

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 комплексной защиты информации

## **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**10.03.01 Информационная безопасность**

*Код и наименование направления подготовки/специальности*

**«Безопасность автоматизированных систем  
(по отрасли или в сфере профессиональной деятельности)»**,

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2024

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ  
Рабочая программа дисциплины

Составитель(и):

*Кандидат технических наук, доцент, и.о. зав. кафедрой КЗИ Д.А. Митюшин*

*Ответственный редактор*

*Кандидат технических наук, доцент, и.о. зав. кафедрой КЗИ Д.А. Митюшин*

.....

УТВЕРЖДЕНО

Протокол заседания кафедры

№ 8 от 14.03.2024 г.

**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 .....	4
2. Структура дисциплины .....	5
3. Содержание дисциплины .....	5
4. Образовательные технологии .....	6
5. Оценка планируемых результатов обучения .....	7
5.1 Система оценивания .....	7
5.2 Критерии выставления оценки по дисциплине .....	8
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине .....	9
6. Учебно-методическое и информационное обеспечение дисциплины .....	10
6.1 Список источников и литературы .....	10
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет». <b>Ошибка! Закладка не определена.</b>	
7. Материально-техническое обеспечение дисциплины .....	12
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов .....	12
9. Методические материалы .....	13
9.1 Планы семинарских/ практических/ лабораторных занятий .....	13
9.2 Методические рекомендации по подготовке письменных работ <b>Ошибка! Закладка не определена.</b>	
9.3 Иные материалы .....	<b>Ошибка! Закладка не определена.</b>
Приложение 1. Аннотация дисциплины .....	16

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

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

Задачи дисциплины:

- овладеть теоретическими, практическими и методическими вопросами обеспечения защиты ПДн;
- изучить методы технической защиты ПДн, обрабатываемых в информационных системах персональных данных (ИСПДн).

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

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
<b>ПК-7</b> <i>Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</i>	<b>ПК-7.1</b> <i>Знает разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении</i>	<b>Знать:</b> <ul style="list-style-type: none"> <li>• методы и принципы технической защиты ПДн,</li> <li>• национальные, межгосударственные и международные стандарты в области защиты ПДн;</li> <li>• способы защиты ИСПДн.</li> </ul>
	<b>ПК-7.2</b> <i>Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении</i>	<b>Уметь:</b> <ul style="list-style-type: none"> <li>• анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки ПДн, установленных на объектах информатизации;</li> <li>• разрабатывать конструкторскую и технологическую документацию на ИСПДн в защищённом исполнении</li> </ul>
	<b>ПК-7.3</b> <i>Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении</i>	<b>Владеть:</b> <ul style="list-style-type: none"> <li>• навыком разработки рабочей и эксплуатационной документации на ИСПДн в защищённом исполнении</li> </ul>

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность информационных систем персональных данных» относится к дисциплинам по выбору 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», «Сети и системы передачи информации», «Программно-аппаратные средства защиты информации», «Защита от несанкционированного доступа к информации в автоматизированных системах».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Безопасность систем баз данных», «Безопасность вычислительных сетей», «Проектирование защищенных автоматизированных систем», «Эксплуатационная практика», «Преддипломная практика»

## 2. Структура дисциплины

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

### 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
6	Лекции	32
6	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. Методы и средства защиты персональных данных, обрабатываемых в информационных и системах персональных данных*

Стадия предпроектного обследования. Составление перечня ПДн, перечня сотрудников, работающих с ПДн. Описание ИСПДн. Выявление угроз безопасности персональных данных при их обработке в ИСПДн. Угрозы безопасности ПДн. Базовая модель угроз ПДн, обрабатываемых в ИСПДн. Разработка частной модели угроз безопасности ПДн. Методы и средства инженерной и физической защиты ПДн. Методы и средства технической защиты ПДн. Методы и средства программно-аппаратной защиты ПДн. Методы и средства криптографической защиты ПДн.

### *Тема 3. Техническое задание на разработку системы защиты ИСПДн*

Составление частного технического задания на разработку системы защиты персональных данных, обрабатываемых в ИСПДн. 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 дискреционного разграничения доступа. Правила мандатного разграничения доступа.

Особенности реализации мандатного разграничения доступа в реляционных СУБД. Правила разграничения доступа на основе ролей

#### **Тема 4. Проектирование систем защиты ИСПДн**

Разработка системы защиты ПДн. Выбор средств защиты информации. Программно-технические комплексы защиты информации от несанкционированного доступа. Технические средства перекрытия технических каналов утечки информации. Принципы и подходы проектирования защищённых ИСПДн. Интегрирование средств, методов и мероприятий в единый, целостный механизм. Условиями обеспечения безопасности ПДн.

Политика безопасности. Функции защиты информации. Программное решение. Сценарии настроек. Процедура входа в систему. Ценовая политика. Этапы проектирования. Обеспечение защиты информации на этапах проектирования системы защиты ИСПДн. Участники проектирования. Типовое содержание работ в части создания системы защиты ИСПДн.

#### **Тема 5. Особенности защиты персональных данных при их обработке в государственных информационных системах**

Особенности защиты ПДн 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.

#### **4. Образовательные технологии**

<b>№ п/п</b>	<b>Наименование темы</b>	<b>Виды учебных занятий</b>	<b>Образовательные технологии</b>
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
1.	<i>Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора</i>	<i>Лекция 1</i>  <i>Самостоятельная работа</i>	<i>Традиционная</i>  <i>Изучение лекционного материала и источников</i>
2.	<i>Методы и средства защиты персональных данных, обрабатываемых в информационных и системах персональных данных</i>	<i>Лекция 2</i>  <i>Самостоятельная работа</i>	<i>Традиционная</i>  <i>Изучение лекционного материала и источников</i>
3.	<i>Техническое задание на разработку системы защиты ИСПДн</i>	<i>Лекция 3</i>  <i>Самостоятельная работа</i>	<i>Традиционная</i>  <i>Изучение лекционного материала и источников</i>
4.	<i>Проектирование систем защиты ИСПДн</i>	<i>Лекция 4</i>  <i>Самостоятельная работа</i>	<i>Традиционная</i>  <i>Изучение лекционного материала и источников</i>
5.	<i>Особенности защиты персональных данных при их обработке в государственных информационных системах</i>	<i>Лекция 5</i>  <i>Самостоятельная работа</i>	<i>Традиционная</i>  <i>Изучение лекционного материала и источников</i>
6.	<i>Практическая работа 1 –</i>	<i>Практическое занятие 1</i>	<i>Защита ПР</i>

	<i>Предпроектное обследование</i>		
7.	<i>Практическая работа 2 – Разработка Частной модели угроз безопасности ПДн</i>	<i>Практическое занятие 2</i>	<i>Защита ПР</i>
8.	<i>Практическая работа 3 – Проектирование системы защиты ИСПДн</i>	<i>Практическое занятие 3</i>	<i>Защита ПР</i>
9.	<i>Практическая работа 4 – Составление частного технического задания на разработку системы защиты ИСПДн</i>	<i>Практическое занятие 4</i>	<i>Защита ПР</i>
10	<i>Практическая работа 5 – Разработка программы и методик аттестации ИСПДн (ГИС)</i>	<i>Практическое занятие 5</i>	<i>Защита ПР</i>

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:		
- <i>опрос</i>	<i>2 балла</i>	<i>10 баллов</i>
- <i>практическое занятие 1...5</i>	<i>10 баллов</i>	<i>50 баллов</i>
Промежуточная аттестация – зачёт с оценкой В традиционной форме по билетам		40 баллов
<b>Итого за семестр</b>		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B

68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

## 5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	отлично/ зачтено	<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>
82-68/ C	хорошо/ зачтено	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо 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 – «хороший».</p>
67-50/ D,E	удовлетворительно/ зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	неудовлетворительно/ не зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>



### 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-7
2.	Назовите причины актуальности проблемы защиты персональных данных	ПК-7
3.	Перечислите основные международные документы в области защиты персональных данных	ПК-7
4.	Права субъекта ПДн	ПК-7
5.	Что такое ИСПДн?	ПК-7
6.	Базовая модель угроз безопасности ПДн	ПК-7
7.	Что такое угроза безопасности ПДн?	ПК-7
8.	Основные категории нарушителей безопасности ПДн	ПК-7
9.	Методы защиты ПДн	ПК-7
10.	Что представляет собой инженерная и физическая защита ПДн	ПК-7
11.	Что такое частное техническое задание?	ПК-7
12.	Основание для разработки системы защиты ПДн	ПК-7

#### Промежуточная аттестация (примерные вопросы к зачёту с оценкой)

№	Вопрос	Реализуемая компетенция
1.	Актуальность проблемы защиты персональных данных в информационных системах персональных данных	ПК-7
2.	Федеральное законодательство Российской Федерации в области защиты персональных данных	ПК-7
3.	Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»	ПК-7
4.	Специальные нормативные документы по технической защите сведений конфиденциального характера	ПК-7
5.	Стадия предпроектного обследования.	ПК-7
6.	Выявление угроз безопасности персональных данных при их обработке в ИСПДн.	ПК-7
7.	Угрозы безопасности ПДн.	ПК-7
8.	Базовая модель угроз ПДн, обрабатываемых в ИСПДн.	ПК-7
9.	Методы и средства инженерной и физической защиты ПДн.	ПК-7
10.	Методы и средства технической защиты ПДн.	ПК-7
11.	Методы и средства программно-аппаратной защиты ПДн.	ПК-7
12.	Методы и средства криптографической защиты ПДн.	ПК-7
13.	Требования методических документов ФСТЭК и ФСБ России к составу и содержанию организационных и технических мер по обеспечению безопасности ПДн.	ПК-7
14.	Выбор средств защиты информации	ПК-7
15.	Программно-технические комплексы защиты информации от	ПК-7

	несанкционированного доступа.	
16.	Принципы и подходы проектирования защищённых ИСПДн	ПК-7
17.	Этапы проектирования ИСПДн	ПК-7

**Примерные тестовые задания – проверка сформированности компетенций – ПК-7**

**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. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
  11. 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.
  12. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // [Электронный ресурс] . – URL: <https://fstec.ru/files/234/----18--2013--N-21/262/----18--2013--N-21.pdf>. — Режим доступа: свободный.
  13. 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.
  14. 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.
  15. 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/files/492/---15--2008-/887/---15--2008-.pdf>. — Режим доступа: свободный.
  16. 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. Корнилова, А. А. Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. — Уфа : БашГУ, 2020. — 120 с. — ISBN 978-5-7477-5228-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/179914>. — Режим доступа: для авториз. пользователей.
2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 108 с. — ISBN 978-5-507-47575-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/392402>. — Режим доступа: для авториз. пользователей.

## 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>. -- Режим доступа: для авториз. пользователей.

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

1. [www.gpntb.ru/](http://www.gpntb.ru/) Государственная публичная научно-техническая библиотека.
2. [www.nlr.ru/](http://www.nlr.ru/) Российская национальная библиотека.
3. [www.nns.ru/](http://www.nns.ru/) Национальная электронная библиотека.
4. [ww.rsl.ru/](http://ww.rsl.ru/) Российская государственная библиотека.
5. [www.microinform.ru/](http://www.microinform.ru/) Учебный центр компьютерных технологий «Микроинформ».
6. [www.intuit.ru/](http://www.intuit.ru/) Образовательный сайт.
7. [www.window.edu.ru/](http://www.window.edu.ru/) Библиотека учебной и методической литературы.
8. [www.osp.ru/](http://www.osp.ru/) Журнал «Открытые системы».
9. [www.ihitika.lib.ru/](http://www.ihitika.lib.ru/) Библиотека учебной и методической литературы.

**7. Материально-техническое обеспечение дисциплины**

Для материально-технического обеспечения дисциплины необходимо:

- 1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

- 2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010 с MS Access	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	КонсультантПлюс	КонсультантПлюс	лицензионное

**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 CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;

- 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 (8 ч.) – Предпроектное обследование***

Задания:

1. Провести предпроектное исследование выбранной организации.
2. Составить перечень ПДн.
3. Провести описание ИСПДн.
4. Оформить отчёт по практической работе и защитить работу

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Преподаватель выдаёт студентам перечень организаций, из которых каждый студент выбирают одну.
3. Ответить на теоретические вопросы в конце практической работы

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, MS Office v.2010 и выше и КонсультантПлюс.

***Практическое занятие 2 (8 ч.) – Разработка Частной модели угроз безопасности ПДн***

Задания:

1. Разработать проект Частной модели угроз безопасности ПДн.
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.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, MS Office v.2010 и выше и КонсультантПлюс.

***Практическое занятие 3 (10 ч.) – Проектирование системы защиты ИСПДн***

Задания:

1. Выполнить проектирование системы защиты ИСПДн

Указания по выполнению заданий:

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

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, MS Office v.2010 и выше и КонсультантПлюс.

***Практическое занятие 4 (4 ч.) – Составление частного технического задания на разработку системы защиты ИСПДн***

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.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, MS Office v.2010 и выше и КонсультантПлюс.

***Практическое занятие 5 (10 ч.) – Разработка программы и методик аттестации ИСПДн (ГИС)***

Задания:

1. Разработать проект программы аттестации ИСПДн (ГИС) по выбранной организации.
2. Разработать проект программы аттестации ИСПДн (ГИС) по выбранной организации.

Указания по выполнению заданий:

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

Материально-техническое обеспечение занятия:

2. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, MS Office v.2010 и выше и КонсультантПлюс.

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 «Безопасность информационных систем персональных данных» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

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

Задачи: овладеть теоретическими, практическими и методическими вопросами обеспечения защиты ПДн; изучить методы технической защиты защиты ПДн, обрабатываемых в ИСПДн.

Дисциплина направлена на формирование следующих компетенций:

- ПК-7 – Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

В результате освоения дисциплины обучающийся должен:

Знать: методы и принципы технической защиты ПДн, национальные, межгосударственные и международные стандарты в области защиты ПДн; способы защиты ИСПДн;

Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки ПДн, установленных на объектах информатизации; разрабатывать конструкторскую и технологическую документацию на ИСПДн в защищённом исполнении;

Владеть: навыком разработки рабочей и эксплуатационной документации на ИСПДн в защищённом исполнении.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.