

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.42 Открытые информационные системы

### рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем

Специализация/профиль – Безопасность открытых информационных систем

Квалификация выпускника – Специалист по защите информации

Форма и срок обучения – очная форма 5 лет, 6 месяцев

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 7 семестр

#### Очная форма обучения

#### Распределение часов дисциплины по семестрам

Семестр	7	Итого
Вид занятий	Часов по УП	Часов по УП
<b>Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*</b>	68	<b>68</b>
– лекции	34	<b>34</b>
– практические (семинарские)	17	<b>17</b>
– лабораторные	17	<b>17</b>
<b>Самостоятельная работа</b>	40	<b>40</b>
<b>Итого</b>	<b>108</b>	<b>108</b>

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 – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

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

<b>1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ</b>	
<b>1.1 Цель дисциплины</b>	
1	изучение технологий, методов, средств и проблем построения открытых информационных систем (ОИС)
<b>1.2 Задачи дисциплины</b>	
1	ознакомление обучаемых с понятием и принципами построения ОИС
2	ознакомление с технологиями ОИС
3	ознакомление с проблемами информационной безопасности (ИБ) в ОИС и способами их решения
<b>1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины</b>	
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	

<b>2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП</b>	
Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть
<b>2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины</b>	
1	Б1.О.36 Сети и системы передачи информации
2	Б1.О.37 Защита информации от утечки по техническим каналам
3	Б1.О.47 Информационные технологии
4	Б1.О.51 Кибербезопасность
<b>2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее</b>	
1	Б1.О.39 Программно-аппаратные средства защиты информации
2	Б1.О.41 Управление информационной безопасностью
3	Б1.О.45 Виртуальные частные сети
4	Б1.О.50 Комплексная защита в информационных системах персональных данных
5	Б1.О.59 Проектирования систем защиты объектов информатизации
6	Б1.О.62 Моделирование процессов и систем защиты информации
7	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
8	Б3.02(Д) Защита выпускной квалификационной работы

<b>3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ</b>		
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ОПК-5.1.1 Знает особенности разработки политики информационной безопасности открытых информационных систем	Знать: понятие взаимодействия ОИС
		Уметь: объяснить порядок взаимодействия ОИС
	ОПК-5.1.2 Умеет формировать исходные требования для разработки политики информационной безопасности	Владеть: представлением об особенностях взаимодействия ОИС, в том числе с точки зрения политики ИБ
		Знать: требования к безопасности ОИС
	ОПК-5.1.3 Имеет навыки обоснования целесообразности реализации политики информационной	Уметь: обосновывать требования к ИБ ОИС
		Владеть: навыками обоснования требований к ИБ ОИС
		Знать: угрозы ИБ ОИС
		Уметь: обосновывать целесообразность политик ИБ применительно к ОИС
		Владеть: представлением об угрозах ИБ применительно к ОИС

	безопасности открытых информационных систем	
ОПК-5.2 Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-5.2.1 Знает особенности проектирования систем защиты информации открытых информационных систем	Знать: модели ОИС
		Уметь: объяснить место сетевых технологий в ОИС
	ОПК-5.2.2 Умеет осуществлять внедрение систем защиты информации открытых информационных систем	Владеть: представлением о взаимосвязи сетевых технологий и технологий ОИС
		Знать: отдельные ОИС
	ОПК-5.2.3 Владеет базовыми методами проектирования, разработки, внедрения в эксплуатацию системы защиты информации открытых информационных систем	Уметь: работать с ОИС
		Владеть: навыками работы с ОИС
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.2 Знает основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития	Знать: понятие ОИС, особенности их разработки и эксплуатации
		Уметь: объяснить отдельные технологии ОИС
		Владеть: представлением о месте и возможностях ОИС в ИТ-индустрии

#### 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма				*Код индикатора достижения компетенции
		Семестр	Часы			
			Лек	Пр	Лаб	
<b>1.0</b>	<b>Раздел 1. Понятие и модели ОИС.</b>					
1.1	Тема 1. Понятие «открытая информационная система (ОИС)». Принципы ОИС. Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем. Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Стандарты ISO/IEC.	7	3	1	3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
1.2	Тема 2. Модели среды ОИС. Архитектура открытых систем. Классификация моделей. Спецификация POSIX и её развитие. Эволюция моделей открытых систем. Модель OSI/ISO. Профили на базе модели OSI/ISO. Эталонная модель OSE/RM. Цели создания модели OSE/RM. Базовая модель информационной системы (ИС). Платформы ИС. Базовая модель информационной системы, её основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы.	7	3	1	3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
1.3	Лабораторная работа № 1. Изучение архитектуры и элементов информационных систем	7			1	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1

#### 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма				*Код индикатора достижения компетенции
		Семестр	Часы			
			Лек	Пр	Лаб	
						ОПК-5.2.2 ОПК-5.2.3
1.4	Лабораторная работа № 2. Технология COM. Создание сервера автоматизации.	7			1	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
1.5	Лабораторная работа № 3. Разработка приложений для работы с базами данных в среде Delphi с использованием ADO-технологии.	7			1	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
1.6	Лабораторная работа № 4. Трехуровневые приложения.	7			2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
1.7	Лабораторная работа № 5. Web-приложения для публикации баз данных.	7			2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
<b>2.0</b>	<b>Раздел 2. Взаимодействие ОИС.</b>					
2.1	Тема 3. Переносимость ОИС. Способы реализации переносимости. Три аспекта переносимости: переносимость прикладных программ, данных и пользователей. Способы реализации переносимости.	7	3	2	3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.2	Тема 4. Взаимодействие ОИС. Способы реализации взаимодействия. Расширение базовой модели ИС для взаимодействующих систем. Взаимодействующие системы и распределённая вычислительная система. Образ единой системы в распределённой вычислительной среде. Способы реализации способности к взаимодействию. Стек протоколов. Коммуникационный интерфейс.	7	3	3	3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.3	Лабораторная работа № 6. Исследование нормативно-правовой базы информационной безопасности предприятия.	7			2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
2.4	Лабораторная работа № 7. Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для программных маршрутизаторов. Политика удаленного доступа.	7			2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1
2.5	Лабораторная работа № 8. Примеры политик безопасности. Политика подключения подразделений к интранету. Политика для конфиденциальной безопасности. Политика для веб-сервера. Политика пересылки электронной почты. Политика подключения новых устройств в интранет.	7			2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
<b>3.0</b>	<b>Раздел 3. Виды и технологии ОИС. Безопасность ОИС.</b>					

#### 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма				*Код индикатора достижения компетенции	
		Семестр	Часы				
			Лек	Пр	Лаб		СР
3.1	Тема 5. Концепция сервисов в ОИС. Сервисы платформы приложений. Стандартизация сервисов. Классификация сервисов платформы приложений. Внутренние сервисы платформы. Сервисы данных. Сервисы человеко-машинного взаимодействия. Сетевые сервисы. Межкатегориальные сервисы. Основные классы прикладных программ.	7	3	1		3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.2	Тема 6. Сервис-ориентированная архитектура ОИС. Стандарты сервис-ориентированной архитектуры. Достоинства и недостатки SOA.	7	3	1		3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.3	Тема 7. Безопасность в сервис-ориентированных архитектурах. Базовые механизмы WS Security. Токены безопасности. Шифрование. Подпись. Отметка о времени. Взаимодействие токенов, шифрования и подписей. Аутентификация. Конфиденциальность. Целостность. Уникальность сообщения.	7	3	1		3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.4	Тема 8. Распределенные вычисления. Уровни распределения обработки данных в архитектуре ОИС. Модель RM-ODP. Модели организации распределённых вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки: диспетчере-ризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок.	7	3	1		3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.5	Тема 9. Распределенное хранение данных. Архитектура распределённого хранения данных. Сети хранения данных (SAN). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN.	7	3	1		3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.6	Тема 10. Глобальная коммуникационная инфраструктура. Концепция глобальной коммуникационной инфраструктуры. Физические способы реализации инфраструктуры: проводные, оптические, радиоканалы.	7	3	1		5	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.7	Тема 11. Транспортные задачи коммуникационной инфраструктуры: эффективное кодирование, помехоустойчивость, управление линией передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay.	7	3	2		4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.8	Тема 12. Криптографические ключи в ОИС. Ключи. Жизненный цикл ключей. Стандарт ISO/IEC 11770. Модели управления ключами: централизованная и децентрализованная. Типовая структура ключевой системы.	7	1	2		4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3
3.9	Лабораторная работа № 9. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.	7			2		ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	Наименование разделов, тем и видов работ	Очная форма				*Код индикатора достижения компетенции	
		Семестр	Часы				
			Лек	Пр	Лаб		СР
3.10	Лабораторная работа № 10. Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций.	7			2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	
	Форма промежуточной аттестации – зачет	7				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	
	Итого часов (без учёта часов на промежуточную аттестацию)		34	17	17	40	

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	Артюшенко, В. В. Компьютерные сети и телекоммуникации : учебно-методическое пособие / В. В. Артюшенко, А. В. Никулин. — Новосибирск : НГТУ, 2020. — 72 с. — URL: <a href="https://e.lanbook.com/book/152244">https://e.lanbook.com/book/152244</a> (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	Череватова, Т. Ф. Нормативное обеспечение в сфере информационных технологий и систем : учебное пособие / Т. Ф. Череватова. — Санкт-Петербург : Лань, 2022. — 84 с. — URL: <a href="https://e.lanbook.com/book/233258">https://e.lanbook.com/book/233258</a> (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.42 Открытые информационные системы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» / П.Н. Наседкин ; ИрГУПС. – Иркутск : ИрГУПС, 2024. – 15 с. - Текст: электронный. - URL: <a href="https://www.irgups.ru/eis/for_site/umkd_files/mu_47634_1529_2024_1_signed.pdf">https://www.irgups.ru/eis/for_site/umkd_files/mu_47634_1529_2024_1_signed.pdf</a>	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», <a href="https://e.lanbook.com/">https://e.lanbook.com/</a>	
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 <a href="http://free-software.com.ua/pdf-viewer/foxit-reader/">http://free-software.com.ua/pdf-viewer/foxit-reader/</a>
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение <a href="https://get.adobe.com/ru/reader/enterprise/">https://get.adobe.com/ru/reader/enterprise/</a>
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
<b>6.3.2 Специализированное программное обеспечение</b>	
6.3.2.1	MathCAD student 15.0 Academic License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01
6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение <a href="https://docs.python.org/3/license.html">https://docs.python.org/3/license.html</a>
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, <a href="https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/">https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/</a>
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01.
<b>6.3.3 Информационные справочные системы</b>	
6.3.3.1	Не предусмотрены
<b>6.4 Правовые и нормативные документы</b>	
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, экран, (ноутбук переносной).
3	Учебная аудитория Д-521 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).
4	Лаборатория Д-514 «Проектирование и эксплуатация программно-информационных систем» 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.
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	<p>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.</p> <p>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,</p>

	<p>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 удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии</p>
<p>Практическое занятие</p>	<p>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.</p> <p>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</p>
<p>Лабораторная работа</p>	<p>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.</p> <p>Исходя из цели, содержанием лабораторных работ могут быть:</p> <ul style="list-style-type: none"> <li>- экспериментальная проверка формул, методик расчета;</li> <li>- проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов;</li> <li>- 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.;</li> <li>- наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения;</li> <li>- имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах;</li> <li>- наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест);</li> <li>- установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.;</li> <li>- ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.;</li> <li>- установление свойств веществ, их качественных и количественных характеристик;</li> <li>- анализ различных характеристик процессов, в том числе производственных и иных процессов;</li> <li>- расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.);</li> <li>- наблюдение развития явлений, процессов и др.</li> </ul> <p>Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций.</p> <p>По характеру выполняемых лабораторных работ возможны:</p> <ul style="list-style-type: none"> <li>- ознакомительные работы, используемые для закрепления изученного теоретического материалы;</li> <li>- аналитические работы, используемые для получения новой информации на основе формализованных методов;</li> <li>- творческие работы, ориентированные на самостоятельный выбор подходов решения задач.</li> </ul>

	<p>Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину</p>
<p>Самостоятельная работа</p>	<p>Обучение по дисциплине «Открытые информационные системы» 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 удастся, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.</p> <p>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»</p>
<p>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</p>	

# **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 «Открытые информационные системы» участвует в формировании компетенций:

ОПК-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

#### Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
<b>7 семестр</b>				
<b>1.0</b>	<b>Раздел 1. Понятие и модели ОИС</b>			
1.1	Текущий контроль	Тема 1. Понятие «открытая информационная система (ОИС)». Принципы ОИС. Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем. Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Стандарты ISO/IEC.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Модели среды ОИС. Архитектура открытых систем. Классификация моделей. Спецификация POSIX и её развитие. Эволюция моделей открытых систем. Модель OSI/ISO. Профили на базе модели OSI/ISO. Эталонная модель OSE/RM. Цели создания модели OSE/RM. Базовая модель информационной системы (ИС). Платформы ИС. Базовая модель информационной системы, её основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
1.3	Текущий контроль	Лабораторная работа № 1. Изучение архитектуры и элементов информационных систем	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)

1.4	Текущий контроль	Лабораторная работа № 2. Технология СОМ. Создание сервера автоматизации.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
1.5	Текущий контроль	Лабораторная работа № 3. Разработка приложений для работы с базами данных в среде Delphi с использованием ADO-технологии.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
1.6	Текущий контроль	Лабораторная работа № 4. Трехуровневые приложения.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
1.7	Текущий контроль	Лабораторная работа № 5. Web-приложения для публикации баз данных.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
<b>2.0</b>	<b>Раздел 2. Взаимодействие ОИС</b>			
2.1	Текущий контроль	Тема 3. Переносимость ОИС. Способы реализации переносимости. Три аспекта переносимости: переносимость прикладных программ, данных и пользователей. Способы реализации переносимости.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
2.2	Текущий контроль	Тема 4. Взаимодействие ОИС. Способы реализации взаимодействия. Расширение базовой модели ИС для взаимодействующих систем. Взаимодействующие системы и распределённая вычислительная система. Образ единой системы в распределённой вычислительной среде. Способы реализации способности к взаимодействию. Стек протоколов. Коммуникационный интерфейс.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
2.3	Текущий контроль	Лабораторная работа № 6. Исследование нормативно-правовой базы информационной безопасности предприятия.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
2.4	Текущий контроль	Лабораторная работа № 7. Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для программных маршрутизаторов. Политика удаленного доступа.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1	Лабораторная работа (письменно/устно)
2.5	Текущий контроль	Лабораторная работа № 8. Примеры политик безопасности. Политика подключения	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Лабораторная работа (письменно/устно)

		подразделений к интранету. Политика для конфиденциальной безопасности. Политика для веб-сервера. Политика пересылки электронной почты. Политика подключения новых устройств в интранет.	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	
<b>3.0</b>	<b>Раздел 3. Виды и технологии ОИС. Безопасность ОИС</b>			
3.1	Текущий контроль	Тема 5. Концепция сервисов в ОИС. Сервисы платформы приложений. Стандартизация сервисов. Классификация сервисов платформы приложений. Внутренние сервисы платформы. Сервисы данных. Сервисы человеко-машинного взаимодействия. Сетевые сервисы. Межкатегориальные сервисы. Основные классы прикладных программ.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.2	Текущий контроль	Тема 6. Сервис-ориентированная архитектура ОИС. Стандарты сервис-ориентированной архитектуры. Достоинства и недостатки СОА.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.3	Текущий контроль	Тема 7. Безопасность в сервис-ориентированных архитектурах. Базовые механизмы WS Security. Токены безопасности. Шифрование. Подпись. Отметка о времени. Взаимодействие токенов, шифрования и подписей. Аутентификация. Конфиденциальность. Целостность. Уникальность сообщения.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.4	Текущий контроль	Тема 8. Распределенные вычисления. Уровни распределения обработки данных в архитектуре ОИС. Модель RM-ODP. Модели организации распределённых вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки: диспетчеризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.5	Текущий контроль	Тема 9. Распределенное хранение данных. Архитектура распределённого хранения данных. Сети хранения данных (SAN). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)

3.6	Текущий контроль	Тема 10. Глобальная коммуникационная инфраструктура. Концепция глобальной коммуникационной инфраструктуры. Физические способы реализации инфраструктуры: проводные, оптические, радиоканалы.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.7	Текущий контроль	Тема 11. Транспортные задачи коммуникационной инфраструктуры: эффективное кодирование, помехоустойчивость, управление линиями передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.8	Текущий контроль	Тема 12. Криптографические ключи в ОИС. Ключи. Жизненный цикл ключей. Стандарт ISO/IEC 11770. Модели управления ключами: централизованная и децентрализованная. Типовая структура ключевой системы.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Собеседование (устно)
3.9	Текущий контроль	Лабораторная работа № 9. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
3.10	Текущий контроль	Лабораторная работа № 10. Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций.	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Лабораторная работа (письменно/устно)
<b>4.0</b>				
	Промежуточная аттестация	Все разделы	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	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 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 материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении	Высокий

	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

#### 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. Понятие «открытая информационная система (ОИС)». Принципы ОИС.

Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем. Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Стандарты ISO/IEC.»

- Что представляет собой понятие "открытая информационная система"?
- Какие принципы лежат в основе открытых информационных систем?
- Как вы можете классифицировать системы информационных технологий?
- Какие проблемы могут возникнуть при обеспечении совместимости в гетерогенной среде?
- Какие основные положения включает концепция открытых систем?
- Какую роль играют стандарты в технологии открытых систем?
- Как организована система стандартизации в области информационных технологий, и какие стандарты ISO/IEC применяются?

Образец типового варианта вопросов для проведения собеседования  
«Тема 2. Модели среды ОИС. Архитектура открытых систем. Классификация моделей. Спецификация POSIX и её развитие. Эволюция моделей открытых систем. Модель OSI/ISO. Профили на базе модели OSI/ISO. Эталонная модель OSE/RM. Цели создания модели OSE/RM. Базовая модель информационной системы (ИС). Платформы ИС. Базовая модель информационной системы, её основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы.»

- Каково определение моделей среды открытых информационных систем?
- Какие модели архитектуры открытых систем вы знаете?
- Что такое спецификация POSIX и как она развивалась?
- Какие профили основаны на модели OSI/ISO?
- Что представляет собой эталонная модель OSE/RM и каковы её цели?
- Каковы основные элементы базовой модели информационной системы (ИС)?
- Как эволюционировало понятие платформы в контексте информационных систем?
- Какие функциональные блоки включает платформа информационной системы, и как они взаимодействуют между собой?

Образец типового варианта вопросов для проведения собеседования  
«Тема 3. Переносимость ОИС. Способы реализации переносимости. Три аспекта переносимости: переносимость прикладных программ, данных и пользователей. Способы реализации переносимости.»

- Что подразумевается под переносимостью в открытых информационных системах?
- Какие аспекты переносимости прикладных программ, данных и пользователей необходимо учитывать?
- Какие способы реализации переносимости существуют?
- Каким образом можно обеспечить переносимость в гетерогенных средах?

Образец типового варианта вопросов для проведения собеседования  
«Тема 4. Взаимодействие ОИС. Способы реализации взаимодействия. Расширение базовой модели ИС для взаимодействующих систем. Взаимодействующие системы и распределённая вычислительная система. Образ единой системы в распределённой вычислительной среде. Способы реализации способности к взаимодействию. Стек протоколов. Коммуникационный интерфейс.»

- Как можно расширить базовую модель ИС для взаимодействующих систем?
- Что представляют собой взаимодействующие системы и распределённые вычислительные системы?
- Каким образом можно реализовать способность к взаимодействию в ОИС?
- Что включает в себя стек протоколов и коммуникационный интерфейс?

Образец типового варианта вопросов для проведения собеседования  
«Тема 5. Концепция сервисов в ОИС. Сервисы платформы приложений. Стандартизация сервисов. Классификация сервисов платформы приложений. Внутренние сервисы платформы. Сервисы данных. Сервисы человеко-машинного взаимодействия. Сетевые сервисы. Межкатегориальные сервисы. Основные классы прикладных программ.»

- Что такое сервисы в контексте открытых информационных систем?
- Какие основные классы сервисов платформы приложений существуют?

- Каким образом происходит стандартизация сервисов?
- Как можно классифицировать сервисы платформы приложений?
- Какие типы сервисов включают в себя внутренние сервисы платформы, сервисы данных, сервисы человеко-машинного взаимодействия, сетевые сервисы и межкатегориальные сервисы?

Образец типового варианта вопросов для проведения собеседования  
 «Тема 6. Сервис-ориентированная архитектура ОИС. Стандарты сервис-ориентированной архитектуры. Достоинства и недостатки SOA.»

- Что представляет собой сервис-ориентированная архитектура в открытых информационных системах?
- Какие стандарты применяются в сервис-ориентированной архитектуре?
- Какие преимущества и недостатки имеет сервис-ориентированная архитектура по сравнению с другими подходами?

Образец типового варианта вопросов для проведения собеседования  
 «Тема 7. Безопасность в сервис-ориентированных архитектурах. Базовые механизмы WS Security. Токены безопасности. Шифрование. Подпись. Отметка о времени. Взаимодействие токенов, шифрования и подписей. Аутентификация. Конфиденциальность. Целостность. Уникальность сообщения.»

- Какие базовые механизмы безопасности используются в сервис-ориентированных архитектурах?
- Что такое токены безопасности, и как они используются?
- Как осуществляется шифрование и подпись данных в контексте безопасности?
- Какие меры принимаются для обеспечения аутентификации, конфиденциальности, целостности и уникальности сообщений в сервис-ориентированных архитектурах?

Образец типового варианта вопросов для проведения собеседования  
 «Тема 8. Распределенные вычисления. Уровни распределения обработки данных в архитектуре ОИС. Модель RM-ODP. Модели организации распределённых вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки: диспетчеризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок.»

- Какие уровни распределения обработки данных существуют в архитектуре ОИС?
- Что представляет собой модель RM-ODP?
- Какие модели организации распределённых вычислений вы можете назвать?
- Какие задачи решаются при распределении обработки данных в ОИС?

Образец типового варианта вопросов для проведения собеседования  
 «Тема 9. Распределенное хранение данных. Архитектура распределённого хранения данных. Сети хранения данных (SAN). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN.»

- Как организована архитектура распределенного хранения данных?
- Что такое сети хранения данных (SAN)?
- Какие средства сетевого хранения данных существуют?
- В чем заключается виртуализация хранения данных и какие преимущества она предоставляет?

— Какие файловые системы используются в сетях хранения данных?

Образец типового варианта вопросов для проведения собеседования  
«Тема 10. Глобальная коммуникационная инфраструктура. Концепция глобальной коммуникационной инфраструктуры. Физические способы реализации инфраструктуры: проводные, оптические, радиоканалы.»

- Что означает концепция глобальной коммуникационной инфраструктуры?
- Какие физические способы реализации инфраструктуры используются?
- Какие транспортные задачи включаются в коммуникационную инфраструктуру?
- Какие архитектуры транспортного уровня можно привести в качестве примеров?

Образец типового варианта вопросов для проведения собеседования  
«Тема 11. Транспортные задачи коммуникационной инфраструктуры: эффективное кодирование, помехоустойчивость, управление линией передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay.»

- Что такое криптографические ключи в контексте открытых информационных систем?
- Как устроен жизненный цикл ключей?
- Какие стандарты регламентируют управление ключами?
- В чем различия между централизованным и децентрализованным управлением ключами?

Образец типового варианта вопросов для проведения собеседования  
«Тема 12. Криптографические ключи в ОИС. Ключи. Жизненный цикл ключей. Стандарт ISO/IEC 11770. Модели управления ключами: централизованная и децентрализованная. Типовая структура ключевой системы.»

- Что такое криптографические ключи в контексте открытых информационных систем?
- Какие функции выполняют ключи в криптографии?
- Что такое жизненный цикл ключей и почему он важен для безопасности ОИС?
- Какой стандарт регламентирует управление ключами в информационной безопасности?
- В чем состоит разница между централизованным и децентрализованным управлением ключами?
- Какие методы используются для генерации и распределения криптографических ключей?
- Каким образом криптографические ключи обеспечивают аутентификацию и конфиденциальность данных в ОИС?
- Какие проблемы могут возникнуть при управлении криптографическими ключами в распределенной среде?

### **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. Изучение архитектуры и элементов информационных систем»

Задание:

- Изучить базовые элементы информационных систем.
- Составить диаграммы, иллюстрирующие архитектурные принципы и структуру информационных систем.

Примерные вопросы для защиты:

- Какие основные элементы составляют информационные системы?
- Что такое архитектура информационных систем и каковы ее основные принципы?
- В чем заключается роль стандартов в архитектуре информационных систем?
- Какие типы информационных систем существуют? Приведите примеры.
- Какие проблемы возникают при обеспечении совместимости в гетерогенной среде?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 2. Технология COM. Создание сервера автоматизации.»

Задание:

- Изучить основные принципы технологии COM.
- Разработать сервер автоматизации, используя технологию COM.

Примерные вопросы для защиты:

- Что такое технология COM и для чего она используется?
- Какие основные концепции лежат в основе технологии COM?
- Как создать сервер автоматизации с использованием технологии COM?
- Какие преимущества и недостатки имеет технология COM по сравнению с альтернативными подходами?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 3. Разработка приложений для работы с базами данных в среде Delphi с использованием ADO-технологии.»

Задание:

- Изучить возможности ADO-технологии для работы с базами данных в среде Delphi.
- Разработать приложение для работы с базой данных, используя ADO-технологии.

Примерные вопросы для защиты:

- Что представляет собой ADO и какие возможности он предоставляет для работы с базами данных?
- Как создать подключение к базе данных с использованием ADO в среде Delphi?
- Как выполняются запросы к базе данных с помощью ADO?
- Как обрабатывать результаты запросов и работать с данными при использовании ADO?
- И так далее для каждой следующей лабораторной работы. Если нужно, я могу продолжить список для остальных лабораторных работ.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 4. Трехуровневые приложения.»

Задание:

- Изучить концепцию трехуровневых приложений.
- Разработать трехуровневое приложение с использованием выбранного языка программирования и фреймворка.
- Примерные вопросы для защиты:
- В чем заключается концепция трехуровневых приложений?
- Какие преимущества предоставляют трехуровневые архитектуры приложений?
- Какие основные компоненты включает в себя трехуровневое приложение?
- Как осуществляется взаимодействие между уровнями в трехуровневой архитектуре?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 5. Web-приложения для публикации баз данных.»

Задание:

- Изучить основные принципы разработки web-приложений.
- Создать web-приложение для публикации базы данных с использованием выбранного веб-фреймворка.

Примерные вопросы для защиты:

- Какие особенности разработки web-приложений нужно учитывать?
- Каковы основные компоненты веб-приложения и их функциональное назначение?
- Как обеспечить безопасность веб-приложения, особенно при работе с базой данных?
- Какие технологии и инструменты используются для разработки и деплоя web-приложений?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 6. Исследование нормативно-правовой базы информационной безопасности предприятия.»

Задание:

- Изучить основные нормативные документы в области информационной безопасности.
- Провести анализ и сделать выводы о соответствии информационной безопасности предприятия требованиям законодательства.

Примерные вопросы для защиты:

- Какие законодательные акты регулируют область информационной безопасности на предприятии?
- Какие требования предъявляются к обеспечению информационной безопасности в соответствии с нормативно-правовой базой?
- Какие меры безопасности должны быть реализованы на предприятии для соблюдения требований законодательства?
- Какие последствия могут быть в случае нарушения требований законодательства в области информационной безопасности?
- И так далее для каждой последующей лабораторной работы. Если нужно, я могу продолжить список для остальных лабораторных работ.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 7. Примеры политик безопасности. Политика использования ресурсов интранета. Политика в отношении паролей. Политика шифрования. Антивирусная политика. Политика оценки рисков. Политика аудита. Политика для программных маршрутизаторов. Политика удаленного доступа.»

Задание:

- Изучить основные принципы и составление политик безопасности.
- Создать несколько примеров политик безопасности для различных аспектов информационной безопасности предприятия.

Примерные вопросы для защиты:

- Что такое политика безопасности и почему она важна для предприятия?
- Какие основные составляющие включает в себя политика безопасности?
- Какие типы политик безопасности можно выделить?

— Какие методы существуют для мониторинга и обновления политик безопасности?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 8. Примеры политик безопасности. Политика подключения подразделений к интранету. Политика для конфиденциальной безопасности. Политика для веб-сервера. Политика пересылки электронной почты. Политика подключения новых устройств в интранет.»

Задание:

— Разработать дополнительные примеры политик безопасности для различных аспектов информационной безопасности предприятия.

Примерные вопросы для защиты:

- Какие конкретные ситуации на предприятии могут потребовать разработки специфических политик безопасности?
- Какие меры предосторожности следует предусмотреть в различных областях, например, в отношении персональных данных или финансовых операций?
- Каков процесс разработки и внедрения новых политик безопасности на предприятии?
- Какие основные принципы эффективной политики безопасности можно выделить?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 9. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов.»

Задание:

— Изучить основные типы межсетевых экранов и схемы их подключения.

— Разработать несколько схем подключения межсетевых экранов для предприятия с учетом его специфики и потребностей.

Примерные вопросы для защиты:

- Что такое межсетевой экран и для чего он используется в информационной безопасности?
- Какие типы межсетевых экранов существуют, и в чем их отличия?
- Какие основные принципы работы межсетевых экранов?
- Какие сценарии использования межсетевых экранов могут быть на предприятии?

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты «Лабораторная работа № 10. Исследование поточных и блочных алгоритмов шифрования. Использование хэш-функций.»

Задание:

— Изучить принципы работы и особенности поточных и блочных алгоритмов шифрования, а также хэш-функций.

— Провести анализ различных алгоритмов и выбрать наиболее подходящие для конкретных задач информационной безопасности.

Примерные вопросы для защиты:

- В чем заключается основное различие между поточными и блочными алгоритмами шифрования?
- Какие алгоритмы шифрования являются самыми распространенными в современных системах?
- Какие методы атаки могут быть использованы против различных алгоритмов шифрования?
- Какие хэш-функции являются наиболее безопасными для использования в системах информационной безопасности, и почему?

### 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-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 1. Понятие «открытая информационная система (ОИС)». Принципы ОИС. Классификация систем ИТ. Основные понятия и определения. Проблемы обеспечения совместимости в гетерогенной среде. Основные положения концепции открытых систем. Среда открытых систем. Роль стандартов в технологии открытых систем. Организационная структура системы стандартизации ИТ. Стандарты ISO/IEC.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 2. Модели среды ОИС. Архитектура открытых систем. Классификация моделей. Спецификация POSIX и её развитие. Эволюция моделей открытых систем. Модель OSI/ISO. Профили на базе модели OSI/ISO. Эталонная модель OSE/RM. Цели создания модели OSE/RM. Базовая модель информационной системы (ИС). Платформы ИС. Базовая модель информационной системы, её основные элементы. Эволюция понятия платформы. Функциональные блоки платформы и способы их взаимодействия: интерфейсы и протоколы.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 3. Переносимость ОИС. Способы реализации переносимости. Три аспекта переносимости: переносимость прикладных программ, данных и пользователей. Способы реализации переносимости.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 4. Взаимодействие ОИС. Способы реализации взаимодействия. Расширение базовой модели ИС для взаимодействующих систем. Взаимодействующие системы и распределённая вычислительная система. Образ единой системы в распределённой вычислительной среде. Способы реализации способности к взаимодействию. Стек протоколов. Коммуникационный интерфейс.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 5. Концепция сервисов в ОИС. Сервисы платформы приложений. Стандартизация сервисов. Классификация сервисов платформы приложений. Внутренние сервисы платформы. Сервисы данных. Сервисы человеко-машинного взаимодействия. Сетевые сервисы. Межкатегориальные сервисы. Основные классы прикладных программ.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 6. Сервис-ориентированная архитектура ОИС. Стандарты сервис-ориентированной архитектуры. Достоинства и недостатки СОА.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 7. Безопасность в сервис-ориентированных архитектурах. Базовые механизмы WS Security. Токены безопасности. Шифрование. Подпись. Отметка о времени. Взаимодействие токенов, шифрования и подписей. Аутентификация. Конфиденциальность. Целостность. Уникальность сообщения.	Знание	1 – ОТЗ 2 – ЗТЗ
		Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2	Тема 8. Распределенные вычисления. Уровни распределения обработки данных в архитектуре ОИС. Модель RM-ODP.	Знание	1 – ОТЗ 2 – ЗТЗ

ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Модели организации распределённых вычислений: клиент-серверная, хостовая, «ведущий-ведомый», иерархическая, одноранговая, объектная. Сильная и слабая связность процессоров: многопроцессорные ВК, кластеры, сетевые вычисления, концепция GRID. Задачи распределения обработки: диспетчеризация, синхронизация, маршрутизация, балансировка, управление ресурсами, обработка ошибок.	Умение	2 – ОТЗ 1 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 9. Распределенное хранение данных. Архитектура распределённого хранения данных. Сети хранения данных (SAN). Средства сетевого хранения. Виртуализация хранения. Файловые системы SAN.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 10. Глобальная коммуникационная инфраструктура. Концепция глобальной коммуникационной инфраструктуры. Физические способы реализации инфраструктуры: проводные, оптические, радиоканалы.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 11. Транспортные задачи коммуникационной инфраструктуры: эффективное кодирование, помехоустойчивость, управление линией передачи данных, управление каналами, задержки в сетях передачи данных, множественный доступ к несущей, маршрутизация, управление потоками. Примеры архитектур транспортного уровня: локальные сети, FDDI, SLIP, ISDN, SONET/SDH, X.25, ATM, FrameRelay.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 0 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3 ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3	Тема 12. Криптографические ключи в ОИС. Ключи. Жизненный цикл ключей. Стандарт ISO/IEC 11770. Модели управления ключами: централизованная и децентрализованная. Типовая структура ключевой системы.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
		Действие	0 – ОТЗ 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)

Угрозы информационной безопасности (основные определения и критерии классификации угроз). Средства защиты.

2. Сценарии реализации угроз информационной безопасности (разглашение конфиденциальной информации и обход средств защиты от разглашения конфиденциальной информации; кража конфиденциальной информации; нарушение авторских прав на информацию; нецелевое использование ресурсов).

3. Вредоносная программа. Классификация вредоносных программ (вирусы; черви; троянские программы; спам; другие вредоносные программы). Способы распространения вредоносных программ.

4. Основы борьбы с вредоносными программами. Диагностика заражения вредоносными программами. Антивирусное программное обеспечение. Комплексные средства антивирусной защиты.

5. Уязвимости ОИС. Причины уязвимости ИС. Классификация уязвимостей.

6. Уязвимости архитектуры клиент-сервер (конфигурация системы, уязвимость операционных систем, уязвимость серверов, уязвимость рабочих станций, уязвимость каналов связи).
7. Уязвимость системных утилит, команд и сетевых сервисов. Уязвимость современных технологий программирования. Ошибки в программном обеспечении.
8. Модель угроз ИБ. Модель нарушителей ИБ. Инсайдеры и аутсайдеры.
9. Атаки на открытые системы. Удаленные атаки на открытые системы. Классификация удаленных атак.
10. Анализ сетевого трафика. Подмена доверенного объекта или субъекта системы. Внедрение ложного объекта в систему.
11. Типичные сценарии и уровни атак. Удаленный контроль над станцией в сети.
12. Классические методы взлома (взлом парольной защиты). Современные методы взлома: перехват данных при их перемещении по каналам связи и перехват ввода с клавиатуры; мониторинг в графических интерфейсах; подмена системных утилит; нападения с использованием сетевых протоколов.
13. Обеспечение информационной безопасности в открытых системах. Комплексный и фрагментарный подходы к защите ИС. Четырехуровневая модель открытой системы.
14. Эшелонированная защита ОИС в целом и отдельных ее элементов. топология сети: физическая изоляция; изоляция протокола; выделенные каналы.
15. Организационно-правовые методы защиты открытых систем.
16. Политика информационной безопасности. Разновидности политик ИБ. Основные положения политики ИБ.
17. Информационная безопасность в глобальных сетях. Удаленные атаки и механизмы их реализации в глобальных сетях.
18. Криптографическая защита информации. Понятия о симметричных криптосистемах (шифры перестановки; шифры сложной замены; одноразовая система шифрования; шифрование методом гаммирования; DES).
19. Криптографическая защита информации. Понятия об асимметричных криптосистемах (однонаправленные функции; криптосистема шифрования данных RSA; электронная цифровая подпись).
20. Криптографическая защита информации. Аппаратно-программные криптографические средства защиты информации.
21. Межсетевые экраны (firewall): прикладного уровня; с пакетной фильтрацией; гибридные межсетевые экраны.
22. Организация и эксплуатация виртуальных частных сетей (VPN).
23. Иерархическая модель доверия. Сетевая модель доверия.
24. Управление ключами и сертификация ключей.
25. Протокол конфиденциального обмена данными SSL. Протокол WEP. Протокол 802.1X - контроль доступа в сеть по портам.
26. Стандарты и спецификации в области информационной безопасности.

### **3.5 Перечень типовых простых практических заданий к зачету**

(для оценки умений)

- 1 Диагностика заражения вредоносными программами.
- 2 Анализ сетевого трафика.
- 3 Удаленный контроль над станцией в сети.
- 4 Настройка политик информационной безопасности.
- 5 Настройка меж сетевого экрана.
- 6 Организация и настройка виртуальной частной сети.

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

(для оценки навыков и (или) опыта деятельности)

- 1 Диагностика заражения вредоносными программами.
- 2 Анализ сетевого трафика.

- 3 Удаленный контроль над станцией в сети.
4. Настройка политик информационной безопасности.
5. Настройка межсетевого экрана.
6. Организация и настройка виртуальной частной сети.

#### **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.