ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «02» июня 2023 г. № 424-1

Б1.О.50 Комплексная защита в информационных системах персональных данных

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	36	**36**
– практические (семинарские)	36	**36**
– лабораторные		
Самостоятельная работа	36	**36**
Итого	108	**108**

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу
Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.
00920FD815CE68F8C4CA795540563D259C с 07.02.2024 05:46 по 02.05.2025 05:46 GMT+03:00
Подпись соответствует файлу документа

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):
к.э.н., доцент, Н.И. Глухов

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «2» июня 2023 г. № 12

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	раскрытие сущности и значения комплексного обеспечения безопасности персональных данных, обеспечение обучающихся теоретическими знаниями и практическими навыками, необходимыми для проведения работ по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями российского законодательства
1.2 Задачи дисциплины	
1	изучение организационно-правовых и технических вопросов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных
2	проведение классификации информационных систем обработки персональных данных
3	изучение методов и процедур выявления угроз безопасности информации, построение модели угроз
4	создание подсистемы информационной безопасности при организации обработки персональ-ных данных
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.26 Теория информации
2	Б1.О.33 Сети и системы передачи информации
3	Б1.О.47 Теоретические основы компьютерной безопасности
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-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение	ОПК-10.1 Знает основные требования к формированию политики информационной безопасности, программные средства скрытого информационного воздействия, утечки информации по техническим каналам	Знать: основные требования к формированию политики информационной безопасности, программные средства скрытого информационного воздействия, утечки информации по техническим каналам
		Уметь: применять основные требования к формированию политики информационной безопасности, программные средства скрытого информационного воздействия, утечки информации по техническим каналам
		Владеть: основными требованиями к формированию политики информационной безопасности, программные средства скрытого информационного воздействия, утечки информации по техническим каналам
	ОПК-10.2 Умеет применять методы определения причин,	Знать: причины, виды, источники и каналы утечки, искажения информации

комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	видов, источников и каналов утечки, искажения информации, организовывает и поддерживает выполнение комплекса мер по обеспечению информационной безопасности	Уметь: организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
		Владеть: навыками и методами определения причин, видов, источников и каналов утечки, искажения информации
	ОПК-10.3 Имеет навыки работы технического специалиста по организации и обеспечению информационной безопасности компьютерных систем при обработке информации на объекте защиты	Знать: навыки работы технического специалиста по организации и обеспечению информационной безопасности компьютерных систем при обработке информации на объекте защиты
		Уметь: понимать навыки работы технического специалиста по организации и обеспечению информационной безопасности компьютерных систем при обработке информации на объекте защиты
		Владеть: навыками работы технического специалиста по организации и обеспечению информационной безопасности компьютерных систем при обработке информации на объекте защиты

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. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах.**						
1.1	Тема 1. Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации	8	3				ОПК-10.1 ОПК-10.2 ОПК-10.3
1.2	Тема 2. Доктрина информационной безопасности Российской Федерации	8		4		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
1.3	Тема 3. Содержание и основные положения Федерального закона "О персональных данных"	8	3	3		3	ОПК-10.1 ОПК-10.2
1.4	Тема 4. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных	8	3	4		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
1.5	Тема 5. Обзор международных и национальных стандартов в сфере информационной безопасности	8	3				ОПК-10.1 ОПК-10.2
2.0	**Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных.**						
2.1	Тема 6. Общие положения и классификация угроз безопасности персональных данных	8	3	4		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
2.2	Тема 7. Классификация информационных систем персональных данных	8	3				ОПК-10.1 ОПК-10.2 ОПК-10.3
2.3	Тема 8. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации	8		3		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
2.4	Тема 9. Угрозы утечки информации по техническим каналам	8	3				ОПК-10.1 ОПК-10.2 ОПК-10.3
2.5	Тема 10. Средства обнаружения технических каналов утечки информации	8		4		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
2.6	Тема 11. Комплекс мероприятий по выявлению каналов утечки информации	8	3				ОПК-10.1 ОПК-10.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
							ОПК-10.3
2.7	Тема 12. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных	8		3		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
2.8	Тема 13. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей ИСПДн	8	3				ОПК-10.2 ОПК-10.3
2.9	Тема 14. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа	8		4		3	ОПК-10.2 ОПК-10.3
2.10	Тема 15. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования	8	3				ОПК-10.1 ОПК-10.2 ОПК-10.3
2.11	Тема 16. Методы и способы защиты персональных данных от несанкционированного доаступа в зависимости от класса информационной системы	8		3		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
3.0	**Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных.**						
3.1	Тема 17. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн	8	3			3	ОПК-10.1 ОПК-10.2 ОПК-10.3
3.2	Тема 18. Уведомление об обработке (о намерении осуществлять обработку) персональных данных	8	1				ОПК-10.1 ОПК-10.2 ОПК-10.3
3.3	Тема 19. Особенности обработки персональных данных без использования средств автоматизации	8		4		3	ОПК-10.1 ОПК-10.2 ОПК-10.3
3.4	Тема 20. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн	8	2			3	ОПК-10.3
	Форма промежуточной аттестации – зачет	8					
	Итого часов (без учёта часов на промежуточную аттестацию)		36	36		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	Лапина, М. А. Информационное право : учебное пособие / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; под ред. И. Ш. Килясханов. — Москва : Юнити-Дана|Закон и право, 2017. — 336 с. — URL: https://biblioclub.ru/index.php?page=book&id=685428 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. — Москва, Берлин	Онлайн

	: Директ-Медиа, 2015. — 255 с. — URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.04.2024). — Текст : электронный.	
6.1.1.3	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — URL: https://e.lanbook.com/book/264242 (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	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. — Самара : Самарский государственный архитектурно-строительный университет, 2014. — 113 с. — URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2.2	Минин, И. В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / И. В. Минин, О. В. Минин. — Новосибирск : Новосибирский государственный технический университет, 2011. — 20 с. — URL: https://biblioclub.ru/index.php?page=book&id=228779 (дата обращения: 18.04.2024). — 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	Глухов Н.И. Методические указания по изучению дисциплины Б1.О.50 Комплексная защита в информационных системах персональных данных по направлению подготовки – 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или сфере в профессиональной деятельности) / Н.И. Глухов; ИрГУПС. – Иркутск: ИрГУПС, 2023. – 11 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_7695_1480_2023_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.2.2	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 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 (переносной), экран (переносной), компьютер
3	Учебная аудитория Д-213 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	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
Самостоятельная работа	Обучение по дисциплине «Комплексная защита в информационных системах персональных данных» 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 «Комплексная защита в информационных системах персональных данных» участвует в формировании компетенций:

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

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. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах**			
1.1	Текущий контроль	Тема 1. Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Доктрина информационной безопасности Российской Федерации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Содержание и основные положения Федерального закона "О персональных данных"	ОПК-10.1 ОПК-10.2	Собеседование (устно)
1.4	Текущий контроль	Тема 4. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
1.5	Текущий контроль	Тема 5. Обзор международных и национальных стандартов в сфере информационной безопасности	ОПК-10.1 ОПК-10.2	Собеседование (устно)
2.0	**Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных**			
2.1	Текущий контроль	Тема 6. Общие положения и классификация угроз безопасности персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.2	Текущий контроль	Тема 7. Классификация информационных систем персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3	Тестирование (компьютерные технологии)
2.3	Текущий контроль	Тема 8. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.4	Текущий контроль	Тема 9. Угрозы утечки информации по техническим каналам	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.5	Текущий контроль	Тема 10. Средства обнаружения технических каналов утечки информации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)

2.6	Текущий контроль	Тема 11. Комплекс мероприятий по выявлению каналов утечки информации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.7	Текущий контроль	Тема 12. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.8	Текущий контроль	Тема 13. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей ИСПДн	ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.9	Текущий контроль	Тема 14. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа	ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.10	Текущий контроль	Тема 15. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
2.11	Текущий контроль	Тема 16. Методы и способы защиты персональных данных от несанкционированного доаступа в зависимости от класса информационной системы	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
3.0	**Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных**			
3.1	Текущий контроль	Тема 17. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
3.2	Текущий контроль	Тема 18. Уведомление об обработке (о намерении осуществлять обработку) персональных данных	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
3.3	Текущий контроль	Тема 19. Особенности обработки персональных данных без использования средств автоматизации	ОПК-10.1 ОПК-10.2 ОПК-10.3	Собеседование (устно)
3.4	Текущий контроль	Тема 20. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн	ОПК-10.3	Собеседование (устно)
	Промежуточная аттестация	Все разделы		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	Тестирование (компьютерные технологии)	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

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

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	Высокий

	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	
	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

Тестирование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

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
«Политика безопасности»

1. Организационно-правовой статус сотрудников информационной безопасности?
2. Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характер?
3. Средства и системы защиты ИС?
4. Локальная безопасность. Антивирусная защита?
5. Защищенные каналы с использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент или других, сертифицированных ФСТЭК?
6. Разграничение прав доступа к информационным системам и системам хранения данных?
7. Организация физической безопасности
8. Как осуществляется хранение информации конфиденциального характера локально на компьютере?
9. Ответственность за соблюдение положений Политики ИБ?
10. Дублирование, резервное копирование и хранение информации

Образец типового варианта вопросов для проведения собеседования
«Назначение, структура и содержание управления комплексной системой защиты информации»

1. Понятие «принятие решений» в широком и узком смысле.
2. Понятие «управленческое решение».
3. Что такое технология разработки решения?
4. Цель, объект и предмет разработки управленческих решений
5. Классификация видов решений.
6. Программируемые и непрограммируемые управленческие решения.
7. Основанные на суждениях, интуитивные и творческие решения.
8. Решения, типичные для общих функций управления
9. Составляющие задачи принятия управленческого решений.
10. Понятие проблемной ситуации.
11. Ограничения и критерии при принятии решения.
12. Схема процесса принятия управленческого решения.
13. Механизм предпочтений лица, принимающего решение.
14. Варианты алгоритмов разработки и принятия решений с учетом проблем и задач, стоящих перед лицами, принимающими решения.

15. Содержание и особенности этапов полного процесса разработки управленческого решения.
16. Линейное уравнение: характеристика, построение, решение примеров задач.

3.2 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-10.1 ОПК-10.2 ОПК-10.3	Тема 1. Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 2. Доктрина информационной безопасности Российской Федерации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2	Тема 3. Содержание и основные положения Федерального закона "О персональных данных"	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 4. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2	Тема 5. Обзор международных и национальных стандартов в сфере информационной безопасности	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 6. Общие положения и классификация угроз безопасности персональных данных	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 7. Классификация информационных систем персональных данных	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 8. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 9. Угрозы утечки информации по техническим каналам	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 10. Средства обнаружения технических каналов утечки информации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 11. Комплекс мероприятий по выявлению каналов утечки информации	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 12. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.2 ОПК-10.3	Тема 13. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей ИСПДн	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.2 ОПК-10.3	Тема 14. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 15. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1		Знание	1 – ЗТЗ

ОПК-10.2 ОПК-10.3	Тема 16. Методы и способы защиты персональных данных от несанкционированного доаступа в зависимости от класса информационной системы	Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 17. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 18. Уведомление об обработке (о намерении осуществлять обработку) персональных данных	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Тема 19. Особенности обработки персональных данных без использования средств автоматизации	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-10.3	Тема 20. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
		Итого	30 – ОТЗ 30 – 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.

Образец типового варианта итогового теста,
предусмотренного рабочей программой дисциплины

1. Выберите правильное определение термина «информация»:
   а) совокупность содержащихся в базах данных сведений;
   б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
   в) сведения (сообщения, данные) воспроизводимые различными системами;
   г) сведения (сообщения, данные) независимо от формы их представления.

2. Выберите правильное определение термина «обладатель информации»:
   а) лицо, самостоятельно создавшее информацию;
   б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
   в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
   г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Предоставление информации – это

Ответ: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

4. Защищаемые помещения – это

Ответ: помещения, специально предназначенные для проведения конфиденциальных мероприятий.

5. Выберите правильное определение термина «контролируемая зона»:
   а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;
в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;
г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

а) методы и способы защиты информации от несанкционированного доступа;
б) методы и способы сокрытия информации от внутренних нарушителей;
в) методы и способы устранения конкурентов;
г) методы и способы защиты информации от утечки по техническим каналам.

7. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

а) полуактивные;
б) пассивные;
в) разноплановые;
г) удостоверяющие;
д) активные.

8. Технический канал утечки информации – это

Ответ: совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

9. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно ____

Ответ: 16.

10. Техническими каналами утечки информации 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.

11. Несанкционированный доступ к информации – это

Ответ: **доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.**

12. Механизм контроля целостности СЗИ Secret Net предназначен для

а) формирония цифровых отпечатков данных;
б) контроля информационных потоков;
в) слежения за неизменностью содержимого ресурсов компьютера.

13. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

а) ограничения использования программного обеспечения на компьютере;
б) установки ограниченного количества программ;
в) сбора сведений об используемых приложениях.

14. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

а) «конфиденциально»;
б) «секретно»;
в) «строго конфиденциально»,
г) «неконфиденциально».

15. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного_____

Ответ: логарифма.

16. Хэш-функции предназначены, главным образом, для _____

Ответ: контроля целостности данных.

17. Длина хэш-кода алгоритма MD5 составляет _____

Ответ: 128 бит.

18. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

Ответ: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы.

3.3 Перечень теоретических вопросов к зачету

1. Основные понятия, термины и определения; предмет и объект защиты;
2. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
3. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
4. Базовые принципы организации ЗИ;
5. Защита информации в АИС от несанкционированного доступа (НСД): подсистема идентификации и аутентификации (методы и средства);
6. Модели разграничения доступа к объектам: избирательное управление; мандатное управление; замкнутая программная среда;
6. Архитектура системы защиты информации (СЗИ) от НСД SecretNet;
7. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
8. СЗИ от НСД Dallas Lock: основные функциональные возможности;
9. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
10. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;
11. Требования к симметричным и асимметричным криптосистемам;
12. Алгоритм DES; свойства стандарта AES;
13. Стандарт ГОСТ 28145-89;
14. Функции хэширования, алгоритм MD5;
15. Электронная подпись; инфраструктура открытых ключей.

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
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста

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.