н.И.	Материалы для самостоятельной работы студентов	Личный кабинет студента	100% онлайн
<b>6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»</b>				
Э.1	Линия защиты «Сюртель» www.suritel.ru			
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
<b>6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем</b>				

<b>6.3.1 Перечень базового программного обеспечения</b>	
6.3.1.1	ОС Microsoft Windows XP Professional, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, <a href="https://ru.libreoffice.org">https://ru.libreoffice.org</a>
<b>6.3.2 Перечень специализированного программного обеспечения</b>	
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.
<b>6.3.3 Перечень информационных справочных систем</b>	
6.3.3.1	«Консультант +» <a href="http://www.consultant.ru/">http://www.consultant.ru/</a>
6.3.3.2	«Техэксперт» <a href="http://www.cntd.ru/">http://www.cntd.ru/</a>
<b>6.4 Перечень правовых и нормативных документов</b>	
6.4.1	Не предусмотрено

<b>7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ</b>	
1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации).
3	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.
5	Помещение А-521 (для хранения и профилактического обслуживания учебного оборудования).

<b>8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ</b>	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить задание на самостоятельную работу и



	<p>выучить лекционный материал к следующей теме. Систематическое выполнение заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины.</p>
Реферат	<p>Реферат – краткое письменное изложение материала по определенной теме, выполняется; цель – привить обучающимся навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу.</p> <p>Реферат – это самостоятельная учебно-исследовательская работа обучающегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер.</p> <p>Ознакомиться со структурой и оформлением реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).</p>
Курсовая работа	<p>Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).</p>
Самостоятельная работа	<p>Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удастся, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.</p>
<p>Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.</p>	

**Приложение 1 к рабочей программе по дисциплине  
Б1.Б.15 «Организационное и правовое обеспечение  
информационной безопасности»**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ  
для проведения текущего контроля успеваемости  
и промежуточной аттестации по дисциплине  
Б1.Б.15 «Организационное и правовое обеспечение  
информационной безопасности»**

## 1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина «Организационное и правовое обеспечение информационной безопасности» участвует в формировании компетенций:

**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности;

**ПК-4:** способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

**ПК-15:** способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

**Таблица траекторий формирования у обучающихся компетенций ОПК-5, ПК-4, ПК-15 при освоении образовательной программы**

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин / практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б1.Б.33 Метрология, стандартизация и сертификация	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б1.Б.27 Правоведение	6	2
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б2.В.03(П) Производственная практика - эксплуатационная	6	2
		Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем	8	3
		Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта	7	2
		Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов	7	2

и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Б1.В.ДВ.02.02 Защита электронного документооборота	7	2
	Б1.Б.21 Основы управления информационной безопасностью	78	2
	Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
	Б2.В.04(Пд) Производственная практика - преддипломная	8	3
	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3

**Таблица соответствия уровней освоения компетенций ОПК-5, ПК-4, ПК-15 планируемым результатам обучения**

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	Раздел 1. Правовое обеспечение информационной безопасности Раздел 2. Организационное обеспечение информационной безопасности Раздел 3. Контроль знаний	Минимальный уровень	Знать: терминологию, основные руководящие и регламентирующие документы в области информационной безопасности
				Уметь: проводить анализ угроз безопасности информационных систем
				Владеть: профессиональной терминологией в области ИБ
			Базовый уровень	Знать: основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ
				Уметь: реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ
				Владеть: навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации
			Высокий уровень	Знать: организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации
				Уметь: разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
				Владеть: навыками работы с нормативно-правовыми актами
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный	Раздел 1. Правовое обеспечение информационной безопасности Раздел 2. Организационное обеспечение информационной	Минимальный уровень	Знать: терминологию, основные руководящие и регламентирующие документы в области информационной безопасности
				Уметь: проводить анализ угроз безопасности информационных систем
				Владеть: профессиональной терминологией в области ИБ

	<p>подход к обеспечению информационной безопасности объекта защиты</p>	<p>безопасности Раздел 3. Контроль знаний</p>	<p>Базовый уровень</p>	<p>Знать: основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ Уметь: реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ Владеть: навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации</p>
			<p>Высокий уровень</p>	<p>Знать: организацию работы и нормативно-правовые акты и стандарты в области технической защиты конфиденциальной информации по аттестации объектов информатизации Уметь: разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации Владеть: навыками работы с нормативно-правовыми актами</p>
<p>ПК-15</p>	<p>способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>Раздел 1. Правовое обеспечение информационной безопасности Раздел 2. Организационное обеспечение информационной безопасности Раздел 3. Контроль знаний</p>	<p>Минимальный уровень</p>	<p>Знать: основные средства и способы обеспечения информационной безопасности Уметь: определять комплекс мер и мероприятий для обеспечения информационной безопасности АС Владеть: профессиональной терминологией в области управления ИБ</p>
			<p>Базовый уровень</p>	<p>Знать: основные методы управления информационной безопасностью Уметь: разрабатывать предложения по совершенствованию системы управления ИБ АС Владеть: методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации</p>
			<p>Высокий уровень</p>	<p>Знать: основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России) Уметь: методы аттестации уровней защищенности АС Владеть: методиками модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России</p>

**Программа контрольно-оценочных мероприятий  
за период изучения дисциплины**

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
<b>4 семестр</b>					
1	1	Текущий контроль	Тема «Задачи и функции правовой защиты информации»	ОПК-5	Реферат (письменно)
2	1	Текущий контроль	Тема «Задачи и функции правовой защиты информации»	ОПК-5	Доклад, сообщение (устно)
3	2	Текущий контроль	Тема «Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)»	ПК-4	Реферат (письменно)
4	2	Текущий контроль	Тема «Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)»	ПК-4	Доклад, сообщение (устно)
5	3	Текущий контроль	Тема «Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны»	ПК-15	Реферат (письменно)
6	3	Текущий контроль	Тема «Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны»	ПК-15	Доклад, сообщение (устно)
7	4	Текущий контроль	Тема «Банковская информация и обеспечение банковской тайны»	ПК-4 ПК-15	Реферат (письменно)
8	4	Текущий контроль	Тема «Банковская информация и обеспечение банковской тайны»	ПК-4 ПК-15	Доклад, сообщение (устно)
9	5	Текущий контроль	Тема «Международные и российские документы, касающиеся использования персональных данных и их правовой защиты»	ОПК-5	Реферат (письменно)
10	5	Текущий контроль	Тема «Международные и российские документы, касающиеся использования персональных данных и их правовой защиты»	ОПК-5	Доклад, сообщение (устно)
11	6	Текущий контроль	Тема «Авторский договор»	ОПК-5	Реферат (письменно)
12	6	Текущий контроль	Тема «Авторский договор»	ОПК-5	Доклад, сообщение (устно)
13	7	Текущий контроль	Тема «Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации»	ОПК-5, ПК-15	Реферат (письменно)
14	7	Текущий контроль	Тема «Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации»	ОПК-5, ПК-15	Доклад, сообщение (устно)
15	8	Текущий контроль	Тема «Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну»	ПК-4	Реферат (письменно)
16	8	Текущий контроль	Тема «Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну»	ПК-4	Доклад, сообщение (устно)

17	9	Текущий контроль	Тема «Оформление допуска сотрудников к конфиденциальной информации»	ОПК-5	Реферат (письменно)
18	9	Текущий контроль	Тема «Оформление допуска сотрудников к конфиденциальной информации»	ОПК-5	Доклад, сообщение (устно)
19	10	Текущий контроль	Тема «Организация разрешительной системы доступа к конфиденциальной информации»	ОПК-5	Реферат (письменно)
20	10	Текущий контроль	Тема «Организация разрешительной системы доступа к конфиденциальной информации»	ОПК-5	Доклад, сообщение (устно)
21	11	Текущий контроль	Тема «Организация физической охраны предприятия»	ПК-15	Реферат (письменно)
22	11	Текущий контроль	Тема «Организация физической охраны предприятия»	ПК-15	Доклад, сообщение (устно)
23	12	Текущий контроль	Тема «Организация пропускного и внутриобъектового режимов»	ПК-15	Реферат (письменно)
24	13	Текущий контроль	Тема «Организация пропускного и внутриобъектового режимов»	ПК-15	Доклад, сообщение (устно)
25	14	Тест	Изученный материал	ОПК-5, ПК-4, ПК-15	Перечень тестовых заданий
26	15	Текущий контроль	Тема «Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями»	ПК-4	Реферат (письменно)
27	15	Текущий контроль	Тема «Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями»	ПК-4	Доклад, сообщение (устно)
28	16	Текущий контроль	Тема «Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам»	ПК-4	Реферат (письменно)
29	16	Текущий контроль	Тема «Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам»	ПК-4	Доклад, сообщение (устно)
31	17	Текущий контроль	Защита курсовой работы /Пр/	ОПК-5, ПК-4, ПК-15	Курсовая работа
32	18	Промежуточная аттестация – экзамен	Разделы: 1. Правовое обеспечение информационной безопасности 2. Организационное обеспечение информационной безопасности 3. Контроль знаний	ОПК-5, ПК-4, ПК-15	Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно; оценка ответов на вопросы теста.

## **2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия

достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Реферат	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор реферата раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Может быть использовано для оценки знаний и умений обучающихся	Темы рефератов
2	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
3	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Курсовой работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовой работу
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

**Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена, а также шкала для оценивания уровня освоения компетенций**



Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

### **Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости**

#### Реферат

Шкала оценивания	Критерии оценивания
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное непонимание

	проблемы. Реферат обучающимся не представлен
--	---

### Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация Power Point, Flash–презентация, видео-презентация и др.) Используются дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация Power Point, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

### Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и

	/или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. курсовой работы не представлена преподавателю. Обучающийся не явился на защиту курсовой работы.

### Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание
Минимальный уровень освоения компетенции	20	Тестовые задания с выбором одного правильного ответа из нескольких	20
		Тестовые задания с выбором нескольких правильных ответов из множества ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	32
Высокий уровень освоения компетенции	5	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	35

### Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 80–87 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 72–79 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 66–71 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-66 баллов	Компетенция не сформирована

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

### **3.1 Перечень типовых тем рефератов**

1 Национальные интересы РФ в информационной сфере и угрозы их безопасности

- 2 Цели, принципы, методы и средства правового обеспечения информационной безопасности РФ.
- 3 Информационная среда как предмет правового регулирования.
- 4 Закон РФ «Об информации, информационных технологиях и о защите информации» как основа регулирования правоотношений в области информатизации.
- 5 Правовые основы организации деятельности государственных органов, обеспечивающих информационную безопасность РФ.
- 6 Организация деятельности подразделений, выполняющих функции обеспечения, в том числе и правового, информационной безопасности и защиты информации.
- 7 Состояние правового обеспечения информационной безопасности РФ в области использования информационной инфраструктуры и информационных ресурсов (фондов), информационно-телекоммуникационных систем и сетей связи.
- 8 Правовые основы деятельности подразделений защиты информации.
- 9 Особенности применения статей уголовного кодекса РФ, непосредственно посвященных защите ГТ
- 10 Правовые основы защиты служебной тайны.
- 11 Практика совершенствования института сведений ограниченного распространения как основа для формирования и совершенствования института служебной тайны
- 12 Особенности федерального закона «О персональных данных» и его связь с существующим международным законодательством
- 13 Понятия «организационное обеспечение информационной безопасности», «организационная защита информации» и «режим защиты информации».
- 14 Различные подходы к определению понятия «организация защиты информации».
- 15 Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.
- 16 Сущность организационных методов защиты информации.
- 17 Соотношение организационных и правовых методов защиты информации.
- 18 Соотношение организационных и технических методов защиты информации при использовании технических, в том числе, электронных средств передачи, обработки, хранения конфиденциальной информации.
- 19 Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях.
- 20 Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности.
- 21 Присвоение грифа и изменение грифа секретности работам, документам и изделиям.
- 22 Понятие «рассекречивание сведений». Основания для рассекречивания конфиденциальных сведений, документов и изделий.

### **3.2 Перечень типовых тем докладов, сообщений**

- 1 Понятие профессиональной тайны.
- 2 Источники права о профессиональной тайне.
- 3 Объекты и субъекты права на профессиональную тайну.
- 4 Критерии охраноспособности права на профессиональную тайну.
- 5 Права доверителя в отношении сведений, ставших на законных основаниях известными держателю профессиональной тайны.
- 6 Обязанности держателя профессиональной тайны. Защита доверителем своих прав.
- 7 Основные источники права о банковской тайне и их сопоставление
- 8 Банковская тайна, как часть коммерческой тайны банка, как коммерческого кредитного учреждения.
- 9 Организационные каналы передачи информации и организационные каналы разглашения и утечки информации и несанкционированного доступа к ней.

- 10 Возможности перекрытия каналов утечки информации организационно-правовыми и организационно-техническими методами.
- 11 Разработка проекта методики определения сведений, составляющих коммерческую тайну предприятия.
- 12 Анализ конкретных документов и определение возможности их рассекречивания.
- 13 Определение, каким нормативным документом необходимо руководствоваться для принятия решения о засекречивании или рассекречивании конкретных документов.

### **3.3 Перечень типовых тем курсовых работ**

- 1 Сущность теории информационного отражения.
- 2 Определение теории тайны
- 3 Роль и место личной тайны в системе тайн.
- 4 Юридическая схема запретов и дозволений в отношении институтов тайн.
- 5 Методы правовой защиты информации.
- 6 Меры правовой защиты информации.
- 7 Предупреждение и пресечение правонарушений в области информационной безопасности.
- 8 Цели и задачи обеспечения информационной безопасности России.
- 9 Определение понятий «безопасность информации» и «защита информации».
- 10 Право человека на доступ к информации.
- 11 Принципы отнесения сведений к гос. тайне и их засекречивание.
- 12 Правовой институт рассекречивания сведений, отнесенных к гос. тайне.
- 13 Институт служебной тайны – основа защиты конфиденциальных сведений в органах государственной власти и органах местного самоуправления.
- 14 Санкции за неправомерное распространение сведений, составляющих служ.тайну.
- 15 Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (Закон «Об информации информационных технологиях и защите информации»)
- 16 Информация как объект правовых отношений,(Закон «Об информации информационных технологиях и защите информации»)
- 17 Право на доступ к информации (Закон «Об информации информационных технологиях и защите информации»).
- 18 Ограничение доступа к информации (Закон «Об информации информационных технологиях и защите информации»).
- 19 Защита информации (Закон «Об информации информационных технологиях и защите информации»).
- 20 Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
- 21 Краткая характеристика основных этапов развития системы защиты коммерческой тайны в России и за рубежом.
- 22 Уровень нормативного регулирования отношений в области коммерческой тайны в России в период возрождения рыночной экономики.
- 23 Действительная и потенциальная коммерческая ценность.
- 24 Необходимые условия в коммерческой организации для сохранности сведений, составляющих коммерческую тайну.
- 25 Законодательство Российской Федерации о коммерческой тайне, (Закон «О коммерческой тайне»)
- 26 Что такое режим коммерческой тайны, (Закон «О коммерческой тайне»)
- 27 Права обладателя информации, составляющей коммерческую тайну
- 28 Охрана конфиденциальности информации в рамках трудовых отношений
- 29 Конфиденциальность персональных данных.
- 30 Условия обработки персональных данных.

- 31 Ответственность за неправомерное распространение персональных данных.
- 32 Применение гражданско-правового института к обязательствам работников, связанным с неправомерным распространением сведений.
- 33 Организационные источники и каналы утечки.
- 34 Силы, средства и условия организационной защиты информации.
- 35 Особенности системы организационной защиты информации.
- 36 Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий.
- 37 Подбор персонала на должности, связанные с работой с конфиденциальной информацией.
- 38 Допуск к секретной информации.
- 39 Организация доступа к конфиденциальной информации.
- 40 Текущая работа с персоналом, обладающим конфиденциальной информацией.
- 41 Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
- 42 Основные функции службы безопасности предприятия.
- 43 Состав и типовая структура службы безопасности.
- 44 Организация охраны территории, зданий, помещений и персонала.
- 45 Организация пропускного и внутриобъектового режимов.
- 46 Требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.
- 47 Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
- 48 Аналитическая работа как основа управления системой организационной защиты информации.
- 49 Методики аналитической работы, обеспечивающие управляемость системы организационной защиты информации.
- 50 Планирование процессов организационной защиты информации.
- 51 Оценка и анализ состояния системы ОЗИ как основа планирования
- 52 Контроль функционирования системы организационной защиты информации.
- 53 Сущность контроля как функции управления.
- 54 Основы обеспечения безопасности человека. Общие положения безопасности человека
- 55 Контроль функционирования системы организационной защиты информации.
- 56 Факторы, влияющие на безопасность предпринимательской деятельности в России, и состояние ее защиты
- 57 Безопасность внутриофисной работы — противодействие мошенничеству, хищениям и утечке информации
- 58 Кражи, совершаемые персоналом
- 59 Анализ рисков нарушений политики информационной безопасности
- 60 Мероприятия по обеспечению политики информационной безопасности
- 61 Изучение конкурентов по рынку аналогичных товаров и услуг
- 62 Концепция информационной безопасности предприятия

### 3.4 Тест

- 1 Что такое политика информационной безопасности
  - а) Методология защиты информации
  - б) Идеология информационной безопасности +
  - в) Концепция защиты информации
- 2 Какой федеральный закон считается рамочным по защите информации?
  - а) ФЗ «О коммерческой тайне»
  - б) ФЗ «О персональных данных»

в) ФЗ «Об информации, информационных технологиях и о защите информации»+

3 Номер ФЗ «Об информации, информационных технологиях и о защите информации» является:

- а) 188 ФЗ
- б) 152 ФЗ
- в) 149 ФЗ +
- г) 214 ФЗ

4 Лицензирование деятельности по распространению криптографических средств, осуществляет:

- а) ФСБ +
- б) ФСТЭК
- в) Роскомнадзор
- г) Ростехнадзор

5 Подключение ИС, обрабатывающих служебную тайну к сети Интернет:

- а) допускается
- б) не допускается
- в) допускается только с использованием специально предназначенных для этого средств +
- г) допускается только с использованием средств защиты известных производителей

6 Специальная проверка это

- а) выявление возможных каналов утечки информации Российскими техническими средствами
- б) определение соответствия условий эксплуатации ОИ требованиям аттестатов соответствия объектам защиты
- в) проверки технических средств на наличие возможно внедренных электронных устройств перехвата информации +

7 Каким документов определяются права человека на доступ к информации?

- а) Доктриной ИБ
- б) Конституцией +
- в) ФЗ «О коммерческой тайне»

8 В соответствии с каким ГОСТом производится аттестация объекта информатизации?

- а) ГОСТ РО 0043-004-2013. +
- б) ГОСТ ISO 17799
- в) BS 7799

9 Источниками угроз несанкционированного доступа являются:

(выберите все верные варианты ответов)

- а) нарушители +
- б) природные факторы
- в) носители вредоносных программ +
- г) аппаратные закладки +
- д) отказы оборудования
- е) отказы программного обеспечения

10 Основные направления обеспечения информационной безопасности указанные в Доктрине ИБ

- а) стратегическое развитие военных конфликтов, которые могут возникнуть в результате применения информационных технологий;
- б) совершенствование Вооруженных Сил Российской Федерации
- в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере; +
- г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере; +

11 Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных являются:

(выберите все верные варианты ответов)

- а) кражи технических средств информационной системы
- б) утечки акустической (речевой) информации +
- в) утечки информации реализуемые через общедоступные информационные сети
- г) утечки видовой информации +
- д) утечки информации по каналам побочных электромагнитных излучений +
- е) утечки информации реализуемые через интернет

12 Документом, определяющим лицензируемые виды деятельности, является:

- а) Постановление правительства РФ от 26 января 2006 г. № 45 Об организации лицензирования отдельных видов деятельности
- б) Постановление Правительство РФ от 15 августа 2006 г. № 504 О лицензировании деятельности по технической защите конфиденциальной информации
- в) Постановление Правительства РФ от 31 августа 2006 г. № 532 О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации
- г) ФЗ «О лицензировании отдельных видов деятельности» 99-ФЗ от 4 мая 2011 г. +
- д) ФЗ «О техническом регулировании» 184-ФЗ от 27 декабря 2002 г.

13 Средствами защиты информации, подлежащими сертификации являются:

(выберите все верные варианты ответов)

- а) строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн
- б) детали интерьера, используемые для размещения ИСПДн
- в) средства контроля эффективности применения средств защиты информации +
- г) средства контроля эффективности прочности ограждений
- д) средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности +

14 Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

- а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации; +
- б) осуществление контроля за населением РФ с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;
- в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления,



повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры; +

г) допущения иностранного контроля за функционированием объектов информатизации, на территории Российской Федерации;

15 Перечислить нормативно-методические документы по анализу угроз и уязвимостей

а) BS 7799-3 +

б) ISO 27005 +

в) BSI IT Baseline Protection Manual +

г) ГОСТ 3328

16 «Информационная система» это:

а) совокупность информации, информационных технологий и технических средств +

б) совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему

в) совокупность информационных технологий и технических средств

г) совокупность информации, технических средств и персонала, обслуживающего информационную систему

д) совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему

17 Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК:

а) 4

б) 5

в) 6

г) 7

д) 8 +

е) 9

18 Классами защищенности автоматизированных систем от несанкционированного доступа являются: (выберите все верные варианты ответов)

а 1Е

б 2Г

в 2А +

г 2В

д 3С

е 3Б +

19 Основными элементами ИС являются:

(выберите все верные варианты ответов)

а помещения для размещения технических средств

б персональные данные, содержащиеся в базах данных +

в контролируемая зона

г информационные технологии +

д обслуживающий персонал

е технические средства обработки информации +

ж ограждающие конструкции

з технические средства перевозки материальных носителей информации

20 Каким нормативными документами регламентируется деятельность по выявлению угроз

а) BS 7799 +

б) ISO 27005 +

в) BSI IT Baseline Protection Manual +

г) ГОСТ 3328

д) Приказ ФСТЭК № 31

21 К методам и способам защиты информации в информационных системах относятся методы и способы защиты информации от \_\_\_\_\_ (Ответ несанкционированного доступа) и методы и способы защиты информации от \_\_\_\_\_ (Ответ утечки по техническим каналам)

22 Классификация угроз информационной безопасности, по виду активов делится на угрозы, направленные против \_\_\_\_\_ (Ответ информационных активов) и угрозы, направленные против \_\_\_\_\_ (Ответ технических средств)

23 Основные требования к системе защиты автоматизированной системы управления должны содержать - \_\_\_\_\_ (Ответ класс защищенности) автоматизированной системы управления, перечень \_\_\_\_\_ (Ответ нормативных правовых актов), локальных правовых актов, \_\_\_\_\_ (Ответ методических документов), национальных стандартов и стандартов организаций, которым должна \_\_\_\_\_ (Ответ соответствовать) автоматизированная система управления и объекты защиты автоматизированной системы управления на каждом из ее уровней; +

24 При проектировании системы защиты автоматизированной системы управления необходимо: определять типы \_\_\_\_\_ (Ответ субъектов доступа (пользователи, процессы и иные субъекты доступа)) и \_\_\_\_\_ (Ответ объектов доступа), являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа), определять \_\_\_\_\_ (Ответ методы управления доступом) (дискреционный, мандатный, ролевой), типы \_\_\_\_\_ (Ответ доступа) (чтение, запись, выполнение) и правила \_\_\_\_\_ (Ответ разграничения) доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления, выбирать меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления;

25 Разрабатывать организационно-распорядительные документы по защите информации, определяющие правила и процедуры (политики) включает в себя \_\_\_\_\_ (Ответ реализацию отдельных мер) защиты информации в автоматизированной системе управления в рамках ее \_\_\_\_\_ (Ответ системы защиты) и \_\_\_\_\_ (Ответ планирования мероприятий) по обеспечению защиты информации в автоматизированной системе управления; +

26 Определите класс автоматизированной системы по следующим классификационным признакам: АС, в которой работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается «Служебная тайна». Класс АС \_\_\_\_\_

27 Ущерб от реализации риска может быть - \_\_\_\_\_ и \_\_\_\_\_  
Ответ 7 материальный и нематериальный

28 При внедрении организационных мер защиты информации осуществляются: введение \_\_\_\_\_ (Ответ ограничений) на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации \_\_\_\_\_ и \_\_\_\_\_ (Ответ технических средств и программного обеспечения), а также \_\_\_\_\_ (Ответ реализация) правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа.

- 29 Опишите основные организационно-правовые мероприятия для обеспечения защиты информации в автоматизированной системе
- 30 Охарактеризуйте операторский уровень многоуровневой системы защиты
- 31 Опишите процесс внедрения системы защиты автоматизированной системы управления
- 32 Что такое объект информатизации на промышленном предприятии
- 33 Дайте развернутую характеристику ISO 27005

### **3.5 Перечень теоретических вопросов к экзамену**

1. Типовые организационные структуры государственной системы защиты информации.
2. Функции контроля и надзора органа государственной власти в области обеспечения безопасности и защиты информации.
3. Специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности.
4. Классификация услуг организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности.
5. Специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственного регулирования.
6. Какие функции выполняет служба безопасности предприятия для решения задачи физической защиты.
7. Функции службы безопасности предприятия для решения задачи обеспечения информационной безопасности.
8. Структура полномасштабной системы обеспечения безопасности и защиты информации.
9. Специфика организации и выполнения охранных функций.
10. Специальные мероприятия и действия сотрудников службы безопасности по организации объектовых режимов.
11. Основное назначение корпоративной нормативной базы службы безопасности.
12. Структура корпоративной нормативной базы службы безопасности.
13. Разделы типового формата положений о структурных подразделениях службы безопасности.
14. Перечень и краткая характеристика основных нормативных документов процедурного уровня ИБ.
15. Чем определяется срок жизненного цикла корпоративной нормативной базы по информационной безопасности.
16. Различия в определениях политики информационной безопасности.
17. Отличия нормативно-методических документов политики безопасности от нормативных документов процедурного уровня.
18. Особенности документального оформления политики безопасности, и чем они объясняются.
19. Типовое содержание политики безопасности, оформленной в виде единого документа.
20. Назначение Концепции обеспечения информационной безопасности организации.
21. Содержание Концепции обеспечения информационной безопасности организации.
22. Цель и задача аудита информационной безопасности.
23. Методология деятельности по обеспечению безопасности объекта на основе политики безопасности.
24. Перечень контрольных мероприятий и действий по оценке уровня безопасности объекта.
25. Определение понятия «режимный объект» и видов обеспечения его безопасности.
26. Цель и задачи организации пропускного режима.
27. Нормативная основа организации пропускного режима и каково ее общее содержание.
28. Порядок пропуска (прохода) физических лиц на территорию режимного объекта.

29. Правила въезда (выезда) транспортных средств на территорию режимного объекта.
30. Особенности организации охраны режимного объекта.
31. Суть и содержание нормативной основы организации охранных мероприятий.
32. Действия охраны при тревоге и других чрезвычайных ситуациях.
33. Цель и задачи организационного обеспечения внутриобъектового режима.
34. Содержание организационного обеспечения режима секретности.
35. Организация конфиденциального делопроизводства.
36. Организационные процедуры обеспечения режима секретности.
37. Организация засекречивания сведений, составляющих государственную тайну.
38. Организация допуска и доступа к сведениям, составляющим государственную тайну.
39. Правила обращения секретных документов.
40. Основные правила организации секретного делопроизводства.
41. Организационный режим делопроизводства и обращения документов с грифом «Для служебного пользования» (ДСП).
42. Особенности современных систем автоматизированного документооборота.
43. Принципиальные отличия технологии workflow от традиционных систем автоматизации управленческой деятельности.
44. Суть и содержание работ по противодействию технической разведке.
45. Определение понятия и краткая характеристика аттестация объектов информатизации.
46. Основной перечень работ по аттестации объектов информатизации.
47. Цель и задачи проведения служебных расследований инцидентов нарушений информационной безопасности.
48. Организация проведения служебного расследования инцидента при реализации угрозы информационной безопасности.
49. Определение эффективности менеджмента в области информационной безопасности.
50. Суть и содержание использования организационных схем определения надежности персонала
51. Суть и содержание использования организационных схем определения профессиограмм при подборе кадров.
52. Нормативно-правовая основа для введения дополнительных ограничений по контролю за деятельностью персонала.
53. Организационные процедуры для составления психологического портрета работника.
54. Особенности верификации сведений о работнике при его приеме на работу.
55. Методы психологического тестирования и графологической экспертизы.
56. Специфика использования метода психофизиологического тестирования.
57. Цель ранжирования должностей по степени риска управления бизнес-процессами.
58. Участие службы безопасности в процедурах увольнения сотрудников.
59. Определение мотивации как метода управления персоналом.
60. Суть и содержание метода положительного стимулирования.
61. Особенности метода отрицательного стимулирования.
62. Создание ориентирующих условий для персонала.
63. Актуальность вопросов самообучения и повышения квалификации.
64. Основные специальности, по которым осуществляется подготовка кадров в области обеспечения информационной безопасности.
65. Основные направления образовательной деятельности в области обеспечения информационной безопасности

### **3.6 Перечень типовых практических заданий к экзамену**

1. Разработать политику информационной безопасности для ИрНИТУ
2. Разработать концепцию информационной безопасности для ООО «ВСЦ ЕВРАС»
3. Подготовить перечень защищаемой информации на ООО «ВСЦ ЕВРАС»

4. Подготовить перечень защищаемых персональных данных согласно Приказа № 21 ФСТЭК в администрации г. Иркутска
5. Подготовить частную модель угроз персональным данным на ООО «ВСЦ ЕВРАС» исходя из «Базовой модели угроз персональным данным ФСТЭК»
6. Оценить уровни защищенности конфиденциальной информации ИрГУПС
7. Подготовить модель внутреннего нарушителя «Аппарата губернатора Иркутской Области»

#### **4 Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Реферат	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит реферат или по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,2; предоставляет реферат преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Курсовой работа	Обучаемый самостоятельно, под руководством преподавателя выполняет курсовую работу на заданную тему. Тема предлагается в общем виде. Конкретные методы и инструменты для ее разработки обучаемый выбирает самостоятельно. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

Для организации и проведения промежуточной аттестации (в форме экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

- перечень теоретических вопросов к экзамену для оценки знаний;
- перечень типовых простых практических заданий к экзамену для оценки умений;
- перечень типовых практических заданий к экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

### **Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения**

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.


Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

### **Образец экзаменационного билета**

	<p><b>Экзаменационный билет № 1</b> по дисциплине «<b>Организационное и правовое обеспечение информационной безопасности</b>» __ семестр</p>	<p>Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС _____</p>
<ol style="list-style-type: none"> <li>1. Функции контроля и надзора органа государственной власти в области обеспечения безопасности и защиты информации.</li> <li>2. Основное назначение корпоративной нормативной базы службы безопасности .</li> <li>3. Разработать макет документа: политикf информационной безопасности для ИрНИТУ</li> </ol>		

В разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.