



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.01.01 ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ
СИСТЕМАХ»**

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:

Преподаватель кафедры Информационно-измерительных систем
Дручинин С. 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 - формирование у обучающихся глубокого понимания актуальных проблем защиты персональных данных, правового регулирования информационных отношений, а также развитие навыков эффективного применения нормативно-правовых актов и технических мер для обеспечения безопасности персональных данных в автоматизированных системах обработки и хранения информации.

Задачи изучения дисциплины:

- Изучение законодательства Российской Федерации в области обработки и защиты персональных данных, включая требования к их обработке и условиям обеспечения безопасности;
- Анализ организационных и технических мер защиты персональных данных в автоматизированных системах, включая предотвращение несанкционированного доступа, защиту от вредоносных программ, обеспечение целостности и доступности данных;
- Формирование модели потенциальных угроз для автоматизированных систем и выбор эффективных методов защиты информации, включая криптографические средства, системы контроля доступа и аутентификации пользователей;
- Развитие практических навыков реализации комплексных мер защиты персональных данных и обеспечения их безопасности в условиях современных информационных технологий.

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/Зн1 основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

Уметь:

ПК-2.1/Ум1 формировать модель нарушителя, учитывая профессиональные, служебные, функциональные и технические возможности потенциальных нарушителей

Владеть:

ПК-2.1/Вл1 навыками построения и формализации модели нарушителя для автоматизированных систем с целью систематизации информации о потенциальных угрозах и нарушителях

ПК-2.2 Классифицирует и оценивает угрозы информационной безопасности

Знать:

ПК-2.2/Зн1 классификацию угроз информационной безопасности по различным признакам: по источнику, по природе возникновения, по степени преднамеренности, по виду воздействия, по месту проявления и другим критериям

Уметь:

ПК-2.2/Ум1 классифицировать угрозы информационной безопасности с учетом различных критериев и признаков, выделять ключевые классы угроз для конкретной автоматизированной системы

Владеть:

ПК-2.2/Нв1 методиками проведения оценки рисков и приоритизации угроз для разработки эффективных мер защиты

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

Знать:

ПК-2.3/Зн1 содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации

Уметь:

ПК-2.3/Ум1 разрабатывать содержание организационно-распорядительных документов, определяющих обязанности, права и ответственность персонала при эксплуатации защищенных автоматизированных систем и систем защиты информации

Владеть:

ПК-2.3/Нв1 навыками системного подхода к разработке и структурированию организационно-распорядительных документов по безопасности информации и персональных данных в автоматизированных системах

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

Знать:

ПК-2.4/Зн1 основные методы и критерии оценки эффективности мер защиты информации в автоматизированных системах

Уметь:

ПК-2.4/Ум1 организовывать и проводить контрольные мероприятия по оценке эффективности реализованных мер защиты информации в автоматизированных системах

Владеть:

ПК-2.4/Нв1 навыками планирования и проведения аудита и мониторинга информационной безопасности в автоматизированных системах

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.ДВ.01.01 «Защита персональных данных в автоматизированных системах» 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, соотнесенные с результатами освоения программы
Раздел 1. Нормативно-правовые основы организации мер по обеспечению безопасности персональных данных	14	2	4	8	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4
Тема 1.1. Нормативно-правовые основы организации мер по обеспечению безопасности персональных данных	14	2	4	8	
Раздел 2. Виды персональных данных. Информационные системы персональных данных	19	3	6	10	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4
Тема 2.1. Виды персональных данных. Информационные системы персональных данных	19	3	6	10	
Раздел 3. Правовые основы обработки персональных данных	19	3	6	10	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4
Тема 3.1. Правовые основы обработки персональных данных	19	3	6	10	
Раздел 4. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных	21	3	6	12	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4
Тема 4.1. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных	21	3	6	12	
Раздел 5. Оценка уровня защищённости информационных систем персональных данных	23	3	6	14	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4

Тема 5.1. Оценка уровня защищённости информационных систем персональных данных	23	3	6	14	
Раздел 6. Организационно-распорядительная и техническая документация для обеспечения эффективной защиты персональных данных	21	3	6	12	ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4
Тема 6.1. Организационно-распорядительная и техническая документация для обеспечения эффективной защиты персональных данных	21	3	6	12	
Итого	117	17	34	66	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Нормативно-правовые основы организации мер по обеспечению безопасности персональных данных

Тема 1.1. Нормативно-правовые основы организации мер по обеспечению безопасности персональных данных

Понятие «персональных данных». Содержание и состав правовых актов, необходимых для эффективной защиты персональных данных. Порядок разработки и содержание приказов об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, о назначении ответственного за обработку персональных данных, о создании комиссии по организации и проведению работ по защите персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Виды персональных данных. Информационные системы персональных данных

Тема 2.1. Виды персональных данных. Информационные системы персональных данных

Проблематика обеспечения безопасности персональных данных. Принципы составления перечня персональных данных, подлежащих защите в информационных системах персональных данных, виды персональных данных, категорирование персональных данных. Понятие информационной системы персональных данных. Технические и криптографические средства обеспечения безопасности персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Правовые основы обработки персональных данных

Тема 3.1. Правовые основы обработки персональных данных

Правовые основания, порядок и условия обработки персональных данных. Цели сбора персональных данных. Состав и содержание согласие субъекта на обработку его персональных данных, уведомительных документов, разрабатываемых оператором персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 4. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных

Тема 4.1. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных

Нормативно-технические документы, определяющие понятие, классификацию угроз безопасности информации, меры противодействия угрозам, включая методические документы по оценке безопасности информации и базовую модель угроз безопасности персональных данных. Состав и содержание модели угроз, включая принципы разработки модели нарушителя. Режимы обработки персональных данных в компьютерных системах. Технические каналы утечки информации и угрозы несанкционированного доступа к информационным системам персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Оценка уровня защищённости информационных систем персональных данных

Тема 5.1. Оценка уровня защищённости информационных систем персональных данных

Классификация уровней защищённости. Принципы и основные положения определения уровня защищённости информационных систем персональных данных, включая методики расчёта показателей исходной защищённости, определения вероятности реализации угроз безопасности персональных данных. Правила определения актуальных угроз безопасности персональных данных. Состав и содержание акта определения уровня защищённости информационной системы персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 6. Организационно-распорядительная и техническая документация для обеспечения эффективной защиты персональных данных

Тема 6.1. Организационно-распорядительная и техническая документация для обеспечения эффективной защиты персональных данных

Организационные и технические мероприятия по обеспечению безопасностью персональных данных. Разработка процедур по обеспечению информационной безопасности. Требования к обеспечению безопасности персональных данных. Требования к техническим средствам защиты информации в информационных системах персональных данных. Состав и содержание организационно-распорядительной, технической, рабочей и эксплуатационной документации по защите персональных данных.

Текущий контроль

Вид (форма) контроля
Тестирование

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 наличия 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. Нормативно-правовые основы организации мер по обеспечению безопасности персональных данных

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

Тема 1.1. Нормативно-правовые основы организации мер по обеспечению безопасности персональных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие из перечисленных документов обязательно должны быть изданы в организации для обеспечения безопасности персональных данных?

- 1) Приказ о назначении ответственного за обработку персональных данных
- 2) Приказ о проведении маркетинговых исследований
- 3) Приказ о создании комиссии по организации работ по защите персональных данных
- 4) Приказ о закупке офисной техники

2. Какой из нормативных актов регулирует порядок обработки и защиты персональных данных в Российской Федерации?

- 1) Федеральный закон № 152-ФЗ
- 2) Федеральный закон № 149-ФЗ
- 3) Федеральный закон № 125-ФЗ
- 4) Федеральный закон № 52-ФЗ

3. Какова основная цель создания комиссии по организации и проведению работ по защите персональных данных?

- 1) Контроль за соблюдением трудовой дисциплины
- 2) Разработка финансового плана организации
- 3) Координация мероприятий по обеспечению безопасности персональных данных
- 4) Организация корпоративных мероприятий

Раздел 2. Виды персональных данных. Информационные системы персональных данных

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

Тема 2.1. Виды персональных данных. Информационные системы персональных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие категории персональных данных требуют особой защиты согласно законодательству РФ?

- 1) Контактные данные, доступные в справочниках
- 2) Общедоступные данные, размещённые в СМИ
- 3) Данные о месте работы и должности
- 4) Биометрические данные и данные о здоровье

2. Что включает в себя понятие информационной системы персональных данных (ИСПДн)?

- 1) Только программное обеспечение для обработки данных
- 2) Совокупность технических средств, программного обеспечения и процедур для обработки ПДн
- 3) Только физические серверы, на которых хранятся данные
- 4) Только персонал, работающий с данными

3. Какие технические средства применяются для обеспечения безопасности персональных данных?

- 1) Криптографические средства, системы контроля доступа, антивирусные программы
- 2) Только средства резервного копирования
- 3) Только программное обеспечение для анализа данных
- 4) Только средства видеонаблюдения

Раздел 3. Правовые основы обработки персональных данных

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

Тема 3.1. Правовые основы обработки персональных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие условия должны быть соблюдены для законной обработки персональных данных?

- 1) Обработка данных только в коммерческих целях
- 2) Обработка данных без уведомления субъекта при любых условиях
- 3) Наличие согласия субъекта, законные цели, соблюдение принципов обработки
- 4) Обработка данных без ограничений при наличии технических средств защиты

2. Какие сведения обязательно должны содержаться в согласии субъекта на обработку персональных данных?

- 1) Цели обработки, перечень обрабатываемых данных, срок обработки, права субъекта
- 2) ФИО субъекта и дата согласия
- 3) Наименование оператора, наименование субъекта, права субъекта
- 4) Контактные данные оператора, контактные данные субъекта

3. Какие документы должен разработать оператор персональных данных для информирования субъектов?

- 1) Инструкцию по эксплуатации офисной техники
- 2) Трудовой договор с сотрудниками
- 3) Финансовый отчет организации
- 4) Уведомление о порядке обработки персональных данных

Раздел 4. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных

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

Тема 4.1. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие из перечисленных угроз относятся к техническим каналам утечки информации?

- 1) Электромагнитные излучения, акустические каналы, побочные излучения оборудования, вибрационные сигналы и паразитные электрические наводки
- 2) Нарушение трудовой дисциплины, социальная инженерия и инсайдерские действия
- 3) Ошибки в документации, неправильное оформление регламентирующих документов и утечка через бумажные носители
- 4) Недостаточная квалификация персонала, несоблюдение процедур и человеческий фактор

2. Что входит в состав базовой модели угроз безопасности персональных данных?

- 1) Только организационные меры защиты, включая инструкции, регламенты и кадровую политику без технических аспектов
- 2) Исключительно перечень известных вредоносных программ и их сигнатур, используемых для атак на персональные данные
- 3) Классификация угроз, описание модели нарушителя, перечень мер организационного, технического и программного противодействия, а также методики оценки рисков и уязвимостей
- 4) Исключительно технические средства защиты, такие как межсетевые экраны, системы обнаружения вторжений и шифрование данных

3. Какие режимы обработки персональных данных существуют в информационных системах?

- 1) Открытый, ограниченный, закрытый
- 2) Открытый, закрытый, неполный
- 3) Закрытый, открытый
- 4) Ограниченный, полный

Раздел 5. Оценка уровня защищённости информационных систем персональных данных

Тема 5.1. Оценка уровня защищённости информационных систем персональных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие показатели учитываются при оценке уровня защищённости ИСПДн?

- 1) Общее количество пользователей системы, их роль и уровень доступа, а также частота их взаимодействия с персональными данными
- 2) Вероятность реализации угроз, степень уязвимости системы, эффективность и полнота применяемых мер защиты, а также количество и категории обрабатываемых персональных данных
- 3) Стоимость оборудования, включая программное обеспечение и технические средства защиты, а также затраты на обслуживание и обновление инфраструктуры
- 4) Скорость обработки данных, пропускная способность каналов связи и время отклика системы на запросы пользователей

2. Что должно содержать заключение (акт) определения уровня защищённости информационной системы персональных данных?

- 1) Подробное описание структуры и характеристик ИСПДн, выявленные актуальные угрозы безопасности, оценка рисков, классификация обрабатываемых персональных данных, а также рекомендации по выбору и внедрению мер защиты, включая организационные и технические аспекты
- 2) Перечень сотрудников с доступом к персональным данным, их должностные инструкции и уровни полномочий, а также сведения об их обучении и аттестации
- 3) Финансовый отчет по проекту, включающий затраты на оборудование, программное обеспечение, услуги специалистов и текущие расходы на поддержку системы
- 4) Технические характеристики серверного оборудования, сетевой инфраструктуры, используемых операционных систем и программных платформ, а также параметры производительности и отказоустойчивости

3. Какие организационные меры относятся к обеспечению безопасности персональных данных?

- 1) Организация регулярного резервного копирования данных, обеспечение отказоустойчивости и восстановления информации после сбоев
- 2) Установка и регулярное обновление антивирусного программного обеспечения, мониторинг сетевого трафика и использование средств защиты от вредоносного ПО
- 3) Применение криптографических средств защиты данных, включая шифрование, цифровые подписи и системы управления ключами
- 4) Назначение ответственных лиц, разработка инструкций, проведение обучения персонала

Раздел 6. Организационно-распорядительная и техническая документация для обеспечения эффективной защиты персональных данных

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

Тема 6.1. Организационно-распорядительная и техническая документация для обеспечения эффективной защиты персональных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие документы относятся к организационно-распорядительной документации по защите персональных данных?

- 1) Приказы о назначении ответственных за обработку и защиту персональных данных, внутренние инструкции и положения по организации и обеспечению безопасности ПДн, регламенты обработки и хранения данных
- 2) Договоры с поставщиками оборудования и услуг, включающие технические условия и соглашения о конфиденциальности

3) Бухгалтерские отчёты, финансовые планы и документы, связанные с управлением финансами организации

4) Маркетинговые планы, стратегии продвижения и анализ целевой аудитории

2. Какие требования предъявляются к техническим средствам защиты информации в ИСПДн?

1) Высокая производительность и скорость обработки данных, позволяющая минимизировать задержки при работе с большими объёмами информации

2) Соответствие нормативным документам, обеспечение конфиденциальности, целостности и доступности данных

3) Низкая стоимость приобретения и эксплуатации технических средств, включая минимальные затраты на обслуживание и обновление

4) Простота и удобство использования технических средств для конечных пользователей без необходимости глубоких технических знаний

3. Какие организационные мероприятия способствуют обеспечению безопасности персональных данных?

1) Разработка и внедрение процедур информационной безопасности, обучение персонала, контроль доступа

2) Установка офисного программного обеспечения для повышения производительности сотрудников и автоматизации рабочих процессов

3) Организация корпоративных мероприятий и тимбилдингов для улучшения командного духа и коммуникации внутри коллектива

4) Закупка новой оргтехники с целью обновления парка оборудования и повышения технической оснащённости офиса

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. Назовите сферу регулирования и цель федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

2. Дайте определение персональным данным (ПДн) и информационной системе персональных данных (ИСПДн) согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

3. Дайте определение обработке и конфиденциальности персональных данных (ПДн) согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

4. Перечислите принципы обработки персональных данных (ПДн) согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

5. В каких случаях допускается обработка персональных данных (ПДн) согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ?

6. Перечислите элементы согласия в письменной форме субъекта персональных данных на обработку его персональных данных (ПДн) согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

7. Перечислите специальные категории персональных данных (ПДн) и условия их обработки согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.
8. Перечислите информацию, на получение которой субъект персональных данных имеет право, касающейся обработки его персональных данных, согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.
9. В каких случаях может быть ограничено право субъекта персональных данных на доступ к его персональным данным согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ?
10. В каких случаях оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных согласно федеральному закону «О персональных данных» от 27 июля 2006 г. № 152-ФЗ?
11. Перечислите состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных, согласно Приказу ФСТЭК РФ от 18.02.2013 N 21.
12. Опишите этапы выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, согласно Приказу ФСТЭК РФ от 18.02.2013 N 21.
13. Перечислите дополнительные меры по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных, согласно Приказу ФСТЭК РФ от 18.02.2013 N 21.
14. Приведите содержание мер по защите информационной системы, ее средств, систем связи и передачи данных согласно Приказу ФСТЭК РФ от 18.02.2013 N 21.
15. Приведите содержание мер по защите машинных носителей персональных данных согласно Приказу ФСТЭК РФ от 18.02.2013 N 21.
16. Дайте определение и перечислите типы актуальных угроз безопасности персональных данных согласно Постановлению Правительства РФ от 01.11.2012 N 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных».
17. Дайте определение безопасности персональных данных, техническим средствам информационной системы персональных данных и угрозам безопасности персональных данных согласно «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. 15.02.2008 ФСТЭК РФ).
18. Дайте определение уязвимости информационной системы персональных данных и приведите причины возникновения данных уязвимостей согласно «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. 15.02.2008 ФСТЭК РФ).

19. Дайте определение программно-математическому воздействию и перечислите функции вредоносных программ согласно «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. 15.02.2008 ФСТЭК РФ).

20. Приведите описание архитектуры безопасности приложения анализа персональных данных согласно ГОСТ Р 59407-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие: учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.] - Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации - Саратов: Вузовское образование, 2024. - 265 с. - 978-5-4487-0942-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/134999.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

4. 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

5. Петренко В. И. Защита персональных данных в информационных системах: лабораторный практикум: лабораторный практикум / В. И. Петренко, И. В. Мандрица. - Защита персональных данных в информационных системах - Ставрополь: Северо-Кавказский федеральный университет, 2018. - 118 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/83198.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Шинаков К. Е. Анализ рисков безопасности информационных систем персональных данных: монография: монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. - Анализ рисков безопасности информационных систем персональных данных - Москва: Ай Пи Ар Медиа, 2020. - 236 с. - 978-5-4497-0535-8. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/95150.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Скрипник Д. А. Обеспечение безопасности персональных данных: учебное пособие: учебное пособие / Д. А. Скрипник. - Обеспечение безопасности персональных данных - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 121 с. - 978-5-4497-2414-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/133952.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Анализ состояния защиты данных в информационных системах: учебно-методическое пособие: учебно-методическое пособие / сост. В. В. Денисов. - Анализ состояния защиты данных в информационных системах - Новосибирск: Новосибирский государственный технический университет, 2012. - 52 с. - 978-5-7782-1969-4. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/44897.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Макаров А. М. Организация защиты персональных данных: лабораторный практикум: лабораторный практикум / А. М. Макаров, И. В. Калиберда, К. О. Бондаренко. - Организация защиты персональных данных - Ставрополь: Северо-Кавказский федеральный университет, 2015. - 92 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/62971.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

Не используются.

Ресурсы «Интернет»

1. <https://www.iprbookshop.ru/> - IPR BOOKS
2. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
3. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"

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)

1. Microsoft Office;

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.

Моноблок - 64 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;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

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.