ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем

рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность
Профиль – "Безопасность автоматизированных систем"
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

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

Формы промежуточной аттестации в семестрах:
зачет (8)

Распределение часов дисциплины по семестрам

Семестр	8	**Итого**
Число недель в семестре	12	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**48**	**48**
– лекции	12	12
– практические (семинарские)	12	12
- лабораторные	24	24
Самостоятельная работа	**60**	**60**
Итого	**108**	**108**

ИРКУТСК

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели освоения дисциплины

1	изучение основ проектирования комплексной системы информационной безопасности (КСИБ), соотношения программных, аппаратных и организационных средств и методов в комплексной деятельности по защите информации (ЗИ) в автоматизированных системах (АС).

1.2 Задачи освоения дисциплины

1	освоение способов выделения информации в АС, подлежащей защите;
2	изучение критериев защищённости АС, методологии построения современных КСИБ, технологий проектирования систем защиты информации;
3	формирование комплексного подхода к обеспечению информационной безопасности АС.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.

Цель достигается по мере решения в единстве следующих задач:
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;
– популяризация научных знаний среди обучающихся;
– содействие повышению привлекательности науки, поддержка научно-технического творчества;
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.

Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологи профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

1	Б1.Б.11 Основы информационной безопасности
2	Б1.Б.16 Техническая защита информации
3	Б1.Б.25 Информационные технологии
4	Б1.В.04 Безопасность операционных систем
6	Б1.В.07 Аудит информационной безопасности
7	Б1.Б.13 Программно-аппаратные средства защиты информации
8	Б1.В.ДВ.08.01 Методология анализа информационных рисков

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

1	Б2.В.04(Пд) Производственная практика - преддипломная

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕС ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Минимальный уровень освоения компетенции	
Знать	методики формирования ПИБ верхнего уровня (цели, концепции, доктрины);
Уметь	разрабатывать ПИБ верхнего уровня (цели, концепции, доктрины);
Владеть	навыками разработки общих положений ПИБ;
Базовый уровень освоения компетенции	
Знать	методики формирования ПИБ среднего уровня (стандарты);
Уметь	формировать ПИБ среднего уровня (стандарты);
Владеть	навыками разработки положений ПИБ среднего уровня детализации;
Высокий уровень освоения компетенции	
Знать	способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции).
Уметь	разрабатывать ПИБ нижнего уровня (методики, процедуры, инструкции);
Владеть	навыками разработки детализированных положений ПИБ.
ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
Минимальный уровень освоения компетенции	
Знать	минимальный набор стандартов информационной безопасности (ИБ);
Уметь	применять минимальный набор стандартов для оценки защищенности объектов и систем;
Владеть	методиками анализа ИБ;
Базовый уровень освоения компетенции	
Знать	основные нормативно-правовые документы ФСТЭК в области ИБ;
Уметь	применять основные нормативно-правовые документы ФСТЭК в области ИБ для анализа уровня защищенности объекта;
Владеть	навыками аудита защищенности объектов информатизации;
Высокий уровень освоения компетенции	
Знать	базовые положения нормативно-правовых документов ФСТЭК и зарубежных стандартов;
Уметь	применять основные нормативно-правовые документы ФСТЭК в области информационной безопасности;
Владеть	навыками применения базового набора нормативно-правовых документов ФСТЭК и зарубежных стандартов в области ЗИ.

В результате освоения дисциплины обучающийся должен

Знать	
1	методики оценки рисков информационной безопасности;
2	типовую структуру КСИБ;
3	требования к компонентам КСИБ;
4	этапы построения КСИБ;
Уметь	
1	применять действующую нормативно-законодательную базу ФСТЭК в области ИБ;
2	проводить аудит информационной безопасности АС;
Владеть	
1	навыками разработки ПИБ АС.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. Постановка задачи комплексного обеспечения ИБ АС				
1.1	Состав компонентов комплексной системы обеспечения информационной безопасности. Функциональные и обеспечивающие подсистемы, технология, управление /Лек/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
1.2	Законодательная, нормативно-методическая и научная базы разработки КСИБ /Пр/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э1 Э2

1.3	Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС) /Пр/	8	4	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
1.4	Инвентаризация АС в соответствии с РД ГТК на базе учебных лабораторий Д508, Д514, Д523, Д525, (инфраструктура, технические, программные и информационные ресурсы (ИР)) /Лаб/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
1.5	Законодательная, нормативно-методическая и научная базы разработки КСИБ /Ср/	8	10	ПК-4, ПК-10	Л4.1 Э1 Э2
	Раздел 2. Методология формирования задач защиты; интеграция средств защиты в технологическую среду				
2.1	Параллельная разработка АС и КСИБ. Системный подход к построению КСИБ. Архитектура защищенных АС /Лек/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
2.2	Соотношение программных, аппаратных и административных средств в комплексном обеспечении информационной безопасности АС /Пр/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
2.3	Разработка и содержание аварийного плана действий в случае нарушения ИБ АС /Пр/	8	4	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
2.4	Анализ уязвимостей АС на примере учебных лабораторий Д508, Д514, Д523, Д525 /Пр/	8	4	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
2.5	Анализ угроз ИР и обеспечивающей инфраструктуре на базе учебных лабораторий Д508, Д514, Д523, Д525. Построение моделей угроз и нарушителя /Лаб/	8	4	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
2.6	Проработка лекционного материала, подготовка к практическим и лабораторным занятиям /Ср/	8	10	ПК-4, ПК-10	Л4.1
	Раздел 3. Типовая структура КСИБ; методы проектирования и оценки качества КСИБ				
3.1	Организация доступа к ресурсам АС. Система разграничения доступа к техническим средствам. Система разграничения доступа к программам и данным. Средства блокировки неправомочных действий субъектов /Лек/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
3.2	Задача интеграции средств защиты информации в технологическую среду АС /Пр/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
3.3	Требования к составу проектной и эксплуатационной документации. Порядок подготовки и проведения аттестации АС. Сертификация программного обеспечения (ПО) /Пр/	8	2	ПК-4, ПК-10	Л1.5 Э1 Э2
3.4	Оценка рисков ИБ АС на базе учебных лабораторий Д508, Д514, Д523, Д525 /Лаб/	8	2	ПК-4, ПК-10	Л3.1
3.5	Проработка лекционного материала, подготовка к практическим и лабораторным занятиям /Ср/	8	11	ПК-4, ПК-10	Л4.1
	Раздел 4. Этапы проектирования КСИБ и требования к ним			ПК-4, ПК-10	
4.1	Предпроектное обследование: инвентаризация ресурсов. Предпроектное обследование: модели угроз и нарушителя. Предпроектное обследование: анализ рисков.Техническое задание. Техническое и	8	4	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8

	рабочее проектирование. Испытания и внедрение в эксплуатацию, сопровождение. Оценка эффективности. Особенности проектирования на современном уровне и синтез КСИБ /Лек/				
4.2	Автоматизация процесса анализа и управления рисками (с помощью пакета Digital Security Гриф). Моделирование процедуры /Пр/	8	2	ПК-4, ПК-10	Л3.1
4.3	Разработка контрмер. Экономическая оценка затрат на защиту информации (на базе учебных лабораторий Д508, Д514, Д523, Д525) /Лаб/	8	4	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
4.4	Проработка лекционного материала, подготовка к практическим и лабораторным занятиям /Ср/	8	11	ПК-4, ПК-10	Л4.1
	Раздел 5. Структура политики информационной безопасности организации				
5.1	Методики формирования ПИБ верхнего уровня (цели, концепции, доктрины); Методики формирования ПИБ среднего уровня (стандарты); Способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции) /Лек/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
5.2	Типовой перечень задач службы информационной безопасности.. Организационно-технические и режимные меры /Пр/	8	2	ПК-4, ПК-10	Л1.1-Л1.7 Л2.1-Л2.3 Э3-Э8
5.3	Проработка лекционного материала, подготовка к практическим занятиям; подготовка к зачету /Ср/	8	18	ПК-4, ПК-10	Л4.1

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

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л1.1	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам; http://e.lanbook.com/books/element.php?pl1_id=5114: для ВПО	Горячая линия-Телеком, 2012	100 % онлайн
Л1.2	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие http://e.lanbook.com/books/element.php?pl1_id=63235	Горячая линия-Телеком, 2013	100% онлайн

Л1.3	Никитин И. А. , Цулая М. Т.	Процессы анализа и управления рисками в области ИТ: Учебная литература для ВУЗов; http://biblioclub.ru/index.php?page=book_red&id=429089:	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100% онлайн
Л1.4	Ададуров С.Е., Глухов А.П., Корниенко А.А., Диасамидзе С.В., Корниенко А.А.	Информационная безопасность и защита информации на железнодорожном транспорте: Учебное пособие для ВО	М.: УМЦ по образованию на ж.-д. трансп., 2014	30
Л1.5	Коваленко Ю.И.	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Для ВПО и курсов переподготовки http://e.lanbook.com/books/element.php?pl1_id=5163	М.: Горячая линия-Телеком, 2012	100% онлайн
Л1.6	Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5178	М.: Горячая линия-Телеком, 2012	100% онлайн
Л1.7	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Управление рисками информационной безопасности. Серия «Вопросы управление информационной безопасностью". Выпуск 2: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5179	М.: Горячая линия-Телеком, 2012	100% онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л2.1	Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.	Основы информационной безопасности: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5121	М:. Горячая линия-Телеком, 2006	100% онлайн
Л2.2	Яковлев В.В., Корниенко А.А.	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учеб. для вузов ж.-д. трансп.	М.: УМК МПС России, 2002	153
Л2.3	Шелупанов А.А. и др.	Основы защиты информации : Учебное пособие в трех частях	Томск: В-Спектр, 2010	25
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия, учебное пособие.	Иркутск: Ир-ГУПС, 2013.	67
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л4.1	Завгородний В.И.	«Комплексная защита информации в компьютерных системах» http://www.proklondike.com/books/defence/zavgorodniy_complex_defence.html; http://bezopasnik.org/article/book/zavgorodniy_-_Complex_Defend.pdf	Личный кабинет	100% онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э1	Сайт ФСТЭК РФ		http://fstec.ru/	
Э2	Сайт ФСБ РФ		http://www.fsb.ru/	

Э3	Материалы "Единые критерии"	http://oplib.ru/random/view/273781
Э4	РД ГТК	http://www.studmed.ru/docs/document16873?view=50&page=5
Э5	РД ГТК	http://oplib.ru/random/view/441942
Э6	Материалы "Парольные системы"	http://infoprotect.net/category/note
Э7	Материалы "Сканеры безопасности, сетевые угрозы"	http://www.securitylab.ru/analytics/365241.php
Э8	Материалы "Комплексная защита информации в компьютерных системах"	http://mexalib.com/view/2248

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень базового программного обеспечения

6.3.1.1	ОС Microsoft Windows XP Professional with Service Pack 2, лицензия Open License, Количество - 427
6.3.1.2	ОС Microsoft Windows 7;
6.3.1.3	Офисный пакет Microsoft Office 2010, OpenLicense, Количество - 155

6.3.2 Перечень специализированных средств и программного обеспечения

6.3.2.1	Пакет Digital Security Кондор/Гриф (свободное ПО)

6.3.3 Перечень информационных справочных систем

6.3.3.1	Информационно-справочная система КонсультантПлюсhttp://www.consultant.ru

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

1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории.
2	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.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторной работе.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов с преподавателем, вызвавших затруднение, Участие в дискуссиях. Контроль качества усвоения пройденного материала.
Лабораторная работа	Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.

Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Приложение 1 к рабочей программе по дисциплине
Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.В.01 «Комплексное обеспечение информационной безопасности автоматизированных систем»

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

Дисциплина «**Комплексное обеспечение информационной безопасности автоматизированных систем**» участвует в формировании компетенций:

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ;
ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

Таблица траекторий формирования у обучающихся компетенций ПК-4, ПК-10 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б2.В.03(П) Производственная практика - эксплуатационная	6	2
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	3
		Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем	8	3
		Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Б1.В.02 Теоретические основы компьютерной безопасности	3	1
		Б1.В.07 Аудит информационной безопасности	6	2
		Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем	8	3
		Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3

Таблица соответствия уровней освоения компетенций ПК-4, ПК-10

планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Раздел 1. Постановка задачи компле-ксного обеспе-чения ИБ АС. Раздел 2. Методология формирования задач защиты; интеграция средств защиты в технологическую среду. Раздел 3. Типовая структура комплексной системы информационной безопаности (КСИБ); методы проектирования и оценки качества КСИБ. Раздел 4. Этапы проектирования КСИБ и требования к ним. Раздел 5. Структура поли-тики информа-ционной безо-пасности органи-зации	Минимальный уровень	Знать: методики формирования ПИБ верхнего уровня (цели, концепции, доктрины);
				Уметь: разрабатывать ПИБ верхнего уровня (цели, концепции, доктрины);
				Владеть: навыками разработки общих положений ПИБ;
			Базовый уровень	Знать: методики формирования ПИБ среднего уровня (стандарты);
				Уметь: формировать ПИБ среднего уровня (стандарты);
				Владеть: навыками разработки положений ПИБ среднего уровня детализации;
			Высокий уровень	Знать: способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции).
				Уметь: разрабатывать ПИБ нижнего уровня (методики, процедуры, инструкции);
				Владеть: навыками разработки детализированных положений ПИБ.
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Раздел 1. Постановка задачи компле-ксного обеспе-чения ИБ АС. Раздел 2. Методология формирования задач защиты; интеграция средств защиты в технологическую среду. Раздел 3. Типовая структура комплексной системы информационной безопаности (КСИБ); методы проектирования и оценки качества КСИБ. Раздел 4. Этапы проектирования КСИБ и требования к ним. Раздел 5. Структура поли-тики	Минимальный уровень	Знать: минимальный набор стандартов информационной безопасности (ИБ);
				Уметь: применять минимальный набор стандартов для оценки защищенности объектов и систем;
				Владеть: методиками анализа ИБ;
			Базовый уровень	Знать: основные нормативно-правовые документы ФСТЭК в области ИБ;
				Уметь: применять основные нормативно-правовые документы ФСТЭК в области ИБ для анализа уровня защищенности объекта;
				Владеть: навыками аудита защищенности объектов информатизации;
			Высокий уровень	Знать: базовые положения нормативно-правовых документов ФСТЭК и зарубежных стандартов;
				Уметь: применять основные нормативно-правовые документы ФСТЭК в области информационной безопасности;
				Владеть: навыками применения базового набора нормативно-правовых документов ФСТЭК и за-

		информа-ционной безо-пасности органи-зации		рубежных стандартов в области ЗИ.

Программа контрольно-оценочных мероприятий
за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
8 семестр					
1	1	Текущий контроль	Инвентаризация АС в соответствии с РД ГТК на базе учебных лабораторий Д508, Д514, Д523, Д525 (инфраструктура, технические, программные и информационные ресурсы (ИР)) /Лаб/	ПК-4 ПК-10	Защита лабораторной работы;
2	5	Текущий контроль	Анализ угроз ИР и обеспечивающей инфраструктуре на базе учебных лабораторий Д508, Д514, Д523, Д525. Построение моделей угроз и нарушителя /Лаб/	ПК-4 ПК-10	Защита лабораторной работы
3	7	Текущий контроль	Оценка рисков ИБ АС на базе учебных лабораторий Д508, Д514, Д523, Д525 /Лаб/	ПК-4 ПК-10	Защита лабораторной работы
4	11	Текущий контроль	Разработка контрмер. Экономическая оценка затрат на защиту информации (на базе учебных лабораторий Д508, Д514, Д523, Д525) /Лаб/	ПК-4 ПК-10	Защита лабораторной работы
5	12	Тест	Разделы1-5 РПД	ПК-4 ПК-10	Перечень тестовых заданий
6	12	Промежуточная аттестация – зачет	Разделы 1- 5 РПД	ПК-4 ПК-10	Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно

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

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

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

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

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

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно 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	Темы лабораторных работ и требования к их защите
2	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
3	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	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 (билетов) к зачету

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

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный

«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

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

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	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»	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

Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание
Минимальный уровень освоения компетенции	19	Тестовые задания с выбором одного правильного ответа из нескольких	1
		Тестовые задания с выбором нескольких правильных ответов из множества ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	4
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	7

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-52 баллов	Компетенция не сформирована

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

3.1 Перечень типовых тем докладов, сообщений

1. Законодательная, нормативно-методическая и научная базы разработки КСИБ;

2. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС);
3. Соотношение программных, аппаратных и административных средств в комплексном обеспечении информационной безопасности АС;
4. Разработка и содержание аварийного плана действий в случае нарушения ИБ АС;
5. Анализ уязвимостей АС на примере учебных лабораторий Д508, Д514, Д523, Д525;
6. Задача интеграции средств защиты информации в технологическую среду АС.
7. Требования к составу проектной и эксплуатационной документации. Порядок подготовки и проведения аттестации АС. Сертификация программного обеспечения (ПО);
8. Автоматизация процесса анализа и управления рисками (с помощью пакета Digital Security Гриф). Моделирование процедуры;
9. Типовой перечень задач службы информационной безопасности.. Организационно-технические и режимные меры.

3.2 Тест

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. Выберите правильное определение термина «предоставление информации»:
   а) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
   б) действия, направленные на распространение сведений в средствах массовой информации;
   в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
   г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённому кругу лиц.
4. Выберите правильное определение термина «защищаемые помещения»:
   а) помещения, специально предназначенные для хранения носителей конфиденциальной информации;
   б) помещения, специально предназначенные для размещения технических средств информационной системы;
   в) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы;
   г) 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. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;

б) детали интерьера, используемые для размещения АС;

в) средства контроля эффективности применения средств защиты информации;

г) средства контроля эффективности прочности ограждений;

д) средства защиты информации (технические, программные, программно-аппаратные) от НСД, блокировки доступа и нарушения целостности.

8. 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.

9. “Технический канал утечки информации” - это:

а) совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б) совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств;

в) совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

г) совокупность объекта технической разведки и средств, которыми добывается защищаемая информация.

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:

а) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

б) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;

в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;

г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

12. Политика информационной безопасности (ПИБ) – это

а) общий документ, где перечисляются правила доступа в хранилище информации;

б) набор документов, регламентирующих порядок хранения, обработки и передачи информации.

13. Определите последовательность следующих процедур (1-2-3):

авторизация субъекта (3);

аутентификация субъекта (2);

идентификация субъекта (1).

14. «Сборка мусора» - это

а) поиск удаленной информации на носителях;

б) вскрытие шифров криптозащиты информации;

б) внедрение программных/аппаратных закладок.

15. Аварийный план предназначен для

а) сокрытия информации от нарушителя;

б) регламентации действий при нарушении ИБ АС;

16. «Анализ информационных рисков» - это

а) выявление уязвимостей АС;

б) выявление угроз;

в) оценка критичности угроз.

17. «Угроза информационной безопасности (ИБ)» - это

а) некоторая уязвимость АС;

б) потенциально возможное событие/действие, которое может нанести ущерб информации.

18. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;

б) детали интерьера, используемые для размещения АИС;

в) средства контроля эффективности применения средств защиты информации;

г) средства контроля эффективности прочности ограждений;

д)средства защиты информации (технические, программные, программно-аппаратные) от НСД, блокировки доступа и нарушения целостности.

19. 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.

20. Вставить одно слово на место пропущенных:

«Идентификация» (Identification) – это присвоение субъектам и объектам доступа _____ (идентификатора) и/или сравнение предъявляемого

_____ (идентификатора) с перечнем присвоенных _____ (идентификаторов).
21. Угроза ИБ всегда направлена на определенную _____ (уязвимость)АС.
22. _____ (Подстановки) могут быть полиалфавитными и моноалфавитными.
23. Средство, осуществляющее перехват всех обращений субъектов к объектам и разграничивающее доступ в соответствии с заданным принципом разграничения доступа, называется _____ (диспетчером) доступа.
24. Выделяют 4 классических вида угроз безопасности информации: угрозы конфиденциальности, целостности, доступности и _____ (раскрытия) параметров АС.
25. Защита информации — комплекс мероприятий _____ (технического), организационного и _____ (организационно-технического) характера.
26. К предпроектному обследованию АС относится; в частности,_____ (инвентаризация) ресурсов.
27. К предпроектному обследованию АС относится; в частности, построение _____ (модели) угроз и нарушителя.
28. В чем заключается анализ рисков?
29. В чем суть разработки технического задания?
30. В чем суть разработки технического проекта?
31. Какова структура ПИБ верхнего уровня?
32. Какова структура ПИБ среднего уровня?
33. Какова структура ПИБ нижнегоуровня?

3.2 Перечень теоретических вопросов к зачету

1. Состав компонентов комплексной системы обеспечения информационной безопасности.
2. Функциональные и обеспечивающие подсистемы, технология, управление.
3. Параллельная разработка АС и КСИБ.
4. Системный подход к построению КСИБ.
5. Архитектура защищенных АС.
6. Организация доступа к ресурсам АС.
7. Система разграничения доступа к техническим средствам.
8. Система разграничения доступа к программам и данным.
9. Средства блокировки неправомочных действий субъектов.
10. Предпроектное обследование: инвентаризация ресурсов.
11. Предпроектное обследование: модели угроз и нарушителя.
12. Предпроектное обследование: анализ рисков.
13. Техническое задание. Техническое и рабочее проектирование.
14. Испытания и внедрение в эксплуатацию, сопровождение. Оценка эффективности.
15. Особенности проектирования на современном уровне и синтез КСИБ.
16. Методики формирования ПИБ верхнего уровня (цели, концепции, доктрины).
17. Методики формирования ПИБ среднего уровня (стандарты);
18. Способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции).

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

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

– перечень теоретических вопросов к зачету для оценки знаний;

– перечень типовых простых практических заданий к зачету для оценки умений;

– перечень типовых практических заданий к зачету для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету 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. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. 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	Оценка
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 в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.

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