

Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ (подпись)

Василенко В.Н.
(Ф.И.О.)

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность персональных данных

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1. Цели и задачи дисциплины (модуля)

Целями и задачами освоения дисциплины «Безопасность персональных данных» являются:

освоение специалистами актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Поставленная цель достигается решением следующих задач:

изучением нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;

изучением методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;

практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области	Основные средства и системы защиты информации, используемые при защите персональных данных. Основные угрозы безопасности персональных данных. Научные и организационные основы	Анализировать программные, архитектурно-технические и схемотехнические решения компонентов информационных систем персональных данных с целью разра-	Навыками разработки технического задания на разработку системы защиты информационной системы персональных данных.

			защиты информации в информационных системах персональных данных.	ботки модели угроз.	
2	ПК-21	Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Информационную систему персональных данных как объект реализации угроз информационной безопасности, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; методы, способы, средства, последовательность и содержание этапов разработки информационных систем персональных данных и подсистем защиты	Проводить классификацию информационных систем персональных данных.	Навыками выбора организационных и технических мероприятий по защите информации персональных данных.
3	ПСК-4.4	Способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	Методологии и методы проектирования систем защиты персональных данных	Разрабатывать техническое задание на разработку системы защиты персональных данных.	Навыками контроля защищенности персональных данных в информационных системах при эксплуатации.

3. Место дисциплины в структуре ОПОП ВО

Дисциплина «Безопасность персональных данных» относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин и прохождении практик:

- Технологии разработки защищенного документооборота;
- Учебная практика, ознакомительная;
- Учебная практика, практика по получению первичных профессиональных умений.

Дисциплина является предшествующей для прохождения практик:

- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;
- Производственная практика, преддипломная практика; защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины (модуля) и виды учебных занятий

Общая трудоемкость дисциплины (модуля) составляет 6 зачетных единиц.

Виды учебной работы	Всего часов	Семестр	
		5	6
	акад.	акад.	акад.
Общая трудоемкость дисциплины	216	72	144

Аудиторная работа	121,25	45,85	75,4
Лекции	57	15	36
<i>в том числе в форме практической подготовки</i>	–	–	–
Практические занятия (ПЗ)	72	30	36
<i>в том числе в форме практической подготовки</i>	72	30	36
Консультации текущие	2,55	0,75	1,8
Консультации перед экзаменом	1,4	–	1,4
<i>Виды аттестации – зачет, экзамен</i>	0,3	0,1	0,2
Самостоятельная работа	94,75	26,15	68,6
Проработка материалов по конспекту лекций	15,75	5,15	10,6
Проработка материалов по учебникам, учебным пособиям	23	5	18
Доклад	8	8	–
Домашнее задание	8	8	–
Курсовая работа	40	–	40
Подготовка к экзамену (контроль)	33,8	–	33,8

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание раздела (указывается в дидактических единицах)	Трудоемкость раздела, час
1	Правовые и организационные вопросы технической защиты информации ограниченного доступа	Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих. Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.	33,15
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования,	32

		<p>функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем. Защита информации в ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.</p>	
3	<p>Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных</p>	<p>Особенности информационного элемента информационной системы персональных данных. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам. Основные принципы обеспечения безопасности персональных данных при их обработке. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий.</p>	33
4	<p>Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных</p>	<p>Классификация информационных систем персональных данных. Состав мер по обеспечению безопасности персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных. Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Обязанности оператора, осуществляющего обработку персональных данных.</p>	70,6
5	<p>Практические реализации типовых моделей защищенных информационных систем обработки персональных данных</p>	<p>Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных. Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации. Виды, формы и способы контроля защиты персональных данных в ин-</p>	55

	формационных системах персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.	
--	--	--

5.2 Разделы дисциплины (модуля) и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СР, час
1	Правовые и организационные вопросы технической защиты информации ограниченного доступа.	8	12	13,15
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	7	18	7
3	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	15	12	6
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	17	18	35,6
5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	10	12	33

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Правовые и организационные вопросы технической защиты информации ограниченного доступа.	Основные понятия в области технической защиты информации (ТЗИ). Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.	4
		Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.	2
		Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных.	2
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации.	2
		Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации.	3
3	Угрозы безопасности персональных данных при их обработке в информационных сис-	Особенности информационного элемента информационной системы персональных данных. Угрозы утечки информации по техническим каналам.	2
		Основные типы актуальных угроз безопасности персо-	2

	темах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	нальных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных.	
		Угрозы утечки информации по техническим каналам.	2
		Основные принципы обеспечения безопасности персональных данных при их обработке.	4
		Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	2
		Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных.	3
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Классификация информационных систем персональных данных.	2
		Состав мер по обеспечению безопасности персональных данных.	4
		Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе.	
		Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.	4
		Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.	2
		Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Обязанности оператора, осуществляющего обработку персональных данных.	3
5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации.	2
		Основное содержание этапов организации обеспечения безопасности персональных данных.	2
		Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.	2
		Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных.	2

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Правовые и организационные вопросы технической защиты информации ограниченного доступа.	Анализ Стратегии национальной безопасности Российской Федерации до 2020 года и Доктрины информационной безопасности Российской Федерации. Концептуальные основы ТЗИ.	4
		Анализ классификационной схемы угроз безопасности информации и их общая характеристика.	4

		Анализ особенностей проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации и методов оценки опасности угроз.	4
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Разработка типовых документов, содержащих классификационную схему угроз безопасности информации при организации обработки персональных данных.	4
		Разработка типовых документов, содержащих информацию о Классификации и категорировании объектов информатизации.	6
		Разработка типовых документов, содержащих общую и частную модели нарушителя.	4
		Анализ типовых моделей нарушителя безопасности информации	4
3	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	Анализ общего порядка организации обеспечения безопасности персональных данных в информационных системах персональных данных.	4
		Анализ категорирования персональных данных обрабатываемых в информационных системах	2
		Разработка документа, содержащего концепцию защиты персональных данных.	4
		Разработка документа, содержащего облик системы защиты персональных данных и ее внедрение	2
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Анализ порядка классификации информационных систем персональных данных	2
		Анализ организационных и технических мероприятий по защите персональных данных в информационных системах	2
		Анализ содержания мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных	4
		Разработка перечня анализ содержания основных этапов при организации работ по обеспечению безопасности персональных данных руководителя организации	2
		Разработка перечня анализ содержания основных этапов при организации работ по обеспечению безопасности персональных данных ответственного за обработку персональных данных	2
		Разработка перечня анализ содержания основных этапов при организации работ по обеспечению безопасности персональных данных ответственного за защиту персональных данных	4
		Анализ порядка разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных	4
5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	Анализ типовых комплексных организационных и технических мероприятий, применяемых для защиты персональных данных	4
		Разработка программы и методики аттестационных испытаний информационных систем персональных данных.	2
		Анализ методов обеспечения эффективности защиты персональных данных в ходе эксплуатации ин-	4

	формационной системы	
	Разработка документов, отражающих вопросы управления системой регистрации и учета информационной системы персональных данных	2
	Итого	72

5.2.4 Самостоятельная работа студентов (СРС)

№ п/п	Наименование раздела дисциплины	Тематика самостоятельной работы	Трудоемкость, час
1	Правовые и организационные вопросы технической защиты информации ограниченного доступа	Проработка материалов по конспекту лекций	2,15
		Проработка материалов по учебникам, учебным пособиям	3
		Доклад по теме «Система документов по защите персональных данных в Российской Федерации».	8
2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	1
		Домашнее задание	4
3	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	Проработка материалов по конспекту лекций	1
		Проработка материалов по учебникам, учебным пособиям	1
		Домашнее задание	4
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Проработка материалов по конспекту лекций	5,6
		Проработка материалов по учебникам, учебным пособиям	10
		Курсовая работа	20
5	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	Проработка материалов по конспекту лекций	5
		Проработка материалов по учебникам, учебным пособиям	8
		Курсовая работа	20

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. М. Ю. Рытов, В. И. Аверченков, Т. Р. Гайнулин, Защита персональных данных в организации, 2016 г. 124 стр.
2. Сабанов А.Г., Зыков В.Д., Мещеряков Р.В., Рылов С.П., Шелупанов А.А., Защита персональных данных в организациях здравоохранения, 2014 г. 206 стр.
3. Борисов М., Особенности защиты персональных данных в трудовых отношениях, 2018 г. – 224 стр.

6.2. Дополнительная литература

1. А.И. Савельев, Научно-практический постатейный комментарий к Федеральному закону «О персональных данных», 2017 г. – 470 стр. Книга для изучения вопроса с юридической стороны.
2. А. С. Дупан (Гутникова), Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет, 2016 г. – 440 стр.
3. Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. М.: МО РФ, 2016.

4. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Щербаков А.Ю.Издательство: Книжный мир, 2016 г. <http://www.knigafund.ru/books/88712>

5. Служба защиты информации: организация и управление: учебное пособие для вузов: Аверченков В.И., Рытов М.Ю.Издательство: Флинта, 2014 г. <http://www.knigafund.ru/books/116368>

6.3 Методические указания для обучающихся по освоению дисциплины (модуля)

Безопасность персональных данных [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, В.А. Хвостов; ВГУИТ, Кафедра информационной безопасности. - Воронеж: ВГУИТ, 2016. - 37 с.

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» федеральный портал	https://www.edu.ru/
Научная электронная библиотека	https://elibrary.ru/defaultx.asp
Национальная исследовательская компьютерная сеть России	https://niks.su/
Информационная система «Единое окно доступа к образовательным ресурсам»	http://window.edu.ru/
Электронная библиотека ВГУИТ	http://biblos.vsu.ru/megapro/web
Сайт Министерства науки и высшего образования РФ	https://minobrnauki.gov.ru/
Портал открытого on-line образования	https://npoed.ru/
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	https://education.vsu.ru/

6.5 Методические указания для обучающихся по освоению дисциплины (модуля)

Безопасность персональных данных [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, В.А. Хвостов; ВГУИТ, Кафедра информационной безопасности. Воронеж: ВГУИТ, 2016. 37 с.

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

MicrosoftOffice, Страж-NT, BackTrackLinux, Avast; локальная сеть университета и глобальная сеть Internet.

7 Материально-техническое обеспечение дисциплины (модуля)

При чтении лекций используется мультимедийное оборудование (проектор) кафедры информационной безопасности (а. 420).

Для проведения лабораторного практикума, а также для проведения обучения и контроля знаний обучающихся на едином портале интернет-

тестирования, для выполнения расчетных работ кафедры информационной безопасности обладает специализированными аудиториями (а. 332а, 420, 424), оснащенными в каждой аудитории 12 ПК IntelCore 2 Duo, сетью Интернет.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 Оценочные материалы (ОМ) для дисциплины включают:
перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
 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;
методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины.**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Безопасность персональных данных

(специализация «Информационные системы» в соответствии с учебным планом)

1 Требования к результатам освоения дисциплины

п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
	ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области	Основные средства и системы защиты информации, используемые при защите персональных данных. Основные угрозы безопасности персональных данных. Научные и организационные основы защиты информации в информационных системах персональных данных.	Анализировать программные, архитектурно-технические и схемотехнические решения компонентов информационных систем персональных данных с целью разработки модели угроз.	Навыками разработки технического задания на разработку системы защиты винформационной системы персональных данных.
	ПК-21	Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Информационную систему персональных данных как объект реализации угроз информационной безопасности, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; методы, способы, средства, последовательность и содержание этапов разработки информационных систем персональных данных и подсистем защиты	Проводить классификацию информационных систем персональных данных.	Навыками выбора организационных и технических мероприятий по защите информации персональных данных.
	ПСК-4.4	Способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	Методологии и методы проектирования систем защиты персональных данных	Разрабатывать техническое задание на разработку системы защиты персональных данных.	Навыками контроля защищенности персональных данных в информационных системах при эксплуатации.

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
1	<p>Правовые и организационные вопросы технической защиты информации ограниченного доступа.</p> <p>Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа</p>	ОК-5	Зачет с оценкой	Уровневая шкала
			Контрольные вопросы к текущим опросам на практических работах	Уровневая шкала
			Домашнее задание	Уровневая шкала
2	<p>Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных</p> <p>Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных</p>	ПК-21	Зачет с оценкой	Уровневая шкала
			Контрольные вопросы к текущим опросам на практических работах	Уровневая шкала
			Домашнее задание	Уровневая шкала
			Доклад	Уровневая шкала
3	Практические реализации	ПСК-4.4	Зачет с оценкой	Уровневая

типовых моделей защищенных информационных систем обработки персональных данных			шкала
	Контрольные вопросы к текущим опросам на лабораторных работах		Уровневая шкала
	Домашнее задание		Уровневая шкала
	Доклад		Уровневая шкала

3 Оценочные средства для промежуточной аттестации

3.1 Вопросы к зачету

ОК-5 - Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области.

1	Что такое защита информации?
2	Что является основным содержанием защиты информации?
3	Что такое защищаемая информация?
4	Что такое угроза безопасности информации?
5	Что такое естественная угроза безопасности информации?
6	Что такое искусственная угроза безопасности информации?
7	Какое отличие между непреднамеренными и преднамеренными угрозами безопасности информации?
8	Какие основные виды преднамеренных угроз безопасности информации?
9	Какими основными законами Российской Федерации регламентирована защита персональных данных в организациях различной ведомственной принадлежности?
10	Какие основные категории персональных данных, обрабатываемых в информационных системах?
11	Какие объекты из состава информационных систем в учреждении требуют реализации организационных и технических мероприятий по защите персональных данных?
12	Какая информация о пациенте должна быть отнесена к категории персональные данные?
13	Какая информация о сотрудниках должна быть отнесена к категории персональные данные?
14	Какая технологическая информация об информационных системах должна быть отнесена к категории персональные данные?
15	Какие данные требуют выполнения ряда мероприятий по защите информации в организации кроме персональных данных?

ПК-21 - Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем

16	Что является информационным основанием функционирования организации различной ведомственной принадлежности?
17	Какой состав программного обеспечения типовой информационной системы?
18	Какой состав аппаратного обеспечения типовой информационной системы?
19	Какими особенностями функционирования обладают информационные системы с точки зрения решения задачи обеспечения защиты персональных данных?
20	Основные способы защиты информации при обработке персональных данных в информационных системах.
21	Основные средства защиты информации при обработке персональных данных в информационных системах.
22	Состав и основные функции систем защиты информации уровня отдельных ЭВМ.
23	Какие основные принципы построения и эксплуатации систем защиты информации?
24	Назовите основные типы систем защиты информации, используемые для защиты персональных данных в информационных системах?
25	Какими защитными функциями обеспечения безопасности информации наиболее распространенных операционных систем можно воспользоваться при построении защиты персональных данных?
26	Какой главный недостаток защитных функций обеспечения безопасности информации наиболее распространенных операционных систем с точки зрения защиты персональных данных?
27	Назовите основные защитные функции, реализуемые операционной системой WINDOWS XP.
28	Назовите основные защитные функции, реализуемые операционной системой LINUX.

29	Какой состав системы защиты информации уровня отдельной ЭВМ?
30	Назовите назначение подсистемы управления доступом системы защиты информации уровня отдельного ЭВМ.
31	Назовите назначение подсистемы регистрации и учета системы защиты информации уровня отдельного ЭВМ.
32	Назовите назначение криптографической подсистемы системы защиты информации уровня отдельного ЭВМ.
33	Назовите назначение подсистемы контроля целостности системы защиты информации уровня отдельного ЭВМ.
34	Назовите назначение межсетевое экрана.

ПСК-4.4 Способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы.

35	Какие параметры могут использоваться в качестве критериев анализа межсетевых экранов.
36	Назовите назначение системы обнаружения вторжений.
37	Назовите назначение средств построения виртуальных частных сетей.
38	Назовите назначение средств централизованного управления информационной безопасностью.
39	Назовите назначение средств анализа защищенности информационных систем.
40	Какие основные этапы и их содержание выполняемых действий руководителем учреждения при организации защиты персональных данных?
41	Какие основные этапы и их содержание выполняемых действий ответственным за обработку персональных данных сотрудником при организации защиты персональных данных?
42	Какие основные этапы и их содержание выполняемых действий ответственным за защиту персональных данных сотрудником при организации защиты?
43	Какие основные признаки классификации информационных систем при организации защиты персональных данных?
44	Какая последовательность действий при проведении классификации информационных систем?
45	Какие основные классы конфиденциальности информационных систем существуют?
46	Что такое акт классификации информационной системы?
47	Что такое политики безопасности персональных данных?
48	Что такое модель угроз безопасности персональных данных?
51	Что такое сертификат ФСТЭК России на устанавливаемые системы защиты?
52	Назовите основное содержание проверки эффективности мероприятий по защите персональных данных?
53	На какие виды деятельности должна иметь лицензию организация, привлекаемая для проверки эффективности мероприятий по защите персональных данных?
54	В чем заключается процесс аттестации информационной системы?
55	Какие основные документы содержат основные результаты и выводы аттестационных испытаний информационной системы?
56	Какой срок действия Аттестата соответствия?
57	Каково содержание основных действий при эксплуатации аттестованной информационной системы?
58	В чем заключается управление подсистемой управления доступом?
59	В чем заключается управление подсистемой контроля целостности?
60	В чем заключается управление криптографической подсистемой?
61	В чем заключается управление подсистемой регистрации и учета?

3.2 Задания к практическим работам

ОК-5 - Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области.

№ задания	Условие задачи (формулировка задания)
1	Стратегии национальной безопасности Российской Федерации до 2020 года и Доктрины информационной безопасности Российской Федерации. Концептуальные основы ТЗИ.
2	Общая характеристика классификационной схемы угроз безопасности информации. Последовательность этапов реализации. Применяемые программные и аппаратные средства реализации несанкционированного доступа.
3	Методы оценки опасности угроз информационной безопасности и проведение комплексного исследования объектов информатизации. Программные средства сканирования уязвимостей сети.
4	Типовые документы, содержащие Классификационную схему угроз безопасности информации при организации обработки персональных данных.
5	Типовые документы, содержащие информацию о Классификации и категорировании объектов информатизации.
6	Общая и частная модели нарушителя. Методы разработки частной модели нарушителя.
7	Оценка возможностей различных нарушителей реализовать угрозы информационной безопасности.

ПК-21 - Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.

8	Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных
9	Порядок категорирования персональных данных обрабатываемых в информационных системах
10	Порядок разработки и содержание документа, содержащего концепцию защиты персональных данных
11	Порядок разработки и содержание документа, содержащего облик системы защиты персональных данных. Порядок внедрения системы защиты персональных данных
12	Классификация информационных систем персональных данных по исходным данным: Вариант 1 Количество субъектов персональных данных менее 1000, персональные данные категории 1. Вариант 2 Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 1. Вариант 3 Количество субъектов персональных данных более 100000, персональные данные категории 1. Вариант 4 Количество субъектов персональных данных менее 1000, персональные данные категории 2. Вариант 5 Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 2. Вариант 6 Количество субъектов персональных данных более 100000, персональные данные категории 2. Вариант 1 Количество субъектов персональных данных менее 1000, персональные данные категории 3. Вариант 2 Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 3. Вариант 3 Количество субъектов персональных данных более 100000, персональные данные категории 3. Вариант 1 Количество субъектов персональных данных менее 1000, персональные данные

	категории 4. Вариант 2 Количество субъектов персональных данных от 1000 до 100000, персональные данные категории 4. Вариант 3 Количество субъектов персональных данных более 100000, персональные данные категории 4.
13	Разработка перечня организационных и технических мероприятий по защите персональных данных в информационных системах
14	Оценка и обсуждение содержания мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных
15	Содержание основных этапов организации работ по защите персональных данных руководителя организации
16	Содержание основных этапов организации работ по защите персональных данных ответственного за их обработку
17	Содержание основных этапов организации работ по защите персональных данных ответственного за их защиту
18	Разработка внутренних нормативных документов и актов ненормативного характера по обработке персональных данных

ПСК-4.4 Способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы..

19	Типовые комплексы организационных и технических мероприятий, применяемых для защиты персональных данных
20	Разработка программы и методики аттестационных испытаний информационной системы персональных данных
21	Методы аудита информационной безопасности персональных данных изучение сканера безопасности
22	Разработка документов регламентирующих вопросы управления системой регистрации и учета информационной системы персональных данных

3.3. Тематика докладов и презентаций

ОК-5 - Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области.

№ задания	Тема доклада
1	Система документов по защите персональных данных в Российской Федерации

3.4 Домашнее задание №1

ПК-15 Способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.

№ задания	Формулировка задания
1	Угрозы безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

3.5. Домашнее задание №2

ПК-19 Способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности.

№ задания	Формулировка задания
2	Результаты разработки комплекта эксплуатационных документов по защите персональных данных в организациях.

Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
<p>ЗНАТЬ Основные средства и системы защиты информации, используемые при защите персональных данных. Основные угрозы безопасности персональных данных. Научные и организационные основы защиты информации в информационных системах персональных данных. Информационную систему персональных данных как объект реализации угроз информационной безопасности, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; методы, способы, средства, последовательность и содержание этапов разработки информационных систем персональных данных и подсистем защиты. Методологии и методы проектирования систем защиты персональных данных.</p>	Зачет с оценкой	Уровень владения материалом	ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена
			ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена
			ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
<p>УМЕТЬ Анализировать программные, архитектурно-технические и схемотехнические решения компонентов информационных систем персональных данных с целью разработки модели угроз. Проводить классификацию</p>	Задания к практическим работам	Уровень умения	студент выполнил задание и допустил не более 1 ошибки	Отлично	Освоена
			студент выполнил задание и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			студент выполнил задание не полностью	Удовлетворительно	Освоена

информационных систем персональных данных. Разрабатывать техническое задание на разработку системы защиты персональных данных			студент не выполнил задание	Неудовлетворительно	Не освоена
ВЛАДЕТЬ Навыками разработки технического задания на разработку системы защиты в информационных системах персональных данных. Навыками выбора организационных и технических мероприятий по защите информации персональных данных. Навыками контроля защищенности персональных данных в информационных системах при эксплуатации.	Доклад	Уровень владения	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена
	Домашнее задание	Уровень владения	выставляется студенту при наличии полного комплекта разработанной документации	Зачтено	Освоена
			выставляется студенту при отсутствии 50% и более предлагаемого комплекта документации	Не зачтено	Не освоена