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.06 Комплексная защита в информационных системах персональных данных

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма обучения – очная
Нормативный срок обучения – 5 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану – 180

Формы промежуточной аттестации в семестрах:
экзамен 9 курсовой проект 9

Распределение часов дисциплины по семестрам

Семестр	9	**Итого**
Число недель в семестре	15	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**72**	**72**
– лекции	36	36
– практические (семинарские)	18	36
– лабораторные	18	18
Самостоятельная работа	**72**	**72**
Экзамен	**36**	**36**
Итого	**180**	**180**

ИРКУТСК

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	раскрытие сущности и значения комплексного обеспечения безопасности персональных данных, обеспечение студентов теоретическими знаниями и практическими навыками, необходимыми для проведения работ по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями российского законодательства.
1.2 Задачи освоения дисциплины	
1	изучение организационно-правовых и технических вопросов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
2	проведение классификации информационных систем обработки персональных данных;
3	изучение методов и процедур выявления угроз безопасности информации, построение модели угроз;
4	создание подсистемы информационной безопасности при организации обработки персональных данных.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	
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	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.Б.1.06 Основы управленческой деятельности
2	Б1.Б.1.25 Техническая защита информации
3	Б1.Б.1.27 Организационное и правовое обеспечение информационной безопасности
4	Б1.В.06 Методология анализа информационных рисков
5	Б2.Б.02(П) Производственная - по получению профессиональных умений и опыта профессиональной деятельности
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.Б.05(П) Производственная - технологическая
2	Б2.Б.06(Пд) Производственная - преддипломная
3	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и

	процедуру защиты

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ПК-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	Математическое моделирование информационных рисков
Уметь	Моделировать информационные риски
Владеть	Программами математического моделирования
Базовый уровень освоения компетенции	
Знать	Базовые модели угроз и нарушителей ИБ
Уметь	Строить частные модели угроз на основе базовых
Владеть	Руководящими документами ФСТЭК по построению частных моделей
Высокий уровень освоения компетенции	
Знать	Методики построения модели угроз и модели нарушителя информационной безопасности автоматизированной системы
Уметь	Применять руководящие документы ФСТЭК
Владеть	Навыками разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК-22: способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Минимальный уровень освоения компетенции	
Знать	Терминологию, основные руководящие и регламентирующие документы в области информационной безопасности
Уметь	Проводить анализ угроз безопасности информационных систем
Владеть	Профессиональной терминологией в области ИБ
Базовый уровень освоения компетенции	
Знать	Основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ
Уметь	Реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ
Владеть	Навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации
Высокий уровень освоения компетенции	
Знать	Нормативно-методические и правовые документы в области информационной безопасности
Уметь	Разрабатывать проекты локальных нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии
Владеть	Навыками работы и способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Минимальный уровень освоения компетенции	
Знать	Основные принципы, методы и процедуры организации работы с информацией ограниченного доступа
Уметь	Реализовывать основные принципы, методы и процедуры организации работы с информацией ограниченного доступа
Владеть	Терминологией по применению основные принципы, методы и процедуры организации работы с информацией ограниченного доступа
Базовый уровень освоения компетенции	
Знать	Методологию применения нормативно-методических документов по организации работы для защиты информации ограниченного доступа
Уметь	Применять нормативно-методических документов по организации работы для защиты информации ограниченного доступа
Владеть	Навыками работы с нормативно-методическими документами по организации работы для защиты информации ограниченного доступа
Высокий уровень освоения компетенции	
Знать	Основные руководящие документы, приказы ФСТЭК и ФСБ по формированию комплекса мер

	(правил, процедур, методов) для защиты информации ограниченного доступа
Уметь	Применять основные руководящие документы, приказы ФСТЭК и ФСБ по формированию комплекса мер (правил, процедур, методов) для защиты информации ограниченного доступа
Владеть	Навыками по применению основных руководящих документов, приказов ФСТЭК и ФСБ по формированию комплекса мер (правил, процедур, методов) для защиты информации ограниченного доступа

В результате освоения дисциплины обучающийся должен

Знать	
1	Действующее российское и международное законодательство по вопросам обеспечения информационной безопасности и защите персональных данных
2	Требования государственных регулирующих органов по технической защите персональных данных, в том числе о лицензировании деятельности по технической защите конфиденциальной информации, сертификации средств защиты информации и аттестации объектов информатизации
3	Структуру комплексной системы защиты персональных данных
4	Методы и средства защиты персональных данных, обрабатываемых в информационных системах
5	Действия операторов персональных данных в рамках трудовых и гражданско-правовых отношений, связанных с передачей и представлением персональных данных третьим лицам
6	Меры ответственности за нарушение установленных требований по защите персональных данных
Уметь	
1	Анализировать состав защищаемых персональных данных
2	Проводить классификацию информационных систем обработки персональных данных
3	Использовать методы оценки уязвимости защищаемых персональных данных, построения модели угроз
3	Применять методы и способы защиты информации в информационных системах персональных данных
4	Оформлять нормативную документацию с учетом применения технологии защищенного документооборота при обработке персональных данных с использованием средств автоматизации и без использования таковых
Владеть	
1	Основами комплексной защиты персональных данных
2	Специальной профессиональной терминологией

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах				
1.1	Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации /Лек/	9	2	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.2	Подготовка к практическому занятию по теме «Доктрина информационной безопасности Российской Федерации» /Ср/	9	4	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.3	Доктрина информационной безопасности Российской Федерации /Пр/	9	2	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.4	Содержание и основные положения Федерального закона «О персональных данных» /Лек/	9	4	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.5	Подготовка к практическому занятию по теме «Содержание и основные положения Федерального закона «О персональных	9	4	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3

	данных» /Ср/				Э1 Э2
1.6	Содержание и основные положения Федерального закона «О персональных данных /Пр/	9	2	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.7	Проработка материала по теме «Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах» /Ср/	9	4	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.8	Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных /Лек/	9	4	ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.9	Подготовка к практическому занятию по теме «Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных» /Ср/	9	4	ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.10	Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных /Пр/	9	2	ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
1.11	Обзор международных и национальных стандартов в сфере информационной безопасности /Лек/	9	2	ПК-22	Л1.2 Л1.3 Л2.2 Э1 Э2
1.12	Подготовка к зачету по разделу/Ср/	9	4	ПК-22	Л1.1 Л1.2 Л2.3
1.13	Зачет по разделу /Зачёт/	9	6	ПК-22	Л1.2 Л1.3
	Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных				
2.1	Общие положения и классификация угроз безопасности персональных данных /Лек/	9	3	ПК-23	Л1.1 Л1.2 Л2.1 Э2
2.2	Подготовка к практическому занятию по теме «Общие положения и классификация угроз безопасности персональных данных» /Ср/	9	4	ПК-23	Л1.1 Л1.2 Л2.1 Э2
2.3	Общие положения и классификация угроз безопасности персональных данных /Пр/	9	2	ПК-23	Л1.1 Л1.2 Л2.1 Э2
2.4	Классификация информационных систем персональных данных /Лек/	9	2	ПК-4	Л1.3 Л2.3 Э1 Э2
2.5	Подготовка к практическому занятию по теме «Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации» /Ср/	9	4	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.6	Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации /Пр/	9	1	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.7	Подготовка к лабораторной работе по теме «Выявление каналов утечки информации» /Ср/	9	4	ПК-4	Л1.3 Л2.3 Э1
2.8	Выявление каналов утечки информации /Лаб/	9	4	ПК-22	Л1.2 Л2.2 Э1 Э
2.9	Угрозы утечки информации по техническим каналам /Лек/	9	4	ПК-22	Л1.1 Л2.2 Э1 Э
2.10	Подготовка к практическому занятию по	9	4	ПК-22	Л1.3 Л2.2,

	теме «Средства обнаружения технических каналов утечки информации» /Ср/				Л2.3 Э1 Э
2.11	Средства обнаружения технических каналов утечки информации /Пр/	9	1	ПК-22	Л1.1 Л2.2, Л2.3 Э1 Э
2.12	Комплекс мероприятий по выявлению каналов утечки информации /Лек/	9	2	ПК-22,ПК-4	Л1.2 Л2.1, Л2.3 Э1 Э
2.13	Подготовка к лабораторной работе по теме «Перехват информации по техническим каналам утечки информации» /Ср/	9	4	ПК-22,ПК-4	Л1.1 Л1.2, Л2.2 Э1 Э
2.14	Перехват информации по техническим каналам утечки информации /Лаб/	9	2	ПК-22,ПК-4	Л1.2 Л2.1, Л2.2 Э1 Э
2.15	Подготовка к практическому занятию по теме «Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных» /Ср/	9	4	ПК-22,ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.16	Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных /Пр/	9	2	ПК-22,ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.17	Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей информационной системы персональных данных /Лек/	9	4	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.18	Подготовка к практическому занятию по теме «Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа» /Ср/	9	4	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.19	Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа /Пр/	9	2	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.20	Подготовка к лабораторной работе по теме «Аттестационные испытания системы защиты от несанкционированного доступа» /Ср/	9	4	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.21	Аттестационные испытания системы защиты от несанкционированного доступа /Лаб/	9	2	ПК-23	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.22	Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования /Лек/	9	2	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.23	Подготовка к практическому занятию по теме «Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы» /Ср/	9	2	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.24	Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы /Пр/	9	2	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
2.25	Зачет по разделу /Зачёт/	9	6	ПК-4	Л1.1 Л1.2 Л2.1 Л2.2

	Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных				
3.1	Общий порядок организации обеспечения безопасности персональных данных в ИСПДн /Лек/	9	3	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.2	Подготовка к практическому занятию по теме «Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации» /Ср/	9	4	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.3	Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации /Пр/	9	1	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.4	Подготовка к лабораторной работе по теме «Аттестация объектов информатизации» /Ср/	9	2	ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Э1 Э2
3.5	Аттестация объектов информатизации /Лаб/	9	4	ПК-4	Л1.1 Л1.2 Л2.2 Э2
3.6	Уведомление об обработке (о намерении осуществлять обработку) персональных данных /Лек/	9	2	ПК-23, ПК-22	Л1.1 Л2.2 Л2.3 Э1 Э2
3.7	Подготовка к практическому занятию по теме «Особенности обработки персональных данных без использования средств автоматизации» /Ср/	9	4	ПК-23, ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.8	Особенности обработки персональных данных без использования средств автоматизации /Пр/	9	1	ПК-23, ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.9	Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн /Лек/	9	4	ПК-23, ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.10	Проработка лекционного материала по теме «Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн» и подготовка к зачету по разделу /Ср/	9	2	ПК-23, ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.11	Проработка теоретической главы курсового проекта /Ср/	9	4	ПК-23, ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.12	Разработка практической главы курсового проекта /Ср/	9	6	ПК-23, ПК-22	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2
3.13	Защита курсового проекта /Лаб/	9	6	ПК-23, ПК-22, ПК-4	Л1.1 Л2.2 Л2.3 Э1 Э2
	Раздел 4. Контроль знаний				
4.1	Экзамен	9	36	ПК-23, ПК-22, ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Э1 Э2

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ

ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

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

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	М.А. Лапина, А.Г. Ревин, В.И. Лапин ; под ред. И.Ш. Килясханова	Информационное право: учебное пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% онлайн
Л1.2	Ю.Н. Загинайлов.	Теория информационной безопасности и методология защиты информации : учебное пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=276557	М. ; Берлин : Директ-Медиа, 2015	100% онлайн
Л1.3	И.Н. Кузнецов	Бизнес-безопасность [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=453908	М. : Издательско-торговая корпорация «Дашков и К°», 2016	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Н.С. Кармановский, О.В. Михайличенко, С.В. Савков	Организационно-правовое и методическое обеспечение информационной безопасности: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/43579	СПб. : НИУ ИТМО, 2013	100% онлайн
Л2.2	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% онлайн
Л2.3	И.В. Минин, О.В. Минин	Защита конфиденциальной информации при электронном документообороте : учебное пособие [Электронный ресурс] biblioclub.ru/index.php?page=book&id=228779	Новосибирск: НГТУ, 2011	100% онлайн

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: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	- Иркутск: ИрГУПС, 2013	55

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	Глухов Н.И.	Материалы для самостоятельной работы студентов	Личный кабинет обучающегося	100% онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Линия защиты «Сюртель» www.suritel.ru			
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
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, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844			
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org			
6.3.2 Перечень специализированного программного обеспечения				
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.			
6.3.3 Перечень информационных справочных систем				
6.3.3.1	«Консультант +» http://www.consultant.ru/			
6.3.3.2	«Техэксперт» http://www.cntd.ru/			
6.4 Перечень правовых и нормативных документов				
6.4.1	Не предусмотрено			

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

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

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 практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить задание на самостоятельную работу и выучить лекционный материал к следующей теме. Систематическое выполнение заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины.
Лабораторная работа	Понимание обучающимися таких фундаментальных понятий лабораторных работ как «цель работы», «выводы» из полученных результатов, рекомендации по их использованию. Порядок проведения лабораторного занятия: текущий контроль подготовленности студентов к выполнению конкретной лабораторной работы, выполнения ее задач, подготовка индивидуального отчета о проделанной работе и защита его перед преподавателем. Выполнение лабораторной работы оценивается преподавателем. Итоговые оценки за выполнение лабораторных работ учитываются при определении итоговой семестровой оценки по соответствующей учебной дисциплине.
Курсовая работа	Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсового проекта (Положение «Требования к оформлению текстовой и графической документации. «Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Реферат	Реферат – краткое письменное изложение материала по определенной теме, выполняется; цель – привить обучающимся навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу. Реферат – это самостоятельная учебно-исследовательская работа обучающегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер. Ознакомиться со структурой и оформление реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Самостоятельная работа	Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.
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.06 «Комплексная защита в информационных системах персональных данных»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.В.06 «Комплексная защита в информационных системах персональных данных»

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

Дисциплина «Комплексная защита в информационных системах персональных данных» участвует в формировании компетенций:

ПК-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

ПК-22: способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;

ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа.

Таблица траекторий формирования у обучающихся компетенций ПК-4, ПК-22, ПК-23 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-4	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Б1.Б.1.22 Основы информационной безопасности	3	1
		Б1.В.05 Методология анализа информационных рисков	8	2
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	3
		Б2.Б.04(Н) Производственная - научно-исследовательская работа	6	4
		Б2.Б.06(Пд) Производственная - преддипломная	А	5
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	5
ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Б1.В.04 Теоретические основы компьютерной безопасности	6	1
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	2
		Б2.Б.06(Пд) Производственная - преддипломная	А	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	3
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Б1.Б.1.19 Безопасность операционных систем	6	1
		Б1.Б.1.23 Криптографические методы защиты информации	7	2
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	3
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4

Таблица соответствия уровней освоения компетенций ПК-4, ПК-22, ПК-23 планируемым результатам обучения

Код компе-тенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-4	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных Раздел 4. Контроль знаний	Минимальный уровень	Знать: Математическое моделирование информационных рисков
				Уметь: Моделировать информационные риски
				Владеть: Программами математического моделирования
			Базовый уровень	Знать: Базовые модели угроз и нарушителей ИБ
				Уметь: Строить частные модели угроз на основе базовых
				Владеть: Руководящими документами ФСТЭК по построению частных моделей
			Высокий уровень	Знать: Методики построения модели угроз и модели нарушителя информационной безопасности автоматизированной системы
				Уметь: Применять руководящие документы ФСТЭК
				Владеть: Навыками разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы
ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных Раздел 3. Рекомендации и	Минимальный уровень	Знать: Терминологию, основные руководящие и регламентирующие документы в области информационной безопасности
				Уметь: Проводить анализ угроз безопасности информационных систем
				Владеть: Профессиональной терминологией в области ИБ
			Базовый уровень	Знать: Основные средства и способы обеспечения ИБ, принципы построения системы защиты ИБ
				Уметь: Реализовывать политику ИБ, применять нормативно-правовые акты и нормативно-правовые документы в области ИБ
				Владеть: Навыками разработки документирования, тестирования и отладки программного обеспечения по защите информации

		основные мероприятия по организации и обеспечению безопасности персональных данных Раздел 4. Контроль знаний	Высокий уровень	Знать: Нормативно-методические и правовые документы в области информационной безопасности
				Уметь: Разрабатывать проекты локальных нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии
				Владеть: Навыками работы и способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных Раздел 4. Контроль знаний	Минимальный уровень	Знать: Основные принципы, методы и процедуры организации работы с информацией ограниченного доступа
				Уметь: Реализовывать основные принципы, методы и процедуры организации работы с информацией ограниченного доступа
				Владеть: Терминологией по применению основные принципы, методы и процедуры организации работы с информацией ограниченного доступа
			Базовый уровень	Знать: Методологию применения нормативно-методических документов по организации работы для защиты информации ограниченного доступа
				Уметь: Применять нормативно-методических документов по организации работы для защиты информации ограниченного доступа
				Владеть: Навыками работы с нормативно-методическими документами по организации работы для защиты информации ограниченного доступа
			Высокий уровень	Знать: Основные руководящие документы, приказы ФСТЭК и ФСБ по формированию комплекса мер (правил, процедур, методов) для защиты информации ограниченного доступа
				Уметь: Применять основные руководящие документы, приказы ФСТЭК и ФСБ по формированию комплекса мер (правил, процедур, методов) для защиты информации ограниченного доступа
				Владеть: Навыками по применению основных руководящих документов, приказов ФСТЭК и ФСБ по формированию комплекса мер

				(правил, процедур, методов) для защиты информации ограниченного доступа

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)
9 семестр					
1	1	Текущий контроль	Тема «Доктрина информационной безопасности Российской Федерации»	ПК-4	Реферат (письменно)
2	1	Текущий контроль	Тема «Доктрина информационной безопасности Российской Федерации»	ПК-4	Доклад, сообщение (устно)
3	1	Текущий контроль	Тема «Содержание и основные положения Федерального закона «О персональных данных»	ПК-23	Реферат (письменно)
4	1	Текущий контроль	Тема «Содержание и основные положения Федерального закона «О персональных данных»	ПК-23	Доклад, сообщение (устно)
5	2	Текущий контроль	Тема «Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах»	ПК-23	Реферат (письменно)
6	2	Текущий контроль	Тема «Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных»	ПК-22	Реферат (письменно)
7	2	Текущий контроль	Тема «Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных»	ПК-22	Доклад, сообщение (устно)
8	3	Текущий контроль	Подготовка к зачету по разделу	ПК-22	Реферат (письменно)
9	4	Текущий контроль	Тема «Общие положения и классификация угроз безопасности персональных данных»	ПК-23	Реферат (письменно)
10	4	Текущий контроль	Тема «Общие положения и классификация угроз безопасности персональных данных»	ПК-23	Доклад, сообщение (устно)
11	5	Текущий контроль	Тема «Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации»	ПК-4	Реферат (письменно)
12	5	Текущий контроль	Тема «Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации»	ПК-4	Доклад, сообщение (устно)
13	5	Текущий контроль	Тема «Выявление каналов утечки информации»	ПК-4	Реферат (письменно)
14	5	Текущий контроль	Тема «Выявление каналов утечки	ПК-4	Защита лабораторной

			информации»		работы (письменно)
15	6	Текущий контроль	Тема «Средства обнаружения технических каналов утечки информации»	ПК-22	Реферат (письменно)
16	6	Текущий контроль	Тема «Средства обнаружения технических каналов утечки информации»	ПК-22	Доклад, сообщение (устно)
17	7	Текущий контроль	Тема «Перехват информации по техническим каналам утечки информации»	ПК-22, ПК-4	Реферат (письменно)
18	7	Текущий контроль	Тема «Перехват информации по техническим каналам утечки информации»	ПК-22, ПК-4	Защита лабораторной работы (письменно)
19	7	Текущий контроль	Тема «Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных»	ПК-22, ПК-4	Реферат (письменно)
20	9	Текущий контроль	Тема «Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных»	ПК-22, ПК-4	Доклад, сообщение (устно)
21	8	Текущий контроль	Тема «Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа»	ПК-23	Реферат (письменно)
22	9	Текущий контроль	Тема «Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа»	ПК-23	Доклад, сообщение (устно)
23	9	Текущий контроль	Тема «Аттестационные испытания системы защиты от несанкционированного доступа»	ПК-23	Реферат (письменно)
24	10	Текущий контроль	Тема «Аттестационные испытания системы защиты от несанкционированного доступа»	ПК-23	Защита лабораторной работы (письменно)
25	10	Текущий контроль	Тема «Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы»	ПК-4	Реферат (письменно)
26	12	Текущий контроль	Тема «Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы»	ПК-4	Доклад, сообщение (устно)
27	13	Текущий контроль	Тема «Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов	ПК-4	Реферат (письменно)

			информатизации»		
28	13	Текущий контроль	Тема «Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации»	ПК-4	Доклад, сообщение
29	14	Текущий контроль	Тема «Аттестация объектов информатизации»	ПК-4	Реферат (письменно)
30	14	Текущий контроль	Тема «Аттестация объектов информатизации»	ПК-4	Защита лабораторной работы (письменно)
31	15	Тест	Изученный материал	ПК-4, ПК-22, ПК-23	Перечень тестовых заданий
32	16	Текущий контроль	Тема «Особенности обработки персональных данных без использования средств автоматизации»	ПК-23, ПК-22	Реферат (письменно)
33	16	Текущий контроль	Тема «Особенности обработки персональных данных без использования средств автоматизации»	ПК-23, ПК-22	Доклад, сообщение
34	17	Текущий контроль	Тема «Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн»	ПК-23, ПК-22	Реферат (письменно)
35	17	Текущий контроль	Защита курсового проекта	ПК-4, ПК-22, ПК-23	Курсовой проект
36	18	Промежуточная аттестация – экзамен	Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных Раздел 4. Контроль знаний	ПК-4, ПК-22, ПК-23	Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно; оценка ответов на вопросы теста.

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

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

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и

корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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

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

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

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Реферат

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

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация Power

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

Курсовой проект

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсового проекта полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсового проекта и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсового проекта обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсового проекта полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсового проекта и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсового проекта обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсового проекта частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсового проекта. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсового проекта обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсового проекта в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много

	грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсового проекта обучающийся демонстрирует слабое понимание программного материала. Курсовой проект не представлен преподавателю. Обучающийся не явился на защиту курсового проекта..

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	18	Тестовые задания с выбором одного правильного ответа из нескольких	18
		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	9	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	36
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	42

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 89-96 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 81-88 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 73-80 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-72 баллов	Компетенция не сформирована

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

3.1 Перечень типовых тем рефератов

1. Информационная система персональных данных;
2. Средства разграничения доступа при обработке персональных данных в информационной системе;

3. Факторы, влияющие на выбор антивирусной защиты при обработке персональных данных в информационной системе;
4. Аттестация защищаемых помещений, как объектов обрабатывающих персональные данные;
5. Характеристика особенностей закона о персональных данных;
6. Сертификация средств защиты информации в ИСПДн;
7. Характеристика программного обеспечения средств защиты информации;
8. Технические способы защиты ПДн обрабатываемых в ИСПДн;
9. Автоматизированная обработка ПДн;
10. Понятие персональных данных;
11. Обработка персональных данных, их хранение и использование;
12. Обработка персональных данных в неавтоматизированном режиме;
13. Передача персональных данных;
14. Цели обеспечения защиты персональных данных;
15. Ответственность за нарушение норм регулирующих обработку и защиту персональных данных;
16. Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» ;
17. Трансграничная передача ПДн;
18. Уведомление об обработке ПДн;
19. Согласие на обработку ПДн;
20. Локальные нормативные акты на предприятии при обработке Пдн;
21. Журналы учета обращений;
22. Положение об обработке персональных данных на предприятии;
23. Специальные категории персональных данных;
24. Категории защищаемых персональных данных;
25. Общедоступные персональные данные;
26. Пассивные способы защиты персональных данных от утечки по техническим каналам;
27 Активные способы защиты персональных данных от утечки по техническим каналам;
28. Характеристика внутренних нарушителей для ИСПДн;
29. Характеристика внешних нарушителей для ИСПДн;
30. Рекомендуемым условием применения линейного электромагнитного зашумления при обработке ПДн.

3.2 Перечень типовых тем докладов, сообщений

1. Ответственность за нарушение ФЗ 152;
2. Основные международные нормативные документы в области защиты персональные данных;
3. Условия трансграничной передача ПДн;
4. Уведомление роскомнадзора об обработке ПДн;
5. Ответственность за нарушение при обработке ПДн;
6. Локальные нормативные документы при обработке Пдн;
7. Журналы учета информационных систем на предприятии;
8. Журналы учета защищаемых помещений и элементов информационных систем при обработке ПДН;
9. Модель положения об обработке персональных данных на предприятии;
10. Защищаемая категория персональных данных.

3.3 Перечень типовых тем курсовых проектов

1. Конфиденциальность персональных данных;
2. Условия обработки персональных данных;

3. Ответственность за неправомерное распространение персональных данных;
4. Применение гражданско-правового института к обязательствам работников, связанным с неправомерным распространением сведений;
5. Организационные источники и каналы утечки;
6. Силы, средства и условия организационной защиты информации;
7. Особенности системы организационной защиты информации;
8. Канал утечки информации за счет структурного звука в стенах и перекрытиях; методы выявления и способы подавления;
9. Видео-закладки, методика их использования для съема информации; выявление и противодействие;
10. Программно-аппаратные закладки в ПЭВМ; выявление и противодействие;
11. Радио-закладки в стенах и мебели; особенности применения, выявление и противодействие;
12. Методы съема акустической информации с окон с применением лазерной техники; способы противодействия;
13. Канал утечки информации образуемый за счет электромагнитных наводок на провода выходящие за пределы контролируемой зоны; методы выявления и способы противодействия;
14. Диктофоны; Технические возможности, способы применения; методы выявления и способы противодействия;
15. Образование высокочастотного канала утечки в бытовой технике; методы выявления и способы подавления;
16. Направленные микрофоны. Съем информации направленным микрофоном; методы противодействия;
17. Способы выявления каналов утечки информации, возникающих за счет акусто-электрических преобразователей в телефонных аппаратах;
18. Канал утечки информации в телефонных аппаратах за счет наличия акустоэлектрического преобразователя в звонковой цепи. Методы подавления;
19. Методы и способы проверки аппаратуры на наличие акусто-электрических преобразователей. Описание стенда и схема исследований;
20. Возникновение опасных сигналов в канале утечки информации образующегося за счет электромагнитного излучения средств вычислительной техники. Методы выявления и противодействие;
21. Поисковой прибор «Пиранья». Способы и методы выявления и оценки опасности утечки информации по виброакустическому каналу и за счет структурного звука;
22. Приборы «ВШВ». Состав. Метод использования дли оценки защищенности по виброакустическому каналу;
23. Поисковой прибор «Пиранья». Методы выявления канала утечки информации по цепям электропитания. Способы подавления;
24. Возникновение канала утечки информации по цепям заземления; выявление и противодействие;
25. Возникновение каналов утечки информации по трансляционной сети и громкоговорящей связи; выявление и противодействие;
26. Возникновение каналов утечки информации по сети охранно-пожарной сигнализации; выявление и противодействие;
27. Принципы построения систем видеонаблюдения (охранное телевидение); Основные технические характеристики применяемых видеокамер;
28. Принцип нелинейной локации. Нелинейные локаторы и способы обнаружения пассивных закладных устройств съема акустической информации в помещениях
29. Радиомониторинг. Принципы обнаружения радиозакладных устройств. Средства и системы применяемые для проведения радиомониторинга.

30. Системы контроля доступа в помещения. Принципы построения. Типовая схема контроля доступа.
31.Аппаратура закрытия телефонных переговоров. Скремблеры - принцип работы, методика применения.
32. Акусто-электрические преобразователи. Принципы работы. Особенности конструкции и использования

3.4 Тест

1 «Информация» это:

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 «Информационная система» это:

а совокупность информации, информационных технологий и технических средств

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

в совокупность информационных технологий и технических средств

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

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

3 Одним из основных факторов учитываемых при выборе средств антивирусной защиты является:

а удобство эксплуатации

б совместимость со штатным ПО

в наличие графического интерфейса

г Быстродействие

4 «Обладатель информации» это:

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

5 «Предоставление информации» это:

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

6 «Защищаемые помещения» это:

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

7 «Контролируемая зона» это:

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

8 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

9 Документом, определяющим лицензируемые виды деятельности, является:

а Постановление правительства РФ от 26 января 2006 г. № 45
Об организации лицензирования отдельных видов деятельности

б Постановление Правительство РФ от 15 августа 2006 г. № 504
О лицензировании деятельности по технической защите конфиденциальной информации

в Постановление Правительства РФ от 31 августа 2006 г. № 532
О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации

г ФЗ “О лицензировании отдельных видов деятельности” 99-ФЗ от 4 мая 2011 г.

д ФЗ “О техническом регулировании” 184-ФЗ от 27 декабря 2002 г.

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

а строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн

б детали интерьера, используемые для размещения ИСПДн

в средства контроля эффективности применения средств защиты информации

г средства контроля эффективности прочности ограждений

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

11 Программное обеспечение средств защиты информации, каких классов ИСПДн должно проходить контроль отсутствия недекларированных возможностей (НДВ)?

а К1

б К2

в К3

г К4

12 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

13 По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, ИСПДн подразделяются на:
(выберите все верные варианты ответов)

а Автоматизированные

б типовые

в Неавтоматизированные

г Специальные

д Специализированные

е Комбинированные

14 “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

15 Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных являются:
(выберите все верные варианты ответов)

а кражи технических средств информационной системы

б утечки акустической (речевой) информации

в утечки информации реализуемые через общедоступные информационные сети

г утечки видовой информации

д утечки информации по каналам побочных электромагнитных излучений

е утечки информации реализуемые через интернет

16 «Несанкционированный доступ» (НСД) 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

17 Выберите информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных:

а Автоматизированные

б типовые

в Неавтоматизированные

г Специальные

д Специализированные

18 «Специальные исследования (специсследования)» это:

а выявление с помощью контрольно - измерительной аппаратуры возможных каналов утечки информации

б определение соответствия условий эксплуатации объектов информатизации требованиям аттестатов соответствия, и других руководящих документов по спецзащите без применения контрольно - измерительной аппаратуры

в проверки технических средств иностранного и совместного производства на наличие возможно внедренных электронных устройств перехвата информации.

19 Пассивными способами защиты информации являются:

а создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств.

б ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны.

в создание маскирующих электромагнитных помех в цепях заземления ИСПДн.

г выставление постов охраны у помещений в которых размещаются технические средства обработки информации

20. Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК составляет_____ (Ответ)8

21. Укажите количество категорий персональных данных_____ (Ответ 4)

22. Укажите количество уровней защищенности ИСПДн _____ (Ответ 4)

23. 3 категория персональных данных — _____ (Ответ общедоступные) ПДн, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

24. Уровень защищенности персональных данных — это _____ (Ответ комплексный) показатель, который характеризует выполнение требований, _____ (нейтрализующих) угрозы безопасности информационных систем персональных данных.

25. Для определения уровня защищенности необходимо установить _____ (Ответ категории обрабатываемых) персональных данных субъектов (Ответ физических лиц), вид обработки по форме отношений между субъектами и организацией,_____ (Ответ количество субъектов), а также _____ (Ответ тип угроз актуальных) для информационной системы.

26. Нормативной основой защиты персональных данных являются нормы _____ (Ответ Конституции РФ), Федерального закона «О персональных данных», Указ Президента РФ _____ (Ответ «О перечне сведений конфиденциального характера») и другие акты.

27. Защита персональных данных — комплекс мероприятий _____ (Ответ технического), организационного и _____ (Ответ организационно-технического) характера, направленных на защиту сведений, относящихся к _____ или _____ (Ответ определенному или определяемому) на основании такой информации физическому лицу (субъекту персональных данных).

28. Укажите все регламентирующие документы в области обеспечения безопасности персональных данных

29. Какая информация относится к первой категории персональных данных

30. Охарактеризуйте каждый уровень защищенности информационной системы персональных данных

31. Охарактеризуйте каждую категорию персональных данных

32. Как осуществляется подбор и отбор персонала для обработки персональных данных

33 Охарактеризуйте специальную категорию персональных данных

3.5 Перечень теоретических вопросов к экзамену

1. Характеристика особенностей закона о персональных данных;
2. Технические способы защиты ПДн обрабатываемых в ИСПДн;
3. Обработка персональных данных, их хранение и использование;
4. Цели обеспечения защиты персональных данных;
5. Передача персональных данных;
6. Локальные нормативные акты на предприятии при обработке Пдн;
7. Положение об обработке персональных данных на предприятии;
8. Категории защищаемых персональных данных;
9. Ответственность за нарушение при обработке ПДн;
10. Журналы учета защищаемых помещений и элементов информационных систем при обработке ПДН;
11. Ответственность за неправомерное распространение персональных данных;
12. Организационные источники и каналы утечки;
13. Особенности системы организационной защиты информации;
14. Конфиденциальность персональных данных;
15. Условия обработки персональных данных;
16. Основные международные нормативные документы в области защиты персональные данных;
17. Пассивные способы защиты персональных данных от утечки по техническим каналам;
18. Активные способы защиты персональных данных от утечки по техническим каналам;
Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных»;
19. Характеристика особенностей закона о персональных данных;
20. Сертификация средств защиты информации в ИСПДн;
21. Характеристика программного обеспечения средств защиты информации;
22. Технические способы защиты ПДн обрабатываемых в ИСПДн;

3.6 Перечень типовых практических заданий к экзамену

1 Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК составляет_____ (Ответ)8
2. Укажите количество категорий персональных данных_____ (Ответ 4)
3. Укажите количество уровней защищенности ИСПДн _____ (Ответ 4)
4. 3 категория персональных данных — _____ (Ответ общедоступные) ПДн, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;
5. Уровень защищенности персональных данных — это _____ (Ответ комплексный) показатель, который характеризует выполнение требований, _____ (нейтрализующих) угрозы безопасности информационных систем персональных данных.
6. Для определения уровня защищенности необходимо установить _____ (Ответ категории обрабатываемых) персональных данных субъектов (Ответ физических лиц), вид обработки по форме отношений между субъектами и организацией,_____ (Ответ количество субъектов), а также _____ (Ответ тип угроз актуальных) для информационной системы.
7. Нормативной основой защиты персональных данных являются нормы _____ (Ответ Конституции РФ), Федерального закона «О персональных данных», Указ Президента РФ _____ (Ответ «О перечне сведений конфиденциального характера») и другие акты.
8. Защита персональных данных — комплекс мероприятий _____ (Ответ технического), организационного и _____ (Ответ организационно-технического) характера, направленных на защиту сведений, относящихся к

_____ или _____ (Ответ определенному или определяемому) на основании такой информации физическому лицу (субъекту персональных данных).

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Реферат	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит реферат или по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,2; предоставляет реферат преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Защита лабораторной работы	Обучаемый письменно излагает суть поставленной задачи и самостоятельно применяет стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводит анализ полученного результата работы. Обучаемый подготавливает индивидуальный отчет о проделанной работе и защищает его перед преподавателем. Выполнение лабораторной работы оценивается преподавателем. Итоговые оценки за выполнение лабораторных работ учитываются при определении итоговой семестровой оценки по соответствующей учебной дисциплине.
Курсовой проект	Обучаемый самостоятельно, под руководством преподавателя выполняет курсовой проект на заданную тему. Тема предлагается в общем виде. Конкретные методы и инструменты для ее разработки обучаемый выбирает самостоятельно. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

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

– перечень теоретических вопросов к зачету/экзамену для оценки знаний;

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

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

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

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

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

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

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

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

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

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Комплексная система в информационных системах персональных данных»** **__ семестр**	Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС _____
1. Цели обеспечения защиты персональных данных. 2. Укажите количество категорий персональных данных 3. Охарактеризуйте каждый уровень защищенности информационной системы персональных данных		

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.