

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«**Российский государственный гуманитарный университет**»  
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ  
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ  
Кафедра информационной безопасности

## **ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**10.03.01 Информационная безопасность**

*Код и наименование направления подготовки/специальности*

**«Организация и технология защиты информации  
(по отрасли или в сфере профессиональной деятельности)»**

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2024

**ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**  
Рабочая программа дисциплины

Составитель:

к.и.н., доцент, заведующая кафедрой ИБ Г.А. Шевцова

Ответственный редактор

к.и.н., доцент, заведующая кафедрой ИБ Г.А. Шевцова

**УТВЕРЖДЕНО**

Протокол заседания кафедры  
Информационной безопасности  
№ 11 от 18.03.2024

## ОГЛАВЛЕНИЕ

1. Пояснительная записка .....	4
1.1. Цель и задачи дисциплины .....	4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций .....	4
1.3. Место дисциплины в структуре образовательной программы .....	6
2. Структура дисциплины .....	6
3. Содержание дисциплины .....	7
4. Образовательные технологии .....	8
5. Оценка планируемых результатов обучения .....	9
5.1 Система оценивания .....	9
5.2 Критерии выставления оценки по дисциплине .....	9
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине .....	10
6. Учебно-методическое и информационное обеспечение дисциплины .....	13
6.1 Список источников и литературы .....	13
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ....	15
6.3 Профессиональные базы данных и информационно-справочные системы .....	16
7. Материально-техническое обеспечение дисциплины .....	16
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов .....	16
9. Методические материалы .....	17
9.1 Планы практических занятий .....	17
Приложение 1. Аннотация рабочей программы дисциплины .....	20

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины – формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Задачи дисциплины:

- овладеть теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- изучить методы защиты персональных данных;
- изучить процесс работы с персональными данными в организации;
- научить разработке документов, регламентирующих работу с персональными данными в организации.

### 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	Знать: базовые международные и российские регуляторы по информационной безопасности
	ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Уметь: работать со стандартами и нормативными документами
	ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации	Владеть: навыками использования международных и национальных стандартов в своей профессиональной деятельности
ПК-10 Способен проводить анализ информационной	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные	Знать: нормативные правовые акты в области защиты ПДн,

безопасности объектов и систем на соответствие требованиям стандартам в области информационной безопасности	и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	национальные, межгосударственные и международные стандарты в области защиты ПДн; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите ПДн;
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки ПДн, установленных на объектах информатизации;
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	Владеть: навыком разработки аналитического обоснования необходимости создания системы защиты ПДн в организации;
ПК-11 Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищённости информационной безопасности объектов и систем	Знать: методики проведения теоретических исследований уровней защищённости ИСПДн;
	ПК-11.2 Умеет составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости на основании аналитического отчёта	Уметь: составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости ИСПДн на основании аналитического отчёта;
	ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости	Владеть: навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости.
ПК-15 Способен организовывать технологический процесс защиты информации ограниченного доступа	ПК-15.1 Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим	Знать: особенности практической деятельности организации и специфика защиты объекта

в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	нормативными и методическими документами	
	ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке	Уметь: осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
	ПК-15.3 Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации	Владеть: способностью Организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными и методическими документами ФСТЭК и ФСБ

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Организация и технологии защиты персональных данных» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Правовое и организационное обеспечение информационной безопасности», «Защита и обработка конфиденциальных документов», «Информационные процессы и системы».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексная защита объектов информатизации», «Аудит информационной безопасности», «Эксплуатационная практика»

## 2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часов.

### Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
5	Лекции	32
5	Практические работы	40
Всего:		72

Объем дисциплины в форме самостоятельной работы обучающихся составляет 72 академических часов.

### **3. Содержание дисциплины**

#### ***Тема 1. Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора***

Анализ международного и Российского законодательства по вопросам обработки ПДн и обеспечения безопасности ПДн. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Права субъекта персональных данных, обязанности оператора.

#### ***Тема 2. Особенности обработки персональных данных без использования средств автоматизации***

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Постановление Правительства РФ от 15.09.2008 № 687.

#### ***Тема 3. Основные этапы обработки и защиты персональных данных***

Состав мероприятий по приведению информационных систем и процессов обработки персональных данных в соответствие с требованиями законодательства о персональных данных. Постановление правительства РФ от 01.11.2012 г. № 1119.

#### ***Тема 4. Анализ объекта информатизации. Составление модели угроз***

Технологическая стадия предпроектного обследования. Составление перечня ПДн, перечня сотрудников, работающих с ПДн. Описание ИСПДн. Выявление угроз безопасности персональных данных при их обработке в ИСПДн. Разработка частной модели угроз безопасности ПДн. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн. Определение актуальности угроз в соответствии с методическими документами ФСТЭК России. Разработка модели нарушителя.

#### ***Тема 5. Техническое задание на систему защиты ПДн***

Составление частного технического задания на разработку системы защиты персональных данных. Обоснование разработки системы защиты ПДн. Требования методических документов ФСТЭК и ФСБ России к составу и содержанию организационных и технических мер по обеспечению безопасности ПДн. Приказ ФСТЭК России от 18.02.2013 г. № 21, Приказ ФСБ России от 10.07.2014 г. № 378. Правила мандатного доступа. Особенности реализации мандатного доступа в реляционных СУБД.

#### ***Тема 6. Стадия проектирования. Требования методических документов***

Организация и технология разработки системы защиты ПДн. Выбор средств защиты информации. Программно-технические комплексы защиты информации от несанкционированного доступа. Технические средства перекрытия технических каналов утечки информации. Организационные мероприятия.

#### ***Тема 7. Технология ввода в действие и эксплуатации СЗПДн***

Этап внедрения. Обучение персонала. Установка, настройка, учёт и контроль СЗИ. Описание системы защиты персональных данных. Проверка эффективности СЗПДн.

#### ***Тема 8. Особенности защиты персональных данных при их обработке в государственных информационных системах***

Особенности защиты персональных данных при их обработке в государственных информационных системах. Постановление Правительства РФ от 21.03.2012 г. № 211 (с изм.). Обезличивание персональных данных при их обработке в ГИС. Аттестация ГИС.

#### ***Тема 9. Контроль в области защиты персональных данных***

Регуляторы в области защиты персональных данных. Проверки Роскомнадзора. Проверки ФСБ России. Проверка ФСТЭК России.

#### 4. Образовательные технологии

№ п/п	Наименование темы	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора	Лекция 1 Практическая работа 1 Самостоятельная работа	Традиционная, Опрос Защита ПР Изучение лекционного материала и источников
2.	Особенности обработки персональных данных без использования средств автоматизации	Лекция 2 Практическая работа 2 Самостоятельная работа	Традиционная, Опрос Защита ПР Изучение лекционного материала и источников
3.	Основные этапы обработки и защиты персональных данных	Лекция 3 Практическая работа 3 Самостоятельная работа	Традиционная, Опрос Защита ПР Изучение лекционного материала и источников
4.	Анализ объекта информатизации. Составление модели угроз	Лекция 4.1 Лекция 4.2 Практическая работа 4 Самостоятельная работа	Традиционная, Опрос Традиционная, Опрос Защита ПР Изучение лекционного материала и источников
5.	Техническое задание на систему защиты ПДн	Лекция 5 Практическая работа 5 Самостоятельная работа	Традиционная, Опрос Защита ПР Изучение лекционного материала и источников
6.	Стадия проектирования. Требования методических документов	Лекция 6.1 Лекция 6.2 Самостоятельная работа	Традиционная, Опрос Традиционная, Опрос Изучение лекционного материала и источников
7.	Технология ввода в действие и эксплуатации СЗПДн.	Лекция 7.1 Лекция 7.2 Самостоятельная работа	Традиционная, Опрос Традиционная, Опрос Изучение лекционного материала и источников
8.	Особенности защиты персональных данных при их обработке в государственных	Лекция 8 Самостоятельная работа	Традиционная, Опрос Изучение лекционного материала



	информационных системах.		и источников
9.	Регуляторы в области защиты персональных данных. Проверки Роскомнадзора. Проверки ФСБ. Проверка ФСТЭК.	Лекция 9.1 Лекция 9.2  Самостоятельная работа	Традиционная, Опрос Традиционная, Опрос  Изучение лекционного материала и источников

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

## 5. Оценка планируемых результатов обучения

### 5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос	2 балла	10 баллов
- практические задания 1-5	10 баллов	50 баллов
Промежуточная аттестация – зачет с оценкой (вопросы по билетам)		40 баллов
<b>Итого за семестр</b>		<b>100 баллов</b>

### 5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	отлично	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво- рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет- ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

### 5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

#### *Устный опрос*

**Устный опрос** – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

#### *Перечень устных вопросов для проверки знаний*

№	Вопрос	Реализуемая компетенция
1.	Что относится к персональным данным?	ПК-5, ПК-10, ПК-11, ПК-15
2.	Назовите причины актуальности проблемы защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
3.	Перечислите основные международные документы в области защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15

4.	Какие права должны быть предоставлены всем лицам по отношению к персональным данным?	ПК-5, ПК-10, ПК-11, ПК-15
5.	Как осуществляется трансграничная передача персональных данных в соответствии с Конвенцией?	ПК-5, ПК-10, ПК-11, ПК-15
6.	В каких случаях участники Конвенции вправе отступить от основных положений трансграничной передачи персональных данных?	ПК-5, ПК-10, ПК-11, ПК-15
7.	Каким образом взаимодействуют между собой регуляторы в области персональных данных различных участников Конвенции?	ПК-5, ПК-10, ПК-11, ПК-15
8.	Какие реквизиты должно содержать ходатайство о помощи, подаваемое лицом, проживающим за границей, на защиту своих прав?	ПК-5, ПК-10, ПК-11, ПК-15
9.	В каких случаях возможна обработка особой категории данных?	ПК-5, ПК-10, ПК-11, ПК-15
10.	Какие данные предоставляются субъекту персональных данных контролёром?	ПК-5, ПК-10, ПК-11, ПК-15
11.	В каких случаях государства-участники могут принимать законодательные меры для ограничения сферы обязательств и прав субъекта данных?	ПК-5, ПК-10, ПК-11, ПК-15
12.	В чем выражается право субъекта данных на возражение?	ПК-5, ПК-10, ПК-11, ПК-15
13.	В чем должна заключаться конфиденциальность и безопасность обработки персональных данных?	ПК-5, ПК-10, ПК-11, ПК-15
14.	Перечислите постановления Правительства РФ, регламентирующие вопросы защиты персональных данных при их автоматизированной обработке в информационных системах.	ПК-5, ПК-10, ПК-11, ПК-15
15.	Назовите признаки информационной системы, обрабатывающей специальные категории персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
16.	Назовите признаки информационной системы, обрабатывающей биометрические персональные данные.	ПК-5, ПК-5, ПК-10, ПК-11, ПК-15
17.	Назовите признаки информационной системы, обрабатывающей общедоступные персональные данные.	ПК-5, ПК-10, ПК-11, ПК-15
18.	Что понимается под актуальными угрозами безопасности персональных данных?	ПК-5, ПК-10, ПК-11, ПК-15
19.	В каком случае для информационной системы актуальны угрозы 1-го, 2-го, 3-го типа?	ПК-5, ПК-10, ПК-11, ПК-15
20.	Кем производится определение типа угроз безопасности персональных данных, актуальных для информационной системы?	ПК-5, ПК-10, ПК-11, ПК-15
21.	Сколько устанавливается уровней защищённости персональных данных?	ПК-5, ПК-10, ПК-11, ПК-15
22.	Поясните порядок определения уровней защищённости персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
23.	Перечислите требования, которые должны быть выполнены для обеспечения каждого уровня защищённости персональных данных при их обработке в информационных системах.	ПК-5, ПК-10, ПК-11, ПК-15
24.	Каковы особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации?	ПК-5, ПК-10, ПК-11, ПК-15
25.	Перечислите меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.	ПК-5, ПК-10, ПК-11, ПК-15

26.	Перечислите требования к материальным носителям биометрических персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
27.	Перечислите постановления Правительства РФ, регламентирующие вопросы защиты персональных данных при их автоматизированной обработке в информационных системах.	ПК-5, ПК-10, ПК-11, ПК-15
28.	Назовите признаки информационной системы, обрабатывающей специальные категории персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
29.	Назовите признаки информационной системы, обрабатывающей биометрические персональные данные.	ПК-5, ПК-10, ПК-11, ПК-15
30.	Назовите признаки информационной системы, обрабатывающей общедоступные персональные данные.	ПК-5, ПК-10, ПК-11, ПК-15
31.	Какие основные положения определяет Федеральный Закон «О персональных данных»?	ПК-5, ПК-10, ПК-11, ПК-15
32.	Какие органы государственной власти уполномочены осуществлять мероприятия по контролю и надзору в отношении соблюдения требований Федерального закона «О персональных данных»?	ПК-5, ПК-10, ПК-11, ПК-15
33.	Поясните основные принципы обработки персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
34.	Перечислите основные условия обработки персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
35.	Какие категории персональных данных выделяются законом «О персональных данных»?	ПК-5, ПК-10, ПК-11, ПК-15
36.	В каких случаях допускается обработка специальных категорий персональных данных?	ПК-5, ПК-10, ПК-11, ПК-15
37.	Поясните основные права субъекта персональных данных.	ПК-5, ПК-10, ПК-11, ПК-15
38.	В каких случаях права субъекта персональных данных могут быть ограничены?	ПК-5, ПК-10, ПК-11, ПК-15
39.	Каковы основные обязанности оператора персональных данных?	ПК-5, ПК-10, ПК-11, ПК-15
40.	В каких случаях оператор не обязан уведомлять Роскомнадзор об обработке ПДн?	ПК-5, ПК-10, ПК-11, ПК-15
41.	В каких случаях случаи не требуется согласие субъекта ПДн на обработку сведений о нем?	ПК-5, ПК-10, ПК-11, ПК-15

***Промежуточная аттестация (примерные вопросы к зачету с оценкой)***

№	Вопрос	Реализуемая компетенция
1.	Актуальность проблемы защиты персональных данных в информационных системах	ПК-5, ПК-10, ПК-11, ПК-15
2.	Основные понятия информационной безопасности согласно ФЗ «Об информации, информационных технологиях и о защите информации»	ПК-5, ПК-10, ПК-11, ПК-15
3.	Международное и национальное право в области защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
4.	Федеральное законодательство Российской Федерации в области защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
5.	Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»	ПК-5, ПК-10, ПК-11, ПК-15
6.	Специальные нормативные документы по технической защите сведений конфиденциального характера	ПК-5, ПК-10, ПК-11, ПК-15

7.	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах. Наиболее часто реализуемые угрозы	ПК-5, ПК-10, ПК-11, ПК-15
8.	Методология формирования модели угроз с использованием Методических рекомендаций ФСБ России	ПК-5, ПК-10, ПК-11, ПК-15
9.	Порядок организации защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
10.	Меры по обеспечению безопасности персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
11.	Построение системы защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
12.	Подсистемы в составе СЗПДн	ПК-5, ПК-10, ПК-11, ПК-15
13.	Аттестация, сертификация и лицензирование в области защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15
14.	Контроль в области защиты персональных данных	ПК-5, ПК-10, ПК-11, ПК-15

**Примерные тестовые задания – проверка сформированности компетенций – ПК-5, ПК-10, ПК-11, ПК-15**

**1) Выберите регуляторов в области защиты персональных данных**

- а) ФСБ России  
 б) МВД России  
 в) Роскомнадзор  
 д) ФСТЭК России  
 е) ФСО России

**6. Учебно-методическое и информационное обеспечение дисциплины**

**6.1 Список источников и литературы**

Источники  
 Основные

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
3. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ [Электронный ресурс] . – URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=469771&dst=100635&cacheid=9F9E668C665FEBA35D8C4E693F675FCF&mode=splus&rnd=0.9404609152849899#3z92p8UcwwHttiG21> — Режим доступа: свободный
4. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
5. Указ Президента Российской Федерации от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
6. Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.

7. Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-ПП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
8. Постановление Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
9. Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
10. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
11. Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» // [Электронный ресурс] . – URL: <http://www.consultant.ru> — Режим доступа: свободный.
12. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
13. Постановление Правительства РФ от 04.03.2010 г. № 125 "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию"// [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
14. Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
15. Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации. Положение ПКЗ 2005)» // [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
16. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»// [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
17. Приказ Минкомвязи России от 20.07.2017 г. № 373 "О признании утратившими силу приказов Министерства связи и массовых коммуникаций РФ" от 21 декабря 2011 №346, от 28 августа 2015 №315 и п.9 приказа Министерства связи и массовых коммуникаций РФ от 24 ноября 2014 №403// [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.

18. Приказ Роскомнадзора от 30.05.2017 г. № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения"// [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
19. Приказ Роскомнадзора от 30.10. 2018 г. № 159 "О внесении изменений в Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 года № 94"// [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
20. Постановление Правительства Российской Федерации от 13.02.2019 № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных" [Электронный ресурс] . – URL: <http://www.consultant.ru>— Режим доступа: свободный.
21. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год [Электронный ресурс] . – URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114spetsialnye-normativnye-dokumenty/379bazovaya-model-ugroz-bezopasnosti-perso-nalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii2008god> — Режим доступа: свободный.
22. Приказ ФСБ России от 10.07.2014 г. № 378. "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости"— URL: <http://www.consultant.ru> — Режим доступа: свободный.

## Литература

### Основная

1. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 108 с. — ISBN 978-5-8114-8370-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/175506>— Режим доступа: для авториз. пользователей.
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1843022>. – Режим доступа: по подписке.

### Дополнительная

3. Лагоша, О. Н. Сертификация информационных систем : учебное пособие / О. Н. Лагоша. — Санкт-Петербург : Лань, 2020. — 112 с. — ISBN 978-5-8114-4668-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/139268> (дата обращения: 01.04.2023). -- Режим доступа: для авториз. пользователей.

## 6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

4. [www.gpntb.ru/](http://www.gpntb.ru/) Государственная публичная научно-техническая библиотека.
5. [www.nlr.ru/](http://www.nlr.ru/) Российская национальная библиотека.
6. [www.nns.ru/](http://www.nns.ru/) Национальная электронная библиотека.
7. [ww.rsl.ru/](http://ww.rsl.ru/) Российская государственная библиотека.
8. [www.microinform.ru/](http://www.microinform.ru/) Учебный центр компьютерных технологий «Микроинформ».

9. [www.intuit.ru/](http://www.intuit.ru/) Образовательный сайт.
10. [www.window.edu.ru/](http://www.window.edu.ru/) Библиотека учебной и методической литературы.
11. [www.osp.ru/](http://www.osp.ru/) Журнал «Открытые системы».
12. [www.ihitika.lib.ru/](http://www.ihitika.lib.ru/) Библиотека учебной и методической литературы.

Национальная электронная библиотека (НЭБ) [www.rusneb.ru](http://www.rusneb.ru)  
 ELibrary.ru Научная электронная библиотека [www.elibrary.ru](http://www.elibrary.ru)  
 Электронная библиотека Grebennikon.ru [www.grebennikon.ru](http://www.grebennikon.ru)

### **6.3 Профессиональные базы данных и информационно-справочные системы**

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

## **7. Материально-техническое обеспечение дисциплины**

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

- 1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity

- 2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. MicrosoftOffice
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. КонсультантПлюс

## **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости



предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA SE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBrailleViewPlus;

- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1 Планы практических занятий**

**Темы** учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем,

ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

**Целью** практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

**Тематика** практических занятий соответствует программе дисциплины.

### ***Практическое занятие 1 (4 ч.) – Изучение нормативных документов по ПДн***

Задания:

1. С использованием программы КонсультантПлюс осуществить поиск нормативных документов по вопросам защиты персональных данных.
2. В отчёте привести краткое описание положений каждого нормативного документа.
3. Привести основные определения ФЗ-152.
4. Оформить отчёт по практической работе и защитить работу

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Ответить на теоретические вопросы в конце практической работы

### ***Практическое занятие 2 (8 ч.) – Разработка Положения об обработке персональных данных сотрудников организации***

Задания:

1. Разработать проект Положения об обработке персональных данных сотрудников организации.
2. Оформить в виде отчёта

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изучить Постановление Правительства РФ от 15.09.2008 № 687
3. Преподаватель выдаёт студентам перечень организаций, из которых каждый студент выбирают одну.
4. Оформить отчёт по практической работе.

### ***Практическое занятие 3 (8 ч.) – Разработка модели угроз и модели нарушителя организации***

Задания:

1. Разработать модель угроз и модель нарушителя персональных данных выбранной организации

Указания по выполнению заданий:

2. Изучить теоретический материал по теме.
3. Ввести в каждую таблицу не менее пяти строк.
4. Ответить на теоретические вопросы в конце практической работы

### ***Практическое занятие 4 (12 ч.) – Составление частного технического задания на разработку системы защиты персональных данных***

Задания:

1. Разработать проект частного технического задания на разработку системы защиты персональных данных.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изучить нормативные документы.

По результатам практических занятий работы обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office 2010 и выше и передаётся преподавателю посредством оговорённой формы связи.

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Организация и технологии защиты персональных данных» реализуется на факультете Информационных систем и безопасности кафедрой информационной безопасности.

Цель дисциплины: формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Задачи: овладеть теоретическими, практическими и методическими вопросами обеспечения информационной безопасности; изучить методы защиты персональных данных; изучить процесс работы с персональными данными в организации; научить разработке документов, регламентирующих работу с персональными данными в организации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-5 – Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
- ПК-10 – Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
- ПК-11 – Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
- ПК-15 – Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

В результате освоения дисциплины обучающийся должен:

- Знать: нормативные правовые акты в области защиты ПДн, национальные, межгосударственные и международные стандарты в области защиты ПДн; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите ПДн; методики проведения теоретических исследований уровней защищённости ИСПДн;
- Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки ПДн, установленных на объектах информатизации; составлять и оформлять аналитический отчёт по проведённым испытаниям, делать выводы по оценке защищённости ИСПДн на основании аналитического отчёта;
- Владеть: навыком разработки аналитического обоснования необходимости создания системы защиты ПДн в организации; навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищённости.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой. Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.