ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

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

рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем
Специализация/профиль – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма 5 лет, 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

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

Формы промежуточной аттестации
очная форма обучения:
экзамен 9 семестр, курсовой проект 9 семестр

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

Семестр	9	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	51	**51**
– лекции	17	**17**
– практические (семинарские)	17	**17**
– лабораторные	17	**17**
Самостоятельная работа	93	**93**
Экзамен	36	**36**
Итого	180	**180**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем утвержденным Приказом Минобрнауки России от от 26.11.2020 № 1457.

Программу составил(и):
к.э.н., доцент, Н.И. Глухов

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

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цель дисциплины

1	раскрытие сущности и значения комплексного обеспечения безопасности персональных данных, обеспечение обучающихся теоретическими знаниями и практическими навыками, необходимыми для проведения работ по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями российского законодательства

1.2 Задачи дисциплины

1	изучение организационно-правовых и технических вопросов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных
2	проведение классификации информационных систем обработки персональных данных
3	изучение методов и процедур выявления угроз безопасности информации, построение модели угроз
4	создание подсистемы информационной безопасности при организации обработки 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

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.О.18 Правоведение
2	Б1.О.33 Основы информационной безопасности
3	Б1.О.34 Документоведение
4	Б1.О.38 Организационное и правовое обеспечение информационной безопасности
5	Б1.О.42 Открытые информационные системы
6	Б1.О.55 Защита объектов критической информационной инфраструктуры
7	Б2.О.01(У) Учебная - учебно-лабораторный практикум

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

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

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ОПК-5.1.1 Знает особенности разработки политики информационной безопасности открытых информационных систем	Знать: особенности разработки политики информационной безопасности открытых информационных систем
		Уметь: готовить документы по разработке политики информационной безопасности открытых информационных систем
		Владеть: навыками по оформлению документов по разработке политики информационной безопасности открытых информационных систем
	ОПК-5.1.2 Умеет формировать исходные требования для разработки политики информационной	Знать: исходные требования для разработки политики информационной безопасности
		Уметь: готовить документы по разработке политики информационной безопасности

	безопасности	Владеть: навыками по оформлению документов по разработке политики информационной безопасности
	ОПК-5.1.3 Имеет навыки обоснования целесообразности реализации политики информационной безопасности открытых информационных систем	Знать: особенности разработки политики информационной безопасности открытых информационных систем
		Уметь: готовить документы по разработке политики информационной безопасности открытых информационных систем
		Владеть: навыками по оформлению документов по разработке политики информационной безопасности открытых информационных систем
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Знает нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	Знать: нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
		Уметь: применять нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
		Владеть: навыками применения нормативно-правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации
	ОПК-5.2 Способен использовать общеправовые знания для организационных мероприятий по защите информации	Знать: методологию общеправовых знаний для организационных мероприятий по защите информации
		Уметь: применять общеправовые знания для организационных мероприятий по защите информации
		Владеть: навыками по применению общеправовых знаний для организационных мероприятий по защите информации
	ОПК-5.3 Имеет навыки оформления документов по организации защиты информации	Знать: оформление документов по организации защиты информации
		Уметь: применять документы по организации защиты информации
		Владеть: навыками по применению документов по организации защиты информации

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах**						
1.1	Тема 1. Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации	9	1				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.2	Тема 2. Доктрина информационной безопасности Российской Федерации	9		2		4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.3	Тема 3. Содержание и основные положения Федерального закона «О персональных данных»	9	2	2		4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.4	Тема 4. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.5	Тема 5. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных	9	1	2		4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.6	Тема 6. Обзор международных и национальных стандартов в сфере информационной безопасности	9	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.0	**Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных.**						
2.1	Тема 7. Общие положения и классификация угроз безопасности персональных данных	9	1	1		2	ОПК-5.1.1 ОПК-5.1.2
2.2	Тема 8. Классификация информационных систем персональных данных	9	2			2	ОПК-5.1.1 ОПК-5.1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
2.3	Тема 9. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации	9		1		2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.4	Тема 10. Выявление каналов утечки информации	9			5	1	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.5	Тема 11. Угрозы утечки информации по техническим каналам	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.6	Тема 12. Средства обнаружения технических каналов утечки информации	9		1		2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.7	Тема 13. Комплекс мероприятий по выявлению каналов утечки информации	9	2				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.8	Тема 14. Перехват информации по техническим каналам утечки информации	9			4	2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.9	Тема 15. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных	9		1		2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.10	Тема 16. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей информационной системы персональных данных	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.11	Тема 17. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа	9		1		2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.12	Тема 18. Аттестационные испытания системы защиты от несанкционированного доступа	9			4	3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.13	Тема 19. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.14	Тема 20. Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы	9		1		3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.0	**Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных.**						
3.1	Тема 21. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн	9	1				ОПК-5.1.1 ОПК-5.1.2
3.2	Тема 22. Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации	9		2		2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.3	Тема 23. Аттестация объектов информатизации	9			4	2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.4	Тема 24. Уведомление об обработке (о намерении осуществлять обработку) персональных данных	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.5	Тема 25. Особенности обработки персональных данных без использования средств автоматизации	9		3		6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.6	Тема 26. Требования к материальным носителям биометрических персональных данных и технологиям их	9	1			6	ОПК-5.1.1 ОПК-5.1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
	хранения вне ИСПДн						ОПК-5.1.3
	Форма промежуточной аттестации – экзамен	9	36				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
	Курсовая работа	9				40	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
	Итого часов (без учёта часов на промежуточную аттестацию)		17	17	17	93	

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Лапина, М. А. Информационное право : учебное пособие / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; под ред. И. Ш. Килясханов. — Москва : Юнити-Дана|Закон и право, 2017. — 336 с. — URL: https://biblioclub.ru/index.php?page=book&id=685428 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. — Москва, Берлин : Директ-Медиа, 2015. — 255 с. — URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — URL: https://e.lanbook.com/book/264242 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. — Самара : Самарский государственный архитектурно-строительный университет, 2014. — 113 с. — URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2.2	Минин, И. В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / И. В. Минин, О. В. Минин. — Новосибирск : Новосибирский государственный технический университет, 2011. — 20 с. — URL: https://biblioclub.ru/index.php?page=book&id=228779 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн

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

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн

6.1.3.1	Глухов Н.И. Методические указания по изучению дисциплины Б1.О.50 Комплексная защита в информационных системах персональных данных по специальности – 10.05.03 Информационная безопасность автоматизированных систем, специализация – Безопасность открытых информационных систем / Н.И. Глухов ; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 15 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47642_1529_2024_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.2.2	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем,

	обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе

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

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

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

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

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

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

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

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

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

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

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
9 семестр				
1.0	**Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах**			
1.1	Текущий контроль	Тема 1. Актуальность проблемы обеспечения безопасности персональных данных. Основные	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)

		понятия в области технической защиты информации		
1.2	Текущий контроль	Тема 2. Доктрина информационной безопасности Российской Федерации	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Содержание и основные положения Федерального закона «О персональных данных»	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно) Тестирование (компьютерные технологии)
1.4	Текущий контроль	Тема 4. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.5	Текущий контроль	Тема 5. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
1.6	Текущий контроль	Тема 6. Обзор международных и национальных стандартов в сфере информационной безопасности	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
2.0	**Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных**			
2.1	Текущий контроль	Тема 7. Общие положения и классификация угроз безопасности персональных данных	ОПК-5.1.1 ОПК-5.1.2	Собеседование (устно) Тестирование (компьютерные технологии)
2.2	Текущий контроль	Тема 8. Классификация информационных систем персональных данных	ОПК-5.1.1 ОПК-5.1.2	Собеседование (устно)
2.3	Текущий контроль	Тема 9. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.4	Текущий контроль	Тема 10. Выявление каналов утечки информации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно) Тестирование (компьютерные технологии)
2.5	Текущий контроль	Тема 11. Угрозы утечки информации по техническим каналам	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.6	Текущий контроль	Тема 12. Средства обнаружения технических каналов утечки информации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.7	Текущий контроль	Тема 13. Комплекс мероприятий по выявлению каналов утечки информации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.8	Текущий контроль	Тема 14. Перехват информации по техническим каналам утечки информации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.9	Текущий контроль	Тема 15. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.10	Текущий контроль	Тема 16. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно) Тестирование (компьютерные технологии)

		информационной системы персональных данных		
2.11	Текущий контроль	Тема 17. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.12	Текущий контроль	Тема 18. Аттестационные испытания системы защиты от несанкционированного доступа	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.13	Текущий контроль	Тема 19. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
2.14	Текущий контроль	Тема 20. Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
3.0	**Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных**			
3.1	Текущий контроль	Тема 21. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн	ОПК-5.1.1 ОПК-5.1.2	Собеседование (устно)
3.2	Текущий контроль	Тема 22. Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
3.3	Текущий контроль	Тема 23. Аттестация объектов информатизации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
3.4	Текущий контроль	Тема 24. Уведомление об обработке (о намерении осуществлять обработку) персональных данных	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
3.5	Текущий контроль	Тема 25. Особенности обработки персональных данных без использования средств автоматизации	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
3.6	Текущий контроль	Тема 26. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
	Промежуточная аттестация	Все разделы	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Курсовая работа (письменно) Курсовая работа (устно)
	Промежуточная аттестация	Все разделы	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

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

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

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

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

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

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

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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 (образец экзаменационного билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	Курсовая работа	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.	Образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты

		Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	

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

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«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
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме экзамена

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

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы

«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы 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. При защите курсовой работы 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 курсовой работы 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 курсовой работы. 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. При защите курсовой работы 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 курсовой работы 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. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Тестирование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования

«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

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

3.1 Типовые контрольные задания для проведения собеседования

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

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования

1. Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации;
2. Доктрина информационной безопасности Российской Федерации;
3. Содержание и основные положения Федерального закона «О персональных данных»;
4. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах;
5. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных;
6. Обзор международных и национальных стандартов в сфере информационной безопасности;
7. Общие положения и классификация угроз безопасности персональных данных;
8. Классификация информационных систем персональных данных;
9. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации;
10. Выявление каналов утечки информации;
11. Угрозы утечки информации по техническим каналам;
12. Средства обнаружения технических каналов утечки информации;
13. Комплекс мероприятий по выявлению каналов утечки информации;
14. Перехват информации по техническим каналам утечки информации;
15. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных;
16. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей информационной системы персональных данных;
17. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа;
18. Аттестационные испытания системы защиты от несанкционированного доступа;
19. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования;
20. Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы;
21. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн;
22. Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации;
23. Аттестация объектов информатизации;

24. Уведомление об обработке (о намерении осуществлять обработку) персональных данных;

25. Особенности обработки персональных данных без использования средств автоматизации;

26. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн.

3.2 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 1. Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации	Знание	1 – ОТЗ
		Умение	2 – ЗТЗ
		Навык	2 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 2. Доктрина информационной безопасности Российской Федерации	Знание	1 – ЗТЗ
		Умение	2 – ОТЗ
		Навык	2 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 3. Содержание и основные положения Федерального закона «О персональных данных»	Знание	1 – ОТЗ
		Умение	2 – ЗТЗ
		Навык	2 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 4. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах	Знание	1 – ЗТЗ
		Умение	2 – ОТЗ
		Навык	2 – ЗТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 5. Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных	Знание	1 – ОТЗ
		Умение	2 – ЗТЗ
		Навык	2 – ОТЗ
ОПК-5.1 ОПК-5.2 ОПК-5.3	Тема 6. Обзор международных и национальных стандартов в сфере информационной безопасности	Знание	1 – ЗТЗ
		Умение	2 – ОТЗ
		Навык	2 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2	Тема 7. Общие положения и классификация угроз безопасности персональных данных	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	2 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2	Тема 8. Классификация информационных систем персональных данных	Знание	2 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	2 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 9. Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации	Знание	2 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	2 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 10. Выявление каналов утечки информации	Знание	2 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	2 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 11. Угрозы утечки информации по техническим каналам	Знание	2 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	2 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 12. Средства обнаружения технических каналов утечки информации	Знание	2 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 13. Комплекс мероприятий по выявлению каналов утечки информации	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 14. Перехват информации по техническим каналам утечки информации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2	Тема 15. Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы,	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ

ОПК-5.1.3	используемые для создания системы защиты персональных данных	Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 16. Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей информационной системы персональных данных	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 17. Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 18. Аттестационные испытания системы защиты от несанкционированного доступа	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 19. Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 20. Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2	Тема 21. Общий порядок организации обеспечения безопасности персональных данных в ИСПДн	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 22. Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 23. Аттестация объектов информатизации	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 24. Уведомление об обработке (о намерении осуществлять обработку) персональных данных	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 25. Особенности обработки персональных данных без использования средств автоматизации	Знание	1 – ОТЗ
		Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Тема 26. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
		Итого	50 – ОТЗ 50 – ЗТЗ

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

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

Образец типового варианта итогового теста,
предусмотренного рабочей программой дисциплины

1. Информация – это

Ответ: сведения (сообщения, данные) независимо от формы их представления.

2. Обладатель информации – это

Ответ: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора 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. 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.

6. 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.

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

а) полуактивные;

б) пассивные;

в) разноплановые;

г) удостоверяющие;

д) активные.

8. Технический канал утечки информации – это

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

9. 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.

10. Несанкционированный доступ к информации – это

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

11. Механизм контроля целостности СЗИ Secret Net предназначен для _____

Ответ: слежения за неизменностью содержимого ресурсов компьютера.

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

а) ограничения использования программного обеспечения на компьютере;

б) установки ограниченного количества программ;

в) сбора сведений об используемых приложениях.

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

а) «конфиденциально»;

б) «секретно»;

в) «строго конфиденциально»,

г) «неконфиденциально».

14. К какому типу криптосистем относится алгоритм AES?

а) несимметричные;

б) асиммеричные;

в) симметричные;

г) полусимметричные.

15. Пассивными способами защиты информации являются _____

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

16. Межсетевой экран служит для _____

Ответ: фильтрации трафика при передачи данных.

17. Хэш-функции предназначены, главным образом, для контроля _____

Ответ: целостности данных.

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

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

3.3 Типовое задание для выполнения курсовой работы

Типовые задания выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты.

Образец типового задания для выполнения курсовой работы

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 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 Перечень теоретических вопросов к экзамену

(для оценки знаний)

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

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста
Курсовая работа	Ход выполнения разделов курсовой работы в рамках текущего контроля оценивается преподавателем исходя из объемов выполненных работ в соответствие со шкалами оценивания. Преподаватель информирует обучающихся о результатах оценивания выполнения курсового проекта сразу после контрольно-оценочного мероприятия.

	В ходе защиты курсовой работы обучающийся делает доклад протяженностью 5 – 7 минут. Преподаватель ставит окончательную оценку за курсовую работу после завершения защиты, учитывая уровень ее защиты

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

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

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

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы 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; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое 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 фондов оценочных средств.

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

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

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Комплексная защита в информационных системах персональных данных»**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. Требования к симметричным и асимметричным криптосистемам 2. Базовые принципы организации ЗИ 3. Алгоритм DES; свойства стандарта AES 4. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа		