ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.О.53 Методология построения защищенных автоматизированных систем

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108

Формы промежуточной аттестации
очная форма обучения:
зачет 8 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	8	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	72	**72**
– лекции	24	**24**
– практические (семинарские)	24	**24**
– лабораторные	24	**24**
Самостоятельная работа	36	**36**
Итого	108	**108**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
Старший преподаватель кафедры ИСиЗИ, П.Н. Наседкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

Зав. кафедрой, к. э. н, доцент Т.К. Кириллова

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цель дисциплины

1	теоретическая и практическая подготовка обучающихся к деятельности, связанной с проектированием защищенных автоматизированных информационных систем в своей профессиональной деятельности

1.2 Задачи дисциплины

1	получение знаний и умений сбора и анализа исходных данных для проектирования защищенных автоматизированных систем, определение требований к защищенным автоматизированным системам
2	участие в проведении аттестации и контрольных проверок на предмет соответствия автоматизированных систем требованиям защиты информации

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

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 психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.О.27 Основы информационной безопасности
2	Б1.О.40 Информационные технологии
3	Б1.О.41 Аттестация объектов информатизации
4	Б1.О.43 Основы кибернетики
5	Б1.О.47 Теоретические основы компьютерной безопасности
6	Б1.О.52 Аудит информационной безопасности
7	Б2.О.01(У) Учебная - ознакомительная практика
8	Б2.О.02(У) Учебная - учебно-лабораторная практика

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
2	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей	ОПК-1.2 Умеет пользоваться нормативными документами, современным программным обеспечением в области информационной безопасности	Знать: основные нормативные акты и руководящие документы по созданию защищенных автоматизированных систем; базовые модели угроз безопасности информации; методики проведения оценок соответствия требованиям безопасности информации
		Уметь: определять перечень и основные требования нормативных актов и руководящих документов по созданию защищенных автоматизированных систем; составлять частные модели угроз безопасности информации; описывать технологические процессы в защищенных автоматизированных системах
		Владеть: специальной терминологией; методами проведения контроля эффективности применения мер

личности, общества и государства;		защиты информации; навыками проведения инструментального контроля эффективности применения мер защиты информации
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	ОПК-4.1.1 Знает основные направления и методы организационной защиты информации в автоматизированных системах	Знать: перечень основных нормативных документов, определяющих порядок применения мер по обеспечению информационной безопасности; требования нормативных документов по защите информации различного уровня доступа и распространения; методики проведения оценок соответствия требованиям безопасности информации
		Уметь: определять необходимый перечень организационно-распорядительных документов по формированию, организации и поддержке выполнения комплекса мер по обеспечению информационной безопасности; составлять план проведения контрольных мероприятий; описывать технологические процессы в защищенных автоматизированных системах
		Владеть: основными терминами и определениями; навыками разработки организационно-распорядительных документов; навыками проведения инструментального контроля эффективности применения мер защиты информации
	ОПК-4.1.2 Умеет анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития	Знать: перечень базовых моделей угроз безопасности информации; основные положения базовых моделей угроз безопасности информации; основные угрозы безопасности информации при эксплуатации АС
		Уметь: составлять перечень базовых угроз безопасности информации для АС; адаптировать базовый набор угроз безопасности информации к организационно-техническим условиям эксплуатации АС; определять актуальные угрозы безопасности АС
		Владеть: навыками составления перечня угроз безопасности информации; навыками разработки методики проведения аттестационных исследований; навыками составления частных моделей угроз безопасности информации.
	ОПК-4.1.3 Имеет навыки организационных методов защиты информации в автоматизированных системах	Знать: перечень основных нормативных актов и руководящих документов по созданию защищенных автоматизированных систем; назначение и сферу действия основных нормативных актов и руководящих документов по созданию защищенных автоматизированных систем; основные положения нормативных актов и руководящих документов по созданию защищенных автоматизированных систем
		Уметь: определять перечень нормативных актов и руководящих документов по созданию защищенных автоматизированных систем; определять основные требования нормативных актов и руководящих документов по созданию защищенных автоматизированных систем; определять основные показатели защищенности автоматизированных систем в зависимости от класса защищенности АС
		Владеть: специальной терминологией; навыками поиска нормативных актов и руководящих документов по созданию защищенных автоматизированных систем; навыками составления плана написания политики информационной безопасности

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.0	**Раздел 1. Нормативная база и руководящие документы по построению защищенных автоматизированных систем (АС).**						
1.1	Тема 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС (лекция/лабораторная в форме ПП).	8	2	1		2	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.2	Тема 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации. Термины и определения. Синонимы. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение (лекция/практика/лабораторная в форме ПП).	8	2	1		2	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.3	Тема 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные (лекция/лабораторная в форме ПП).	8	2	1		2	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.4	Тема 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).	8	2	1		2	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.5	Тема 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к сегментам АС. Классификация средств защиты автоматизированных систем (лекция/ лабораторная в форме ПП).	8	2	1		2	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.6	Тема 6. Показатели защищенности от несанкционированного доступа к информации (лекция).	8	2	1		2	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.7	Тема 7. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ) (лекция/ лабораторная в форме ПП).	8	2	2		4	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.8	Тема 8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классифи	8	2	2		4	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.9	Лабораторная работа № 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС	8			2		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.10	Лабораторная работа № 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации.	8			2		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
	Термины и определения. Синонимы. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение						ОПК-4.1.3
1.11	Лабораторная работа № 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные	8			2		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.12	Лабораторная работа № 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).	8			2		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.13	Лабораторная работа № 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к сегментам АС. Классификация средств защиты автоматизированных систем.	8			4		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.14	Лабораторная работа № 6. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ).	8			2		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
1.15	Лабораторная работа № 7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классификация средств защиты электронной подписи.	8			4		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
2.0	**Раздел 2. Моделирование угроз безопасности информации.**						
2.1	Тема 9. Базовые модели угроз безопасности информации. Базовая модель угроз безопасности персональных данных (лекция).	8	2	2		4	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
2.2	Тема 10. Методика оценки угроз в системах и сетях на этапе создания и эксплуатации. Сценарии реализации угроз безопасности информации в определении актуальных угроз (лекция).	8	2	2		4	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
2.3	Лабораторная работа № 8. Поиск в открытых источниках и изучение моделей угроз безопасности информации, в том числе и частных моделей угроз. Построение модели угроз безопасности информации (практика/ лабораторная в форме ПП).	8			4		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
3.0	**Раздел 3. Методики проведения оценки соответствия требованиям безопасности информации.**						
3.1	Тема 11. Этапы построения защищенных автоматизированных систем (лекция).	8	2	5		4	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
3.2	Тема 12. Оценка соответствия принятых мер требованиям безопасности информации Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности. Экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты. (лекция/ лабораторная в форме ПП).	8	2	5		4	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
3.3	Лабораторная работа № 9. Оценка соответствия принятых мер требованиям безопасности информации Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности. Экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты.	8			2		ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
	Форма промежуточной аттестации – зачет	8					ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3
	Итого часов (без учёта часов на промежуточную аттестацию)		24	24	24	36	

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 оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — URL: https://e.lanbook.com/book/292247 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 120 с. — URL: https://e.lanbook.com/book/257564 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Ковцур, М. М. Безопасность беспроводных локальных сетей : учебное пособие / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахрамеева. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2021. — 71 с. — URL: https://e.lanbook.com/book/279623 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Наседкин П.Н. Методические указания по изучению дисциплины Б1.О.53 Методология построения защищенных автоматизированных систем по направлению подготовки 10.03.01 Информационная безопасность, профиль: Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) / П.Н. Наседкин ; ИрГУПС. – Иркутск :	Онлайн

	ИрГУПС, 2024. – 15 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47559_1480_2024_1_signed.pdf	
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.1.10	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License.	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Б-202 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, мультимедиапроектор, экран, компьютер. Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты).
3	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации Основное оборудование: Специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной). Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты).
4	Учебная аудитория Д-313 для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: Специализированная мебель, мультимедиапроектор, экран, компьютер. Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты).
5	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; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей

	области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
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 домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций.

	По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Методология построения защищенных автоматизированных систем» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Методология построения защищенных автоматизированных систем» участвует в формировании компетенций:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
8 семестр				
1.0	**Раздел 1. Нормативная база и руководящие документы по построению защищенных автоматизированных систем (АС)**			
1.1	Текущий контроль	Тема 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС (лекция/лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации. Термины и определения. Синонимы. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение (лекция/практика/лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные (лекция/лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.4	Текущий контроль	Тема 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.5	Текущий контроль	Тема 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к сегментам АС. Классификация средств защиты автоматизированных систем (лекция/ лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)

1.6	Текущий контроль	Тема 6. Показатели защищенности от несанкционированного доступа к информации (лекция).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.7	Текущий контроль	Тема 7. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ) (лекция/ лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.8	Текущий контроль	Тема 8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классифи	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
1.9	Текущий контроль	Лабораторная работа № 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
1.10	Текущий контроль	Лабораторная работа № 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации. Термины и определения. Синонимы. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
1.11	Текущий контроль	Лабораторная работа № 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
1.12	Текущий контроль	Лабораторная работа № 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
1.13	Текущий контроль	Лабораторная работа № 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)

		сегментам АС. Классификация средств защиты автоматизированных систем.		
1.14	Текущий контроль	Лабораторная работа № 6. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
1.15	Текущий контроль	Лабораторная работа № 7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классификация средств защиты электронной подписи.	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Моделирование угроз безопасности информации**			
2.1	Текущий контроль	Тема 9. Базовые модели угроз безопасности информации. Базовая модель угроз безопасности персональных данных (лекция).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
2.2	Текущий контроль	Тема 10. Методика оценки угроз в системах и сетях на этапе создания и эксплуатации. Сценарии реализации угроз безопасности информации в определении актуальных угроз (лекция).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
2.3	Текущий контроль	Лабораторная работа № 8. Поиск в открытых источниках и изучение моделей угроз безопасности информации, в том числе и частных моделей угроз. Построение модели угроз безопасности информации (практика/ лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)
3.0	**Раздел 3. Методики проведения оценки соответствия требованиям безопасности информации**			
3.1	Текущий контроль	Тема 11. Этапы построения защищенных автоматизированных систем (лекция).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
3.2	Текущий контроль	Тема 12. Оценка соответствия принятых мер требованиям безопасности информации Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности. Экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты. (лекция/ лабораторная в форме ПП).	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Собеседование (устно)
3.3	Текущий контроль	Лабораторная работа № 9. Оценка соответствия принятых мер требованиям безопасности информации Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности. Экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты.	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Лабораторная работа (письменно/устно)

	Промежуточная аттестация	Все разделы	ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
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 двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	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 к зачету
2	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по	Фонд тестовых заданий

		дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«зачтено»	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
	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
	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
«не зачтено»	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	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения,

		демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»		Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	«не зачтено»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования

«Тема 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС (лекция/лабораторная в форме ПП).»

1. Что такое информационная безопасность, и какова ее роль в современных организациях?
2. Какие основные угрозы могут возникать для информационной безопасности предприятий/организаций?
3. Какие ключевые термины и определения связаны с информационной безопасностью?
4. Расскажите о структуре защищенных автоматизированных систем (АС). Какие компоненты они включают?
5. Каковы основные принципы построения защищенных АС?
6. Что такое аутентификация и какие методы аутентификации существуют?
7. Каким образом реализуется авторизация в информационных системах?
8. Объясните принципы работы систем контроля доступа к информационным ресурсам.
9. Какие меры защиты могут быть приняты для обеспечения конфиденциальности данных в защищенных АС?
10. Какие технологии шифрования используются для защиты информации в транспорте и в хранении на устройствах?

Образец типового варианта вопросов для проведения собеседования

«Тема 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации. Термины и определения. Синонимы.

1. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение (лекция/практика/лабораторная в форме ПП).»
2. Какова роль нормативно-правовой базы в области защиты информации, и почему она важна для организаций?
3. Какие основные классификации нормативно-правовой базы по защите информации вы знаете?
4. Назовите основные нормативно-правовые акты в области защиты информации, которые применяются в вашей стране.
5. Какие термины и определения используются в нормативно-правовых актах по защите информации?
6. Какие синонимы существуют для терминов, используемых в области защиты информации?
7. Можете ли вы описать логическую схему локально вычислительной сети в информационной системе организации?
8. Какие режимы пользования обычно устанавливаются в информационных системах организаций, и для чего они нужны?
9. Какой состав оборудования обычно присутствует в информационной системе организации?
10. Какое программное обеспечение обычно используется для защиты информации в информационной системе организации?
11. Какие меры безопасности могут быть приняты для обеспечения защиты информации в локальной вычислительной сети организации?
12. Образец типового варианта вопросов для проведения собеседования
13. «Тема 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные (лекция/лабораторная в форме ПП).»

Образец типового варианта вопросов для проведения собеседования

«Тема 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые

данные»

1. Какие специальные нормативные документы регулируют обработку конфиденциальных данных в вашей организации?
2. Как вы понимаете концепцию конфиденциальных данных и почему она важна для организации?
3. Какие шаги вы предпринимаете для обеспечения защиты конфиденциальных данных в рамках своей работы?
4. Какие типы персональных данных могут обрабатываться в вашей организации и в каких целях?
5. Каковы основные требования законодательства относительно обработки персональных данных в вашей стране?
6. Какие меры безопасности вы применяете для защиты персональных данных от несанкционированного доступа?
7. Какие специфические права имеют субъекты персональных данных согласно законодательству вашей страны?
8. Как организация управляет открытыми данными и как они могут использоваться для обеспечения прозрачности деятельности?
9. Какие методы вы используете для мониторинга и контроля потоков информации в организации?
10. Какие последствия могут возникнуть в случае нарушения требований по обработке и защите конфиденциальных и персональных данных в вашей организации?

Образец типового варианта вопросов для проведения собеседования

«Тема 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС.

1. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).»
2. Какие основные угрозы и уязвимости вы видите для средств вычислительной техники и автоматизированных систем в современном информационном мире?
3. Какие методы аутентификации и авторизации могут быть использованы для защиты доступа к информации в компьютерных системах?
4. Как вы понимаете концепцию "принципа наименьших привилегий" в контексте защиты информации и какие меры можно применить для её реализации?
5. Каковы основные этапы разработки общей концепции защиты автоматизированных систем, и какие шаги вы предпринимаете для их реализации?
6. Какие методы обнаружения и предотвращения несанкционированного доступа к информации вы применяете в вашей работе?
7. Какие категории злоумышленников могут представлять угрозу для безопасности информации в автоматизированных системах, и какие методы защиты от них вы используете?
8. Каковы основные принципы и подходы к разработке безопасных архитектур информационных систем?
9. Как вы проводите анализ рисков безопасности информации в автоматизированных системах и какие действия предпринимаете на основе полученных результатов?
10. Какие инструменты и технологии вы используете для мониторинга и аудита безопасности информационных систем?
11. Как вы следите за последними трендами и разработками в области информационной безопасности, и какие действия предпринимаете для постоянного обновления своих знаний и навыков?

Образец типового варианта вопросов для проведения собеседования

«Тема 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к

сегментам АС. Классификация средств защиты автоматизированных систем (лекция/ лабораторная в форме ПП).»

1. Что такое классификация автоматизированных систем, и почему она важна для обеспечения безопасности информации?
2. Какие критерии вы используете для классификации сегментов автоматизированных систем с точки зрения их значимости и уровня защиты?
3. Какие основные этапы включает в себя процесс проведения классификации сегментов автоматизированных систем, и какие шаги вы предпринимаете на каждом из них?
4. Что такое акт классификации автоматизированных систем, и какие данные должны быть включены в этот документ?
5. Какие требования к сегментам автоматизированных систем обычно учитываются при их классификации с точки зрения защиты информации?
6. Какие методы и инструменты вы используете для оценки уровня защиты сегментов автоматизированных систем?
7. Какие виды средств защиты автоматизированных систем вы рассматриваете при их классификации, и какие из них предпочтительны в различных ситуациях?
8. Каковы основные принципы выбора средств защиты для сегментов автоматизированных систем в зависимости от их классификации?
9. Как вы обеспечиваете соответствие средств защиты автоматизированных систем установленным требованиям безопасности?
10. Какие вызовы и трудности могут возникнуть при проведении классификации и выборе средств защиты для автоматизированных систем, и как вы их преодолеваете?

Образец типового варианта вопросов для проведения собеседования
«Тема 6. Показатели защищенности от несанкционированного доступа к информации (лекция).»

1. Какие основные показатели защищенности от несанкционированного доступа к информации вы считаете наиболее важными для оценки безопасности информационных систем?
2. Какие типы метрик вы используете для измерения эффективности системы защиты от несанкционированного доступа к информации?
3. Какие параметры вы учитываете при определении уровня риска несанкционированного доступа к информации в организации?
4. Какие инструменты и методики вы применяете для анализа и оценки показателей защищенности информационных систем?
5. Какие стратегии и тактики вы применяете для улучшения показателей защищенности от несанкционированного доступа к информации?
6. Как вы интерпретируете и используете результаты аудита защищенности от несанкционированного доступа к информации для улучшения общей ситуации в организации?
7. Какие методы и подходы вы используете для мониторинга и отслеживания изменений в показателях защищенности от несанкционированного доступа к информации?
8. Какова ваша стратегия в отношении реагирования на инциденты несанкционированного доступа к информации, и какие шаги вы предпринимаете для их предотвращения в будущем?
9. Какие тенденции и новации в области защиты информации вы учитываете при разработке и совершенствовании своих методов и практик?
10. Как вы оцениваете эффективность внедренных мер по защите от несанкционированного доступа к информации, и какие планы у вас есть на будущее для улучшения этой эффективности?

Образец типового варианта вопросов для проведения собеседования
«Тема 7. Программное обеспечение средств защиты информации. Классификация по уровню

контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ) (лекция/ лабораторная в форме ПП).»

1. Как вы понимаете понятие "недекларированные возможности" в программном обеспечении средств защиты информации (СЗИ), и почему они могут быть опасны для безопасности?
2. Какие основные классификации по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении средств защиты информации вы знаете?
3. Какие методы и технологии обеспечивают высокий уровень контроля отсутствия недекларированных возможностей в программном обеспечении средств защиты информации?
4. Какие меры безопасности вы принимаете при выборе и установке программного обеспечения средств защиты информации для минимизации риска появления недекларированных возможностей?
5. Какие инструменты и методики используются для анализа программного обеспечения средств защиты информации на наличие недекларированных возможностей?
6. Каковы основные этапы процесса тестирования программного обеспечения средств защиты информации на предмет отсутствия недекларированных возможностей?
7. Какие действия вы предпринимаете в случае обнаружения недекларированных возможностей в программном обеспечении средств защиты информации?
8. Какие стандарты и рекомендации следует учитывать при разработке и использовании программного обеспечения средств защиты информации с учётом контроля отсутствия недекларированных возможностей?
9. Какие методы и подходы вы применяете для обновления и модернизации программного обеспечения средств защиты информации с целью улучшения контроля отсутствия недекларированных возможностей?
10. Как вы оцениваете эффективность программного обеспечения средств защиты информации с точки зрения контроля отсутствия недекларированных возможностей, и какие шаги предпринимаете для постоянного улучшения этой эффективности?

Образец типового варианта вопросов для проведения собеседования «Тема 8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классифи»

1. Что такое Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), и какие основные аспекты они охватывают?
2. Каково определение класса межсетевого экрана, и какие критерии учитываются при его классификации?
3. Какие классы защиты существуют для средств вычислительной техники (СВТ), и какие основные требования обычно предъявляются к каждому из них?
4. Как происходит классификация средств защиты систем обнаружения вторжений, и какие характеристики учитываются при этом?
5. Какие классы защиты существуют для средств антивирусной защиты информации, и какие методы обычно используются для их определения?
6. Что такое классы защиты средств доверенной загрузки, и как они помогают обеспечить безопасность системы?
7. Какие классы защиты средств контроля съемных машинных носителей существуют, и каковы основные характеристики каждого из них?
8. Как происходит классификация операционных систем для обеспечения защиты

информации, и какие факторы учитываются при этом?
9. Какие классы защиты существуют для изделий информационных технологий, и какие требования они предъявляют к уровню безопасности?
10. Что такое средства криптографической защиты информации (СКЗИ), каковы их основные классификации, и как они взаимодействуют с другими средствами защиты?

Образец типового варианта вопросов для проведения собеседования «Тема 9. Базовые модели угроз безопасности информации. Базовая модель угроз безопасности персональных данных (лекция).»

1. Что такое базовые модели угроз безопасности информации, и какова их роль в анализе угроз?
2. Какие основные компоненты включает в себя базовая модель угроз безопасности информации?
3. Какие виды угроз безопасности информации вы знаете и как они классифицируются в рамках базовой модели?
4. Каковы основные принципы и подходы к анализу угроз безопасности информации с использованием базовых моделей?
5. Какие методы и техники используются для идентификации и оценки угроз безопасности информации с использованием базовых моделей?
6. Какие могут быть последствия для организации при возникновении угроз безопасности информации, описанных в базовых моделях?
7. Как вы оцениваете уровень риска в контексте базовых моделей угроз безопасности информации, и какие действия предпринимаете для его снижения?
8. Какие меры предосторожности вы рекомендуете принимать для защиты от угроз безопасности информации, исходя из базовых моделей?
9. Как базовая модель угроз безопасности персональных данных отличается от общей базовой модели угроз безопасности информации?
10. Какие основные виды угроз безопасности персональных данных могут возникать, и какие меры защиты вы рекомендуете применять для их предотвращения?

Образец типового варианта вопросов для проведения собеседования «Тема 10. Методика оценки угроз в системах и сетях на этапе создания и эксплуатации. Сценарии реализации угроз безопасности информации в определении актуальных угроз (лекция).»

1. Какие этапы включает в себя методика оценки угроз в системах и сетях на этапе создания и эксплуатации, и какие инструменты вы используете для каждого из них?
2. Какие основные шаги вы предпринимаете при анализе и оценке потенциальных угроз безопасности информации в системах и сетях?
3. Какие методы и техники вы применяете для выявления сценариев реализации угроз безопасности информации на этапе оценки угроз?
4. Какова роль статического и динамического анализа при оценке угроз безопасности информации, и какие методы вы используете для их проведения?
5. Какие категории активов и уязвимостей учитываются при определении актуальных угроз безопасности информации, и как вы их классифицируете?
6. Какие инструменты и технологии вы используете для моделирования сценариев реализации угроз безопасности информации на этапе оценки угроз?
7. Как вы проводите анализ вероятности реализации угроз безопасности информации, и какие факторы вы учитываете при этом?
8. Какие методы и подходы вы применяете для оценки потенциального вреда, который могут причинить реализованные угрозы безопасности информации?
9. Какие меры предосторожности вы рекомендуете для минимизации рисков, выявленных на этапе оценки угроз?
10. Как вы обновляете и дорабатываете методику оценки угроз в системах и сетях на этапе создания и эксплуатации, учитывая новые угрозы и тенденции в области

информационной безопасности?

Образец типового варианта вопросов для проведения собеседования
«Тема 11. Этапы построения защищенных автоматизированных систем (лекция).»

1. Какие основные этапы включает в себя процесс построения защищенных автоматизированных систем?
2. Какие шаги вы предпринимаете на этапе определения требований к безопасности при построении защищенных автоматизированных систем?
3. Какова роль анализа угроз и уязвимостей на этапе проектирования защищенных автоматизированных систем, и какие методы вы используете для их выявления?
4. Как вы определяете и классифицируете активы и угрозы при построении защищенных автоматизированных систем?
5. Какие принципы и подходы вы используете при разработке архитектуры защищенных автоматизированных систем?
6. Какие меры безопасности вы внедряете на этапе разработки и программирования защищенных автоматизированных систем?
7. Как происходит тестирование и верификация защищенных автоматизированных систем на предмет соответствия требованиям безопасности?
8. Какие меры вы принимаете на этапе внедрения и настройки защищенных автоматизированных систем для обеспечения их безопасной эксплуатации?
9. Как вы реагируете на обнаружение уязвимостей или инцидентов безопасности в защищенных автоматизированных системах, и какие шаги предпринимаете для их устранения?
10. Как вы обеспечиваете постоянное обновление и совершенствование защищенных автоматизированных систем с учетом изменяющихся угроз и требований безопасности?

Образец типового варианта вопросов для проведения собеседования
«Тема 12. Оценка соответствия принятых мер требованиям безопасности информации
Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности.
Экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты. (лекция/ лабораторная в форме ПП).»

1. Как вы оцениваете соответствие принятых мер безопасности информации установленным требованиям, и какие методы вы используете для этой цели?
2. Какие основные критерии вы учитываете при выборе средств защиты информации (СЗИ) от несанкционированного доступа (НСД) и средств криптографической защиты информации (СКЗИ) в соответствии с определенными классами защищенности?
3. Какие этапы включает в себя процесс подбора СЗИ и СКЗИ согласно классам защищенности, и какие документы вы используете для документирования этого процесса?
4. Как вы определяете экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты информации, и какие факторы учитываете при этом?
5. Какие методы и инструменты вы используете для оценки экономической эффективности и эффективности в целом при внедрении средств защиты информации?
6. Какова роль стоимостного анализа при выборе и внедрении СЗИ и СКЗИ в системе защиты информации?
7. Как вы обеспечиваете соответствие выбранных средств защиты информации установленным бюджетным ограничениям?
8. Как вы оцениваете риски, связанные с возможным несоответствием принятых мер безопасности информации установленным требованиям, с учетом экономических аспектов?
9. Какие стратегии и тактики вы используете для оптимизации экономических затрат на техническое и программно-аппаратное обеспечение в системе защиты информации?
10. Какие рекомендации вы можете дать организации для эффективного управления

затратами на техническое и программно-аппаратное обеспечение в системе защиты информации, с учетом требований безопасности?

3.2 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС»

Задание:

– привести примеры описания структуры организаций по направлению деятельности: наличие филиалов, удаленных подразделений, кол-во сотрудников, структура организации.

– используя справочно-правовые системы и другие официальные источники информации по законодательству Российской Федерации приведите НПА и дайте ответ на один из следующих вопросов:

1. Содержание и требования к оформлению технического задания на создание защищенной АС;
2. Сформулируйте основные требования, предъявляемые к современным АС;
3. Содержание и требования к оформлению пояснительной записки;
4. Модель взаимодействия открытых систем;
5. Содержание и требования к оформлению документа «Описание комплекса аппаратных и программных средств»;
6. Содержание и требования к оформлению документа «Спецификация оборудования и программных средств»;
7. Основные функции сеансового, транспортного и сетевого уровней модели взаимодействия открытых систем;
8. Содержание и требования к оформлению документа «Рабочая документация»;
9. Содержание и требования к оформлению документа «Спецификация оборудования, изделий и материалов»;
10. Содержание и требования к оформлению документа «Программы и методики испытаний»;
11. Содержание и требования к оформлению документа «Эксплуатационная документация»;
12. Содержание и требования к оформлению документа «Руководство по эксплуатации и техническому обслуживанию защищённых АС»;
13. Содержание и требования к оформлению документа «Руководство пользователя защищённых АС»;
14. Содержание и требования к оформлению документа «Справочник по аварийной сигнализации»;
15. Содержание и требования к оформлению документа «Исполнительная документация»;
16. Основные требования к техническому заданию на создание защищённых АС;
17. Требования к содержанию технического проекта на создание защищённых АС;
18. Требования к содержанию документа «Рабочая документация» на защищённых АС;
19. Требования к содержанию документа «Программы и методики испытаний».

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации. Термины

и определения. Синонимы. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение»

Задание:

– привести пример описания информационной системы управления организацией:

1. логическая схема локально-вычислительной сети,
2. режимы пользования,
3. состав оборудования,
4. программное обеспечение,
5. модель угроз безопасности информации.

– используя литературные источники в области ИБ Методологические основы построения защищенных автоматизированных систем:

1. Определить и описать основные этапы построения защищенных АС;
2. Указать по каждой позиции этапа построения защищенных АС используемые актуальные версии НПА:
   2.1. представить документы НПА в виде электронного архива.

1 Этап «Формирование требований к ЗАС» содержит:

1) _____;
2) _____;
3) _____;

2 Этап «Разработка концепции ЗАС» включает в себя:

1) _____;
2) _____;
3) _____;
4) _____.

3 Этап «Техническое задание» посвящен _____на создание ЗАС.

4 Этап «Эскизный проект» посвящен:

1) _____;
2) _____;

5 Этап «Технический проект» включает:

1) _____;
2) _____;
3) _____;
4) _____.

6 Этап «Рабочая документация» посвящен: разработке _____.

7 Этап «Ввод в действие» состоит из: _____.

8 Этап «Сопровождение» включает:

1) _____;
2) _____.

На практике перечисленные этапы могут быть сведены к меньшему количеству:

1. _____;
2. _____;
3. _____;
4. _____;
5. _____.

ГОСТ допускает объединение стадий 3 и 4, либо 4 и 5.

Таким образом, в большинстве случаев **(**из-за временных и стоимостных ограничений) создание ЗАС реализуется по сокращенным схемам:

1. _____;
2. _____;
3. _____.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные»

Задание:

– привести примеры и описания потоков информации в организации: конфиденц-ые, ПДн, открытые данные.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).»

Задание:

– разработать общую концепцию защиты ИС управления организации.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к сегментам АС. Классификация средств защиты автоматизированных систем.»

Задание:

– разработать пример классификации демилитаризованных зон-сегментов (ip-план) в организации. Составить акт классификации.

– используя литературные источники в области ИБ:

1. Описать процесс классификации автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требований по защите информации в АС различных классов;
   1.1. Указать и представить документ НПА в виде электронного архива в соответствие с которым осуществляется классификация АС.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 6. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ).»

Задание: описать уровни контроля на отсутствие недекларированных возможностей (НДВ) в ПО средств защиты информации и провести анализ СЗИ.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 7. Специальные требования и рекомендации по технической защите

конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классификация средств защиты электронной подписи.»

Задание: разработать техническое задание на создание защищенной АС. Выбор бизнес-процесса и сектор экономики произвести самостоятельно.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 8. Поиск в открытых источниках и изучение моделей угроз безопасности информации, в том числе и частных моделей угроз. Построение модели угроз безопасности информации (практика/ лабораторная в форме ПП).»

Задание:

– разработать и предоставить ЧМУ для выбранного любого виртуального предприятия:

1.1. Указать и представить документы НПА в виде электронного архива в соответствии с которым осуществляется разработка ЧМУ АС.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 9. Оценка соответствия принятых мер требованиям безопасности информации Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности. Экономические затраты на техническое и программно-аппаратное обеспечение в системе защиты.»

Задание:

– разработать стенд-систему защиты информации для АС.

– описать основные этапы аттестации АС в защищённом исполнении.

– описать экономические затраты (текущие и капитальные) на техническое и программно-аппаратное обеспечение в системе защиты.

3.3 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 1. Введение. Основные термины и определения. Описание общей организационной структуры предприятий/организаций и общих принципов построения защищенных АС (лекция/лабораторная в форме ПП).	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 2. Классификация нормативно-правовой базы по защите информации. Основные нормативно-правовые акты в области защиты информации. Термины и определения. Синонимы. Описание информационной системы организации: логическая схема локально вычислительной сети, режимы пользования, состав оборудования, программное обеспечение (лекция/практика/лабораторная в форме ПП).	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2		Знание	2 – ОТЗ

ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 3. Специальные нормативные документы. Обзор и назначение. Описание потоков информации в организации: конфиденциальные данные, персональные данные, открытые данные (лекция/лабораторная в форме ПП).		2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 4. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Разработка общей концепции защиты АС. Поиск в открытых источниках и изучение концепций безопасности организаций(лекция/практика/лабораторная в форме ПП).	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 5. Классификация автоматизированных систем и требования по защите информации. Проведение классификации сегментов АС. Акт классификации. Определение требований к сегментам АС. Классификация средств защиты автоматизированных систем (лекция/ лабораторная в форме ПП).	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 6. Показатели защищенности от несанкционированного доступа к информации (лекция).	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 7. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (НДВ) в программном обеспечении (ПО) средств защиты информации (СЗИ) (лекция/ лабораторная в форме ПП).	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Определение класса межсетевого экрана, средств вычислительной техники (СВТ), классификация средств защиты систем обнаружения вторжений, классификация защищенности средств антивирусной защиты информации, классы защиты средств доверенной загрузки, классы защиты средств контроля съемных машинных носителей, классификация операционных систем для обеспечения защиты информации, классификация защищенности изделий информационных технологий, классификация средств криптографической защиты информации (СКЗИ), классифи	Знание	2 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 2 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 9. Базовые модели угроз безопасности информации. Базовая модель угроз безопасности персональных данных (лекция).	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1– ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 10. Методика оценки угроз в системах и сетях на этапе создания и эксплуатации. Сценарии реализации угроз безопасности информации в определении актуальных угроз (лекция).	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1– ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 11. Этапы построения защищенных автоматизированных систем (лекция).	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-1.2 ОПК-4.1.1 ОПК-4.1.2 ОПК-4.1.3	Тема 12. Оценка соответствия принятых мер требованиям безопасности информации Подбор СЗИ от НСД и СКЗИ согласно определенным классам защищенности. Экономические затраты на техническое и программно-	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 2– ЗТЗ
		Действие	0 – ОТЗ

	аппаратное обеспечение в системе защиты. (лекция/ лабораторная в форме ПП).		0 – ЗТЗ
		Итого	40 – ОТЗ 41– ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

3.4 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Основные термины и определения
2. Классификация нормативно-правовой базы по защите информации
3. Федеральные законы, регламентирующие деятельность по защите информации и их основные положения.
4. Основные специальные нормативные документы
5. Основные российские стандарты в области защиты информации
6. Основные международные стандарты в области защиты информации
7. Классификация информации в соответствии с действующим законодательством РФ.
8. Права и обязанности обладателя информации.
9. Защита информации в соответствии с действующим законодательством РФ.
10. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Общие положения
11. Определение НСД.
12. Основные принципы защиты от НСД
13. Модель нарушителя в АС
14. Основные способы НСД
15. Основные направления обеспечения защиты от НСД
16. Основные функции СРД
17. Основные функции обеспечивающие средства для СРД
18. Способы реализации СРД
19. СРД Secret Net. Назначение и основные функции
20. Основные характеристики технических средств защиты от НСД
21. Организация работ по защите от НСД. Классификация АС
22. Основные этапы классификации АС
23. Необходимые исходные данные для проведения классификации конкретной АС
24. Определяющие признаки, по которым производится группировка АС в различные классы
25. Группы и классы АС
26. Требования по защите информации от НСД для АС. Основные подсистемы системы защиты информации от НСД
27. Требования к классам защищенности 3 группы
28. Требования к классам защищенности 2 группы
29. Требования к классам защищенности 1 группы
30. Показатели защищенности МЭ
31. Классы защищенности МЭ
32. Требования к четвертому классу защищенности МЭ
33. Сертификация МЭ по требованиям безопасности информации
34. Недекларированные возможности. РД, определяющий требования к отсутствию НДВ
35. Требования к уровню контроля отсутствия НДВ
36. Требования к четвертому уровню контроля
37. СВТ. Защита от НСД к информации. Общие положения РД
38. Показатели защищенности СВТ от НСД

39. Дискреционный принцип контроля доступа
40. Мандатный принцип контроля доступа
41. Требования к показателям пятого класса защищенности
42. СТР-К. Основные положения документа
43. Основные вопросы защиты, определяемые СТР-К
44. Защищаемые объекты информатизации
45. Основные вопросы защиты конфиденциальной информации в соответствии с СТР-К
46. Ответственность и организация работ по защите конфиденциальной информации
47. Перечень сведений конфиденциального характера
48. Стадии создания системы защиты информации
49. Мероприятия, выполняемые на предпроектной стадии
50. Мероприятия, выполняемые на стадии проектирования
51. Мероприятия, выполняемые на стадии ввода в действие объекта информатизации
52. Технический паспорт на объект информатизации

3.5 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1. Основные термины и определения
2. Классификация нормативно-правовой базы по защите информации
3. Федеральные законы, регламентирующие деятельность по защите информации и их основные положения.
4. Основные специальные нормативные документы
5. Основные российские стандарты в области защиты информации
6. Основные международные стандарты в области защиты информации
7. Классификация информации в соответствии с действующим законодательством РФ.
8. Права и обязанности обладателя информации.
9. Защита информации в соответствии с действующим законодательством РФ.
10. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Общие положения
11. Определение НСД.
12. Основные принципы защиты от НСД
13. Модель нарушителя в АС
14. Основные способы НСД
15. Основные направления обеспечения защиты от НСД
16. Основные функции СРД
17. Основные функции обеспечивающие средства для СРД
18. Способы реализации СРД
19. СРД Secret Net. Назначение и основные функции
20. Основные характеристики технических средств защиты от НСД
21. Организация работ по защите от НСД. Классификация АС
22. Основные этапы классификации АС
23. Необходимые исходные данные для проведения классификации конкретной АС
24. Определяющие признаки, по которым производится группировка АС в различные классы
25. Группы и классы АС
26. Требования по защите информации от НСД для АС. Основные подсистемы системы защиты информации от НСД
27. Требования к классам защищенности 3 группы
28. Требования к классам защищенности 2 группы
29. Требования к классам защищенности 1 группы
30. Показатели защищенности МЭ
31. Классы защищенности МЭ
32. Требования к четвертому классу защищенности МЭ
33. Сертификация МЭ по требованиям безопасности информации

34. Недекларированные возможности. РД, определяющий требования к отсутствию НДВ
35. Требования к уровню контроля отсутствия НДВ
36. Требования к четвертому уровню контроля
37. СВТ. Защита от НСД к информации. Общие положения РД
38. Показатели защищенности СВТ от НСД
39. Дискреционный принцип контроля доступа
40. Мандатный принцип контроля доступа
41. Требования к показателям пятого класса защищенности
42. СТР-К. Основные положения документа
43. Основные вопросы защиты, определяемые СТР-К
44. Защищаемые объекты информатизации
45. Основные вопросы защиты конфиденциальной информации в соответствии с СТР-К
46. Ответственность и организация работ по защите конфиденциальной информации
47. Перечень сведений конфиденциального характера
48. Стадии создания системы защиты информации
49. Мероприятия, выполняемые на предпроектной стадии
50. Мероприятия, выполняемые на стадии проектирования
51. Мероприятия, выполняемые на стадии ввода в действие объекта информатизации
52. Технический паспорт на объект информатизации

3.6 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Реализация систем контроля доступа
2. Оценка класса защищенности СВТ (сертификация СВТ)
3. Рекомендуемая структура модели угроз безопасности информации в соответствие с методикой ФСТЭК от 05.02.2021 г. при оценки угроз безопасности информации.
4. Техническое (частное техническое) задание на разработку СЗИ
5. Аттестат соответствия требованиям по безопасности информации

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

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
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия

Для организации и проведения промежуточной аттестации 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 и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.