



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.В.ДВ.01.02 РАЗРАБОТКА РЕГЛАМЕНТА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ
ДАННЫХ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Старший преподаватель кафедры
Информационно-измерительных систем Бельшева Ю. В.

Старший преподаватель кафедры
Информационно-измерительных систем Нахаева А. С.

Преподаватель кафедры Информационно-измерительных систем
Рыжиков К. С.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - приобретение обучающимися знаний в области организационно-правового обеспечения защиты персональных данных, а также формирование практических навыков разработки локальных нормативных актов оператора персональных данных, соответствующих требованиям законодательства Российской Федерации.

Задачи изучения дисциплины:

- изучение законодательной и нормативно-методической базы Российской Федерации в сфере персональных данных;
- формирование у обучающихся системного понимания процесса идентификации и классификации персональных данных, обрабатываемых в организации;
- приобретение навыков анализа угроз безопасности персональных данных при их обработке в информационных системах.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-2 Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах

ПК-2.1 Осведомлен об основных угрозах безопасности информации и модели нарушителя в автоматизированных системах

Знать:

ПК-2.1/Зн3 Классификацию основных угроз безопасности персональных данных при их обработке в информационных системах

Уметь:

ПК-2.1/Ум3 Идентифицировать и классифицировать актуальные угрозы безопасности персональных данных применительно к конкретному автоматизированному рабочему месту или информационной системе

Владеть:

ПК-2.1/Нв3 Навыками к обоснованному выбору организационных и технических мер защиты, адекватных выявленной модели угроз и профилю нарушителя, для включения в текст регламента

ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности

Знать:

ПК-2.2/Зн3 Особенности классификации угроз в зависимости от структуры автоматизированной системы и категории обрабатываемых персональных данных

Уметь:

ПК-2.2/Ум4 Классифицировать выявленные угрозы безопасности персональных данных по заданным признакам

Владеть:

ПК-2.2/Нв3 Методикой классификации угроз информационной безопасности применительно к информационным системам персональных данных

ПК-2.3 Разрабатывает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации

Знать:

ПК-2.3/Зн4 Типовую структуру и содержание организационно-распорядительной документации, определяющей деятельность персонала при работе с информационными системами персональных данных

Уметь:

ПК-2.3/Ум4 Проектировать организационную структуру системы защиты персональных данных и распределять зоны ответственности между сотрудниками

Владеть:

ПК-2.3/Нв3 Методикой разработки «Политики информационной безопасности» и «Положения о защите персональных данных» в части, касающейся прав и обязанностей персонала

ПК-2.4 Контролирует эффективность принятых мер по защите информации в автоматизированных системах

Знать:

ПК-2.4/Зн3 Методики и процедуры проведения внутреннего аудита и контроля состояния защиты персональных данных в автоматизированных системах

Уметь:

ПК-2.4/Ум4 Разрабатывать планы и программы контрольных мероприятий соблюдения персоналом требований регламента защиты персональных данных

Владеть:

ПК-2.4/Нв2 Методикой проведения внутреннего аудита системы защиты персональных данных на соответствие требованиям законодательства и локальным регламентам

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.ДВ.01.02 «Разработка регламента по защите персональных данных» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 7.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
7 семестр	144	4	17	34	66	Экзамен (27)
Всего	144	4	17	34	66	27

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий (часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотношенные с результатами освоения программы
Раздел 1. Анализ объекта защиты и идентификация персональных данных	28	6	6	16	ПК-2.1
Тема 1.1. Введение в разработку регламентов защиты ПДн	8	6		2	
Тема 1.2. Инвентаризация персональных данных и субъектов	8		2	6	
Тема 1.3. Картирование потоков персональных данных	12		4	8	
Раздел 2. Оценка угроз и рисков безопасности персональных данных	26	2	10	14	ПК-2.1 ПК-2.2
Тема 2.1. Моделирование угроз безопасности ПДн	13	1	6	6	
Тема 2.2. Оценка рисков и их документирование	13	1	4	8	
Раздел 3. Проектирование организационных и технических мер защиты	45	6	13	26	ПК-2.3 ПК-2.4
Тема 3.1. Организационные и технические меры защиты ПДн	30	4	10	16	
Тема 3.2. Распределение ответственности и регламентация действий персонала	15	2	3	10	
Раздел 4. Регламентация процедур обработки и жизненный цикл документа	18	3	5	10	ПК-2.3 ПК-2.4
Тема 4.1. Взаимодействие с субъектами персональных данных	11	2	3	6	
Тема 4.2. Управление инцидентами и изменениями	7	1	2	4	
Итого	117	17	34	66	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Анализ объекта защиты и идентификация персональных данных

Тема 1.1. Введение в разработку регламентов защиты ПДн

Нормативно-правовая база РФ в области персональных данных (152-ФЗ, подзаконные акты).
Понятие оператора, субъекта, обработки.

Текущий контроль
Вид (форма) контроля
Тестирование
Практическая работа

Тема 1.2. Инвентаризация персональных данных и субъектов

Классификация категорий персональных данных (общедоступные, специальные, биометрические). Составление детального перечня ПДн и определение перечня обрабатываемых категорий. Категории субъектов ПДн: сотрудники, клиенты, контрагенты и т.д.

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 1.3. Картирование потоков персональных данных

Методы сбора информации о движении данных внутри организации и за её пределами. Построение карты потоков персональных данных для выявления мест хранения, передачи и потенциальных уязвимостей. Анализ схем взаимодействия подразделений и внешних контрагентов.

Текущий контроль
Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Оценка угроз и рисков безопасности персональных данных

Тема 2.1. Моделирование угроз безопасности ПДн

Классификация угроз (источники, типы, векторы). Изучение Банка данных угроз ФСТЭК России. Определение основных угроз безопасности ПДн для заданной организации.

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 2.2. Оценка рисков и их документирование

Понятие риска информационной безопасности: вероятность и ущерб. Методики анализа рисков (качественный и количественный подходы). Выявление и анализ рисков: составление реестра рисков на основе данных из банка угроз ФСТЭК и карты потоков.

Текущий контроль
Вид (форма) контроля
Тестирование
Практическая работа

Раздел 3. Проектирование организационных и технических мер защиты

Тема 3.1. Организационные и технические меры защиты ПДн

Состав и содержание организационных и технических мер защиты информации (Приказ ФСТЭК № 21). Определение перечня необходимых организационных и технических мер на основе проанализированных угроз и рисков. Требования к помещениям, в которых обрабатываются ПДн: организация режима и контроля доступа.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 3.2. Распределение ответственности и регламентация действий персонала

Определение обязанностей ответственных лиц по хранению и защите ПДн. Права и обязанности оператора ПДн как юридического лица. Разработка должностных инструкций и памяток для сотрудников.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 4. Регламентация процедур обработки и жизненный цикл документа

Тема 4.1. Взаимодействие с субъектами персональных данных

Права и обязанности субъекта ПДн: порядок доступа, отзыва согласия, обжалования действий оператора. Порядок и условия обработки ПДн: цели, способы, сроки. Разработка согласия на обработку ПДн: структура и обязательные элементы документа.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 4.2. Управление инцидентами и изменениями

Разработка порядка реагирования на инциденты, связанные с ПДн: выявление, регистрация, расследование, уведомление уполномоченных органов. Порядок уничтожения, блокирования, исправления и актуализации ПДн: основания и процедуры. Ответственность за нарушение норм обработки и защиты ПДн: административная, уголовная, дисциплинарная. Обстоятельства изменения регламента: пересмотр документа при изменении законодательства, структуры организации, технологий обработки.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 7 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Анализ объекта защиты и идентификация персональных данных

Контролируемые ИДК: ПК-2.1

Тема 1.1. Введение в разработку регламентов защиты ПДн

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Идентификация персональных данных и субъектов в организации

Определите гипотетическую организацию, для которой будет разрабатываться регламент. Определите перечень обрабатываемых категорий ПДн. Определите категории субъектов ПДн

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое регламент защиты персональных данных?
2. Какие основные нормативные правовые акты регулируют обработку персональных данных в РФ?
3. Какие сведения необходимо определить при выборе гипотетической организации для разработки регламента?

Тема 1.2. Инвентаризация персональных данных и субъектов

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Назовите категории персональных данных по 152-ФЗ.
2. Приведите примеры специальных категорий персональных данных.
3. Какие категории субъектов персональных данных можно выделить в типичной организации?

Тема 1.3. Картирование потоков персональных данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Моделирование потоков персональных данных и определение мер защиты

Построение DFD-диаграммы для вашей организации. Определение перечня организационных и технических мер по обеспечению информационной безопасности. Детализация списка ПДн.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое карта (схема) потоков персональных данных?
2. Какие элементы обязательно отражаются на DFD-диаграмме потоков ПДн?
3. С какой целью строится карта потоков персональных данных?

Раздел 2. Оценка угроз и рисков безопасности персональных данных

Контролируемые ИДК: ПК-2.1 ПК-2.2

Тема 2.1. Моделирование угроз безопасности ПДн

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что понимается под угрозой безопасности персональных данных?
2. Назовите основные источники угроз для персональных данных.
3. Какие классификации угроз используются при моделировании?
4. Где можно получить актуальный перечень угроз безопасности ПДн?

Тема 2.2. Оценка рисков и их документирование

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Оценка уровня защищенности и регламентация прав субъектов персональных данных

Определение уровня защищенности ПДн. Описание прав субъекта ПДн.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое риск информационной безопасности при обработке ПДн?
2. Какие методы оценки рисков существуют?
3. Что включает в себя реестр рисков?

Раздел 3. Проектирование организационных и технических мер защиты

Контролируемые ИДК: ПК-2.3 ПК-2.4

Тема 3.1. Организационные и технические меры защиты ПДн

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Формирование раздела мер и условий обеспечения безопасности персональных данных

Описание мер и условий защиты и обеспечения безопасности персональных данных.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие группы мер защиты персональных данных предусмотрены нормативными документами?
2. Приведите примеры организационных мер защиты ПДн.
3. Что относится к техническим мерам защиты ПДн?
4. Какие требования предъявляются к помещениям, где обрабатываются ПДн?

Тема 3.2. Распределение ответственности и регламентация действий персонала

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Разработка раздела о правах и обязанностях оператора и согласия на обработку ПДн
- Описание прав и обязанностей оператора ПДн. Составление согласия на обработку ПДн клиента или сотрудника.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие должностные лица обычно назначаются ответственными за обеспечение безопасности ПДн в организации?
2. Какие обязанности включаются в должностные инструкции сотрудников, работающих с ПДн?
3. Что должно быть указано в разделе регламента «Права и обязанности оператора»?
4. Какие обязанности у оператора при сборе персональных данных через интернет-сайт?

Раздел 4. Регламентация процедур обработки и жизненный цикл документа

Контролируемые ИДК: ПК-2.3 ПК-2.4

Тема 4.1. Взаимодействие с субъектами персональных данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Регламентация порядка и условий обработки персональных данных
- Описание порядка и условий обработки ПДн.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие права имеет субъект персональных данных согласно 152-ФЗ?
2. Какие обязательные элементы должно содержать согласие на обработку персональных данных?
3. В течение какого срока оператор обязан предоставить субъекту информацию о наличии его персональных данных?

Тема 4.2. Управление инцидентами и изменениями

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Определение порядка уничтожения, блокирования, исправления, актуализации ПДн и обстоятельств изменения регламента
- Описание порядка уничтожения, блокирования, исправления и актуализации ПДн. Описание обстоятельств изменения регламента.
2. Разработка порядка реагирования на инциденты и описание ответственности за нарушения

Разработка порядка реагирования на инциденты, связанные с ПДн. Описание ответственности за нарушение норм обработки и защиты ПДн.

3. Компонировка и оформление итогового регламента по защите персональных данных
Формирование регламента по защите ПДн (на основе предыдущих практических работ).

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Каков порядок уничтожения персональных данных по требованию субъекта или по истечении срока обработки?
2. Что должно быть предусмотрено в порядке реагирования на инциденты, связанные с ПДн?
3. Какие обстоятельства могут служить основанием для изменения регламента защиты ПДн?

8. Оценочные материалы промежуточной аттестации

7 семестр, Экзамен

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4

Вопросы/Задания:

1. Юридическая и техническая природа регламента защиты персональных данных: соотношение понятий, место в системе локальных нормативных актов оператора.
2. Специфика идентификации и документирования специальных и биометрических персональных данных при разработке регламента.
3. Категории субъектов персональных данных и особенности правового режима обработки данных разных категорий
4. Соотношение понятий «угроза», «уязвимость» и «риск» применительно к разработке раздела регламента об оценке угроз
5. Методика определения актуальных угроз безопасности персональных данных с использованием Банка данных угроз ФСТЭК России
6. Соотношение требований Приказа ФСТЭК № 21 и других нормативных документов при формировании перечня мер защиты в регламенте
7. Особенности регламентации защиты персональных данных в зависимости от уровня защищенности информационной системы
8. Проблема обеспечения достаточности и избыточности мер защиты при разработке регламента
9. Требования к помещениям, в которых осуществляется обработка персональных данных
10. Распределение ответственности за обеспечение безопасности персональных данных между различными категориями персонала
11. Права и обязанности оператора персональных данных

12. Юридически значимые элементы согласия на обработку персональных данных и последствия их отсутствия

13. Основания и порядок отзыва согласия на обработку персональных данных

14. Процедуры уничтожения, блокирования, исправления и актуализации персональных данных

15. Порядок реагирования на инциденты информационной безопасности, связанные с персональными данными

16. Виды ответственности за нарушение норм обработки и защиты персональных данных

17. Основания и процедура пересмотра регламента защиты персональных данных в условиях изменяющейся нормативной среды

18. Система законодательства РФ в области персональных данных

19. Сравнительный анализ понятий «оператор», «обработка», «распространение», «предоставление» и «трансграничная передача» персональных данных

20. Критерии отнесения персональных данных к специальным, биометрическим и общедоступным категориям

21. Взаимосвязь уровня защищенности персональных данных и выбранных мер защиты: как результаты оценки рисков трансформируются в требования регламента?

22. Права субъекта персональных данных

23. Правовое регулирование обработки персональных данных работников

24. Правовое регулирование обработки персональных данных клиентов

25. Порядок действий оператора при получении требования субъекта о прекращении обработки или отзыве согласия

26. Понятие инцидента информационной безопасности, связанного с персональными данными

27. Особенности разработки регламента для оператора, осуществляющего трансграничную передачу персональных данных

28. Обработка персональных данных без использования средств автоматизации

29. Методика проведения внутреннего аудита соблюдения требований регламента защиты персональных данных

30. Проблемные аспекты локализации баз данных персональных данных на территории РФ

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Информационная безопасность и правовые основы защиты персональных данных: учебное пособие: учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. - Информационная безопасность и правовые основы защиты персональных данных - Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2023. - 80 с. - 978-5-8265-2648-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/141049.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Петренко В. И. Защита персональных данных в информационных системах: учебное пособие: учебное пособие / В. И. Петренко. - Защита персональных данных в информационных системах - Ставрополь: Северо-Кавказский федеральный университет, 2016. - 201 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/66023.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Голембиовская О. М. Формализация подходов к обеспечению защиты персональных данных: монография: монография / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков. - Формализация подходов к обеспечению защиты персональных данных - Саратов: Ай Пи Эр Медиа, 2019. - 198 с. - 978-5-4486-0726-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/81851.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Кухаренко Т. А. Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (3-е издание переработанное и дополненное) / Т. А. Кухаренко, Н. А. Захарова. - Комментарий к Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (3-е издание переработанное и дополненное) - Саратов: Ай Пи Эр Медиа, 2016. - 151 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/49154.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. <https://www.garant.ru/> - Информационно-правовой портал "Гарант"
2. <https://student2.consultant.ru/cgi/online.cgi> - Правовой Сервер КонсультантПлюс

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
3. <https://intuit.ru/> - Электронная образовательная среда "ИНТУИТ"
4. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
5. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
6. <https://www.elibrary.ru/> - НЭБ eLIBRARY

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

9.4. Оборудование и технические средства обучения

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.