ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказ ректора
от «07» июня 2021 г. №78

Б1.0.50 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 6 мес
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	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**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 ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденным Приказом Министерства образования и науки Российской Федерации от 26.11.2020 г. № 1457

Программу составил:
к.э.н. доцент кафедры «ИСиЗИ» Н.И. Глухов

Рабочая программа дисциплины обсуждена и рекомендована к применению в образовательном процессе для обучения обучающихся по специальности 10.05.03 Информационная безопасность автоматизированных систем на заседании кафедры «Информационные системы и защита информации».
Протокол от «04» 06 2021 г. № 11/2

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

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.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Основы управленческой деятельности
2	Техническая защита информации
3	Организационное и правовое обеспечение информационной безопасности
4	Методология анализа информационных рисков
5	Производственная – проектно-технологическая практика
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Аудит информационной безопасности
2	Производственная - преддипломная
3	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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1 Знает нормативно-правововые акты, нормативные и методические документы, регламентирующие деятельность по защите информации ОПК-5.2 Способен использовать общеправовые знания для организационных мероприятий по защите информации ОПК-5.3 Имеет навыки оформления документов по организации защиты информации	**Знать:** нормативно-правововые 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-5.1.1 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 безопасности	**Знать:** исходные требования для разработки политики информационной безопасности **Уметь:** готовить документы по разработке политики информационной 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

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	Срс	
	Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах						ОПК-5.1 ОПК-5.2 ОПК-5.3
1.1	Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации /Лек/	9	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.2	Подготовка к практическому занятию по теме «Доктрина информационной безопасности Российской Федерации» /Ср/	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.3	Доктрина информационной безопасности Российской Федерации /Пр/	9		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.4	Содержание и основные положения Федерального закона «О персональных данных» /Лек/	9	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.5	Подготовка к практическому занятию по теме «Содержание и основные положения Федерального закона «О персональных данных» /Ср/	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.6	Содержание и основные положения Федерального закона «О персональных данных /Пр/	9		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.7	Проработка материала по теме «Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах» /Ср/	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.8	Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных /Лек/	9	1				ОПК-5.1 ОПК-5.2 ОПК-5.3
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	ОПК-5.1 ОПК-5.2 ОПК-5.3

1.10	Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных /Пр/	9		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.11	Обзор международных и национальных стандартов в сфере информационной безопасности /Лек/	9	1				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.12	Подготовка к зачету по разделу/Ср/	9				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.13	Зачет по разделу /Зачёт/	9		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
	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	1				ОПК-5.1.1 ОПК-5.1.2
2.2	Подготовка к практическому занятию по теме «Общие положения и классификация угроз безопасности персональных данных» /Ср/	9				2	ОПК-5.1.1 ОПК-5.1.2
2.3	Общие положения и классификация угроз безопасности персональных данных /Пр/	9		1			ОПК-5.1.1 ОПК-5.1.2
2.4	Классификация информационных систем персональных данных /Лек/	9	1				ОПК-5.1.1 ОПК-5.1.2
2.5	Подготовка к практическому занятию по теме «Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации» /Ср/	9				2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.6	Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации /Пр/	9		1			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.7	Подготовка к лабораторной работе по теме «Выявление каналов утечки информации» /Ср/	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.8	Выявление каналов утечки информации /Лаб/	9			5		ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.9	Угрозы утечки информации по техническим каналам /Лек/	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.10	Подготовка к практическому занятию по теме «Средства обнаружения технических каналов утечки информации» /Ср/	9				2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.11	Средства обнаружения технических каналов утечки информации /Пр/	9		1			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.12	Комплекс мероприятий по выявлению каналов утечки информации /Лек/	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.13	Подготовка к лабораторной работе по теме «Перехват информации по техническим каналам утечки информации» /Ср/	9				2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.14	Перехват информации по техническим каналам утечки информации /Лаб/	9			4		ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.15	Подготовка к практическому занятию по теме «Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые	9				2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3

	для создания системы защиты персональных данных» /Ср/						
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		1			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.17	Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей информационной системы персональных данных /Лек/	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
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				2	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.19	Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа /Пр/	9		1			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.20	Подготовка к лабораторной работе по теме «Аттестационные испытания системы защиты от несанкционированного доступа» /Ср/	9				33	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.21	Аттестационные испытания системы защиты от несанкционированного доступа /Лаб/	9			4		ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.22	Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования /Лек/	9	1				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
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				3	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.24	Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы /Пр/	9		1			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
2.25	Зачет по разделу /Зачёт/	9				4	
	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					
3.2	Подготовка к практическому занятию по теме «Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации» /Ср/	9				2	
3.3	Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации /Пр/	9		1			
3.4	Подготовка к лабораторной работе по теме «Аттестация объектов информатизации» /Ср/	9				2	
3.5	Аттестация объектов информатизации /Лаб/	9			4		
3.6	Уведомление об обработке (о намерении осуществлять обработку) персональных	9	1				

	данных /Лек/						
3.7	Подготовка к практическому занятию по теме «Особенности обработки персональных данных без использования средств автоматизации» /Ср/	9				2	
3.8	Особенности обработки персональных данных без использования средств автоматизации. Раздача тем курсовых работ /Пр/	9		1			
3.9	Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн /Лек/	9	1				
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	
3.11	Проработка теоретических разделов курсовой работы /Ср/	9				2	
3.12	Разработка практических разделов курсовой работы /Ср/	9				5	
3.13	Защита курсовой работы /Пр/	9					
	Раздел 4. Контроль знаний						
4.1	Подготовка к промежуточной аттестзделовации (Экзамен)	9	17	17	17	57 (36)	

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

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по 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	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие //biblioclub.ru/index.php?page=book&id=276557	М. ; Берлин : Директ-Медиа, 2015	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 7 Professional, лицензия № 49379844, обновление - контракт №03341000100180000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 03341000100190000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд		
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №03341000100180000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 03341000100190000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice 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.	

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости
и промежуточной аттестации по дисциплине

Б1.0.50 Комплексная защита в информационных системах персональных данных

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем

ИРКУТСК

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 Университета, а так же 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 (модуля) или прохождения практики*;

– 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 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-5.1 Знает нормативно-правововые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

ОПК-5.2 Способен использовать общеправовые знания для организационных мероприятий по защите информации

ОПК-5.3 Имеет навыки оформления документов по организации защиты информации

ОПК-5.1.1 Знает особенности разработки политики информационной безопасности открытых информационных систем

ОПК-5.1.2. Умеет формировать исходные требования для разработки политики информационной безопасности

ОПК-5.1.3 Имеет навыки обоснования целесообразности реализации политики информационной безопасности открытых информационных систем

Программа контрольно-оценочных мероприятий за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения)
9 семестр					
			Раздел 1. Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах		
1	2	Текущий контроль	Актуальность проблемы обеспечения безопасности персональных данных. Основные понятия в области технической защиты информации /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
2	2	Текущий контроль	Подготовка к практическому занятию по теме «Доктрина информационной безопасности Российской Федерации» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
3	3	Текущий контроль	Доктрина информационной безопасности Российской Федерации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
4	3	Текущий контроль	Содержание и основные положения Федерального закона «О персональных данных» /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
5	4	Текущий контроль	Подготовка к практическому занятию по теме «Содержание и основные положения Федерального закона «О персональных данных» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
6	4	Текущий контроль	Содержание и основные положения Федерального закона «О персональных данных /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
7	4	Текущий контроль	Проработка материала по теме «Нормативно-правовое обеспечение безопасности персональных данных, обрабатываемых в информационных системах» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
8	5	Текущий контроль	Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
9	5	Текущий контроль	Подготовка к практическому занятию по теме «Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно
10	6	Текущий контроль	Правовые и нормативно-методические документы по технической защите конфиденциальной информации и обеспечению безопасности персональных данных /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)

11	6	Текущий контроль	Обзор международных и национальных стандартов в сфере информационной безопасности /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
12	6	Текущий контроль	Подготовка к зачету по разделу/Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
13	6	Текущий контроль	Зачет по разделу /Зачёт/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
14			**Раздел 2. Выявление угроз и уязвимостей безопасности персональных данных. Методы и способы технического обеспечения безопасности персональных данных**		
15	7	Текущий контроль	Общие положения и классификация угроз безопасности персональных данных /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
16	7	Текущий контроль	Подготовка к практическому занятию по теме «Общие положения и классификация угроз безопасности персональных данных» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
17	8	Текущий контроль	Общие положения и классификация угроз безопасности персональных данных /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
18	8	Текущий контроль	Классификация информационных систем персональных данных /Лек/ Подготовка к практическому занятию по теме «Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
19	9	Текущий контроль	Классификация и характеристики аппаратуры перехвата информации по техническим каналам утечки информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
20	9	Текущий контроль	Подготовка к лабораторной работе по теме «Выявление каналов утечки информации» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
21	10	Текущий контроль	Выявление каналов утечки информации /Лаб/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
22	10	Текущий контроль	Угрозы утечки информации по техническим каналам /Лек/Подготовка к практическому занятию по теме «Средства обнаружения технических каналов утечки информации» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
23	10	Текущий контроль	Средства обнаружения технических каналов утечки информации /Пр/Комплекс мероприятий по выявлению каналов утечки информации	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование

			/Лек/		
24	11	Текущий контроль	Подготовка к лабораторной работе по теме «Перехват информации по техническим каналам утечки информации» /Ср/Перехват информации по техническим каналам утечки информации /Лаб/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
25	11	Текущий контроль	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/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
26	12	Текущий контроль	Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы, используемые для создания системы защиты персональных данных /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
27	13	Текущий контроль	Угрозы несанкционированного доступа к информации в ИСПДн. Характеристика источников угроз НСД и уязвимостей информационной системы персональных данных /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
28	13	Текущий контроль	Подготовка к практическому занятию по теме «Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа» /Ср/ Общая характеристика результатов несанкционированного или случайного доступа. Методика аттестационных испытаний системы защиты от несанкционированного доступа /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
29	14	Текущий контроль	Подготовка к лабораторной работе по теме «Аттестационные испытания системы защиты от несанкционированного доступа» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
30	14	Текущий контроль	Аттестационные испытания системы защиты от несанкционированного доступа /Лаб/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
31	14	Текущий контроль	Методика определения и разработка частной модели угроз безопасности персональных данных в ИСПДн с учетом их назначения, условий и особенностей функционирования /Лек/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
32	15	Текущий контроль	Подготовка к практическому занятию по теме «Методы и	ОПК-5.1 ОПК-5.2	Собеседование (устно)

			способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы» /Ср/	ОПК-5.3	
33	15	Текущий контроль	Методы и способы защиты персональных данных от несанкционированного доступа в зависимости от класса информационной системы /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
34	15	Текущий контроль	Зачет по разделу /Зачёт/		
35			**Раздел 3. Рекомендации и основные мероприятия по организации и обеспечению безопасности персональных данных**		
36	16	Текущий контроль	Общий порядок организации обеспечения безопасности персональных данных в ИСПДн /Лек/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
37	16	Текущий контроль	Подготовка к практическому занятию по теме «Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации» /Ср/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
38	16	Текущий контроль	Лицензирование деятельности по технической защите конфиденциальной информации. Сертификация средств защиты информации и аттестация объектов информатизации /Пр/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
39	17	Текущий контроль	Подготовка к лабораторной работе по теме «Аттестация объектов информатизации» /Ср/ Аттестация объектов информатизации /Лаб/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
40	17	Текущий контроль	Уведомление об обработке (о намерении осуществлять обработку) персональных данных /Лек/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
41	17	Текущий контроль	Подготовка к практическому занятию по теме «Особенности обработки персональных данных без использования средств автоматизации» /Ср/ Особенности обработки персональных данных без использования средств автоматизации /Пр/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
42	17	Текущий контроль	Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне ИСПДн /Лек/ 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/	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
43	18	Текущий контроль	Проработка теоретической главы	ОПК-5.1	Собеседование

			курсового проекта /Ср/	ОПК-5.2 ОПК-5.3 ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	(устно)
44	18	Текущий контроль	Разработка практической главы курсового проекта /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
45	18	Текущий контроль	Защита курсового проекта /Лаб/	ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
46			**Раздел 4. Контроль знаний**		
47	18	Текущий контроль	Подготовка к промежуточной аттестации (Экзамен)	ОПК-5.1 ОПК-5.2 ОПК-5.3 ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)

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

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

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

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

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	Собеседование	Средство, позволяющее оценить умение обучающегося излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Перечень вопросов и заданий для обсуждения

2	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
3	Курсовой проект (работа)	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 (работу)
4	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 результатов обучения при проведении текущего контроля успеваемости

Тест (структура теста по компетенциям)

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

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенции

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

Курсовой проект (работа) – *пример 1*

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсового проекта (работы) полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта (работы) логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсового проекта (работы) и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсового проекта (работы) обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсового проекта (работы) полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсового проекта (работы) логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсового проекта (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. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсового проекта (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 курсового проекта (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 курсового проекта (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. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсового проекта (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 курсового проекта (работы) в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсового проекта (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 (работы) обучающийся демонстрирует слабое понимание программного материала. Курсовой проект (работа) не представлена преподавателю. Обучающийся не явился на защиту курсового проекта (работы)

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. Тест

1. Выберите правильное определение термина «информация»:
   а) совокупность содержащихся в базах данных сведений;
   б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
   в) сведения (сообщения, данные) воспроизводимые различными системами;
   г) сведения (сообщения, данные) независимо от формы их представления.
2. Выберите правильное определение термина «обладатель информации»:
   а) лицо, самостоятельно создавшее информацию;
   б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
   в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
   г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
3. Выберите правильное определение термина «предоставление информации»:
   а) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
   б) действия, направленные на распространение сведений в средствах массовой информации;
   в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
   г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённому кругу лиц.
4. Выберите правильное определение термина «защищаемые помещения»:
   а) помещения, специально предназначенные для хранения носителей конфиденциальной информации;
   б) помещения, специально предназначенные для размещения технических средств информационной системы;
   в) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы;
   г) помещения, специально предназначенные для проведения конфиденциальных мероприятий;
5. Выберите правильное определение термина «контролируемая зона»:
   а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;
   б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;
   в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;

г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):
   а) методы и способы защиты информации от несанкционированного доступа;
   б) методы и способы сокрытия информации от внутренних нарушителей;
   в) методы и способы устранения конкурентов;
   г) методы и способы защиты информации от утечки по техническим каналам;
7. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):
   а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;
   б) детали интерьера, используемые для размещения 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.
8. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):
   а) полуактивные;
   б) пассивные;
   в) разноплановые;
   г) удостоверяющие;
   д) активные.
9. “Технический канал утечки информации” - это:
   а) совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
   б) совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств;
   в) совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
   г) совокупность объекта технической разведки и средств, которыми добывается защищаемая информация.
10. Техническими каналами утечки информации являются (выберите все верные варианты ответов):
   а) кражи технических средств информационной системы;
   б) утечки акустической (речевой) информации;
   в) утечки информации, реализуемые через общедоступные информационные сети;
   г) утечки видовой информации;
   д) утечки информации по каналам побочных электромагнитных излучений;
   е) утечки информации, реализуемые через интернет;
11. «Несанкционированный доступ к информации» - это:
   а) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
   б) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;
   в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;
   г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

12. «Персональный идентификатор» — это
    а) устройство для хранения зашифрованной информации пользователя;
    б) устройство для хранения информации, необходимой при идентификации и аутентификации пользователя;
    в) устройство для хранения журнала аудита.
13. Механизм контроля целостности СЗИ Secret Net предназначен для
    а) формирония цифровых отпечатков данных;
    б) контроля информационных потоков;
    в) слежения за неизменностью содержимого ресурсов компьютера.
14. 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.
15. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями
    а) «конфиденциально»;
    б) «секретно»;
    в) «строго конфиденциально»,
    г) «неконфиденциально».
16. Длина ключа шифрования алгоритма ГОСТ 28147-89 равна
    а) 56 бит;
    б) 256 бит;
    в) 1024 бит;
    г) 128 бит.
17. К какому типу криптосистем относится алгоритм AES?
    а) несимметричные;
    б) асиммеричные;
    в) симметричные;
    г) полусимметричные.
18. 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;
    г) выставление постов охраны у помещений, в которых размещаются технические средства обработки информации.
19. Межсетевой экран служит для:
    а) разграничения доступа в помещения АИС;
    б) фильтрации трафика при передачи данных;
    в) защиты от утечек информации путем экранирования стен;
    г) контроля целостности программного обеспечения.
20. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно _____ (16).
21. В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____ (NTFS).
22. Практическая стойкость алгоритма RSA основана на сложности решения задачи _____ (факторизации).
23. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного_____ (логарифма).

24. Эффективным средством защиты от утечки информации из АИС показали себя _____ (DLP) – системы.
25. Хэш-функции предназначены, главным образом, для контроля _____(целостности) данных.
26. Технология электронной подписи разработана с целью подтверждения _____ (авторства) и _____ (подлинности) сообщений.
27. Длина хэш-кода алгоритма MD5 составляет _____ (128) бит.
28. Как в СЗИ Secret Net происходит включение режима хранения пароля в идентифика торе?

    (Основной тезис: происходит добавление в базу данных Secret Net сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора).
29. Каким образом в СЗИ Secret Net происходит присвоение пользователю персонального идентификатора?

    (Основной тезис: происходит добавление в базу данных Secret Net сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером).
30. Каким образом в СЗИ Secret Net реализуется затирание файлов?

    (Основной тезис: при действии механизма затирания в область диска, где физически было расположено содержимое удаленного файла, записывается последовательность случайных чисел).
31. Что происходит при выборе способа очистки журнала СЗИ Secret Net при его переполнении «Затирать события по мере необходимости»?

    (Основной тезис: при переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей).
32. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

    (Основной тезис: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы).
33. Кратко описать назначение и функции Удостоверяющего Центра в системе PCI.

3.2. Перечень теоретических вопросов к семинарам

1. Резервирование и восстановление информации; повышение надежности АИС;
2. Блокировка ошибочных операций пользователей; минимизация ущерба от аварий и стихийных бедствий;
3. Инженерно-физическая защита объектов информатизации; система контроля и управления доступом;
4. Организация работ с конфиденциальными информационными ресурсами;
5. защита от злоумышленных действий обслуживающего персонала и пользователей;
6. Понятие и возможности DLP-систем;
7. Методы и средства защиты информации в АИС от утечек по техническим каналам;
8. Противодействие наблюдению в оптическом диапазоне; противодействие утечкам по группе акустических каналов;
9. Методы и средства защиты от побочных электромагнитных излучений и наводок;
10. Компьютерные вирусы; троянские программы; сетевые черви; сертифицированные средства антивирусной защиты;

11. Средства сетевой безопасности: межсетевые экраны, сканеры безопасности;
12. Средства сетевой безопасности: средства построения виртуальных частных сетей (VPN), системы обнаружения вторжений.

3.3. Перечень теоретических вопросов к экзамену

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

3.4. Перечень типовых простых практических заданий к экзамену

Формируется на основании требований теоретических вопросов.

3.5.Перечень тем курсовых работ.

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.

1. Канал утечки информации за счет структурного звука в стенах и перекрытиях; методы выявления и способы подавления;
2. Видио-закладки, методика их использования для съема информации; выявление и противодействие;
3. Программно-аппаратные закладки в ПЭВМ; выявление и противодействие;

4. Радио-закладки в стенах и мебели; особенности применения, выявление и противодействие;
5. Методы съема акустической информации с окон с применением лазерной техники; способы противодействия;
6. Канал утечки информации образуемый за счет электромагнитных наводок на провода выходящие за пределы контролируемой зоны; методы выявления и способы противодействия;
7. Диктофоны; Технические возможности, способы применения; методы выявления и способы противодействия;
8. Образование высокочастотного канала утечки в бытовой технике; методы выявления и и способы подавления;
9. Направленные микрофоны. Съем информации направленным микрофоном; методы противодействия
10. Способы выявления каналов утечки информации, возникающих за счет акусто - электрических преобразователей в телефонных аппаратах.
11. Канал утечки информации в телефонных аппаратах за счет наличия акустоэлектрического преобразователя в звонковой цепи. Методы подавления.
12. Методы и способы проверки аппаратуры на наличие акусто-электрических преобразователей. Описание стенда и схема исследований.
13. Возникновение опасных сигналов в канале утечки информации образующегося за счет электромагнитного излучения средств вычислительной техники. Методы выявления и противодействие;
14. Поисковой прибор «Пиранья». Способы и методы выявления и оценки опасности утечки информации по виброакустическому каналу и за счет структурного звука.
15. Приборы «ВШВ». Состав. Метод использования дли оценки защищенности по виброакустическому каналу.
16. Поисковой прибор «Пиранья». Методы выявления канала утечки информации по цепям электропитания. Способы подавления
17. Возникновение канала утечки информации по цепям заземления; выявление и противодействие;
18. Возникновение каналов утечки информации по трансляционной сети и громкоговорящей связи; выявление и противодействие;
19. Возникновение каналов утечки информации по сети охранно-пожарной сигнализации; выявление и противодействие;
20. Принципы построения систем видеонаблюдения (охранное телевидение); Основные технические характеристики применяемых видеокамер;
21. Принцип нелинейной локации. Нелинейные локаторы и способы обнаружения пассивных закладных устройств съема акустической информации в помещениях
22. Радиомониторинг. Принципы обнаружения радиозакладных устройств. Средства и системы применяемые для проведения радиомониторинга.
23. Системы контроля доступа в помещения. Принципы построения. Типовая схема контроля доступа.
24. Аппаратура закрытия телефонных переговоров. Скремблеры - принцип работы, методика применения.
25. Акусто-электрические преобразователи. Принципы работы. Особенности конструкции. и использования.

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
Тест	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Курсовой проект (работа)	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения

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 2021-2022 учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** **__ ____ семестр**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. …… 2. …… 3. …….. 4. …….. 5 ……..…… Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		

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.

Составитель _____к.э.н, доцент Н.И. Глухов