МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И.Н.Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника – Специалист по защите информации

Специализация: «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Министерства образования и науки 01.12.2016 г. №1509

СОСТАВИТЕЛЬ:
кандидат физ.-мат. наук, доцент Д.В. Ильин

ОБСУЖДЕНО:
на заседании кафедры МиАОИС факультета ИВТ 30 августа 2017 г., протокол № 1

заведующий кафедрой Д.В. Ильин

СОГЛАСОВАНО:
Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета А.В. Щипцова

Директор научной библиотеки Н.Д. Никитина

Начальник управления информатизации И.П. Пивоваров

Начальник учебно-методического управления В.И. Маколов

Оглавление

1. Цель преподавания дисциплины

Целью дисциплины «Обеспечение безопасности персональных данных» является освоение теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Задачи дисциплины:

- изучение нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;
- изучение методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;
- практическая отработка способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Место дисциплины в профессиональной подготовке специалиста

Дисциплина «Обеспечение безопасности персональных данных» относится к базовой части, дисциплинам специализации.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплины «Правоведение» Дисциплина «Обеспечение безопасности персональных данных» является предшествующей для преддипломной практики и государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

(З1): содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

(З2): основные виды угроз безопасности персональных данных в информационных системах персональных данных;

(З3): порядок применения организационных мер и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

уметь:

(У1): разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных;

(У2): проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

владеть навыками:

(Н1): определения уровня защищенности систем персональных данных;

(Н2): выявления угроз безопасности персональных данных в информационных системах персональных данных.

4. Структура и содержание учебной дисциплины.

Образовательная деятельность по дисциплине проводится:

- в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);
- в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины.

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Правовые и организационные основы технической защиты персональных данных	ОПК-6, ПСК-4.1	З1, У1
Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.		
Раздел 2. Угрозы безопасности персональных данных	ПК-4	З2, У2, Н2
Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё.		
Раздел 3. Обеспечение безопасности персональных данных	ОПК-6, ПК-4, ПСК-4.1	З3, У2, Н1
Определение необходимых уровней защищенности персональных данных Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.		
Зачет	ОПК-6, ПК-4, ПСК- 4.1	З1, З2,З3, У1, У2, Н1, Н2

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения.

Аудиторные занятия	Всего час.	Контактная работа, час.				СРС, час.	ИФР, час	К, час.
		Л	П/р	Л/р	КСР			
Раздел 1. Правовые и организационные основы технической защиты персональных данных								

Тема 1. Правовые и организационные основы технической защиты информации ограниченного доступа	16	2	2	4		8	4	
Раздел 2. Угрозы безопасности персональных данных								
Тема 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	22	4	4	6		8	8	
Тема 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	23	4	4	6		9	8	
Раздел 3. Обеспечение безопасности персональных данных								
Тема 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	25	4	4	8		9	8	
Тема 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	20	2	2	8		8	4	
Зачет	2				2			
Итого	**108 3 з.е.**	**16**	**16**	**32**	**2**	**42**	**32**	

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

РАЗДЕЛ 1. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 1. Правовые и организационные основы технической защиты информации ограниченного доступа

1. Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.

Практическое занятие. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ.

2. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных

данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Практическое занятие. Способы защиты прав субъектов персональных данных.

РАЗДЕЛ 2. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Тема 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

3. Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз. Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP.

Практическое занятие. Методы оценки опасности угроз.

4. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Практическое занятие. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

5. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Практическое занятие. Порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Тема 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

6. Особенности информационного элемента информационной системы персональных данных. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам.

Практическое занятие. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения.

7. Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных

ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии. Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа.

Практическое занятие. Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.

8. Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

Практическое занятие. Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

РАЗДЕЛ 3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Тема 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

9. Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных. Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

Практическое занятие. Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

10. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных. Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.

Практическое занятие. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.

11. Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных. Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации.

Практическое занятие. Основные этапы при организации работ по обеспечению безопасности персональных данных.

12. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление. Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки

персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их деобезличивание. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Практическое занятие. Порядок и методы обезличивания персональных данных, их деобезличивание.

Практическое занятие. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных

Тема 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных

13. Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных.

Практическое занятие. Основное содержание этапов организации обеспечения безопасности персональных данных.

14. Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.

Практическое занятие. Типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.

15. Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

Практическое занятие. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

5.2 Лабораторные работы

На лабораторные занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений.

1. Определение перечня персональных данных на примере банка и больницы.
2. Определение угроз безопасности предприятия на примере банка и больницы.
3. Рассмотрение статей 149 ФЗ «Об информации, информационных технологиях и о защите информации»
4. Рассмотрение статей 152 ФЗ «О персональных данных»
5. Рассмотрение статей ФЗ 98 «О коммерческой тайне», ФЗ 99 «О лицензировании отдельных видов деятельности».
6. Рассмотрение статей УК РФ и Коап РФ, связанных с преступлениями в сфере ИТ и защиты ПДн.
7. Определение уровня защищенности персональных данных предприятия на примере банка и больницы
8. Составление модели актуальных угроз предприятия

5.3. Вопросы для самостоятельной работы студента в соответствии с содержанием разделов дисциплины

Тема	Вопрос

Тема 1. Правовые и организационные основы технической защиты информации ограниченного доступа	Ознакомление с законодательством в сфере защиты информации ограниченного доступа (ФЗ 149, ФЗ 152, ФЗ 98, ФЗ 99)
Тема 2. Выявление угроз безопасности информации на объектахинформатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Составить и заполнить опросный лист для определения исходного уровня защищенности информационной системы персональных данных
Тема 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	Ознакомление с базовой моделью угроз безопасности персональных данных (ФСТЭК 15.02.2008)
Тема 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Ознакомление с методикой определения актуальных угроз безопасности персональных данных (ФСТЭК 14.02.2008)
Тема 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	Самостоятельная работа с моделью угроз на предприятии, выработка предложений по мерам устранения выявленных угроз.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- диагностики;
- целеполагания;
- управления процессом освоения учебной информации;
- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.);
- контроля качества и оценивания результатов образовательной деятельности (технология оценивания качества знаний, рейтинговая технология оценки знаний и др.)

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;
- лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны)для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая

по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ литературы по теме, подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание проверка отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся:

7.1. Примерный перечень вопросов к зачету

1. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ.
2. Лицензирование деятельности в области технической защиты информации.
3. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.
4. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
5. Способы защиты прав субъектов персональных данных
6. Целостность, конфиденциальность и доступность информации.
7. Классификационная схема угроз безопасности информации и их общая характеристика.
8. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации.
9. Классификация объектов информатизации.
10. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз.
11. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ,
12. Особенности программно-математического воздействия в сетях общего пользования.
13. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё.
14. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования
15. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
16. Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
17. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения.

18. Угрозы несанкционированного доступа к информации в информационных системах персональных данных.

19. Угрозы утечки информации по техническим каналам.

20. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

21. Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.

22. Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации.

23. Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.

24. Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

25. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.

26. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.

27. Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.

28. Организация обеспечения безопасности персональных данных в организациях и учреждениях.

29. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных.

30. Обязанности оператора, осуществляющего обработку персональных данных.

31. Порядок и условия обработки персональных данных без средств автоматизации.

32. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

33. Основное содержание этапов организации обеспечения безопасности персональных данных.

34. Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных.

Оценивание результатов зачета

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания в течение семестра, имеются твердые и полные знания программного материала, правильные действия по применению знаний на практике, четкое изложение материала

Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания в течение семестра, либо наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять

знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение учебной дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература.

(ежегодное обновление перечня и условия доступа представлены в Приложениях к рабочей программе)

№	Название
1.	Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"[Электронный ресурс]: http://ivo.garant.ru/#/document/12148567/paragraph/24880:2
2.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" [Электронный ресурс]: http://ivo.garant.ru/#/document/12148555/paragraph/3471:3
3.	Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]: http://ivo.garant.ru/#/document/70380924/paragraph/1:7

8.2. Рекомендуемая дополнительная литература.

(ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№	Название
1.	«Методика определениях актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России14 февраля 2008 г.[Электронный ресурс]: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god
2.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god
3.	Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"[Электронный ресурс]: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
	MS Windows/Arch linux	лицензия университета/ свободное лицензионное соглашение (https://www.archlinux.org/download/)
	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Российская Государственная Библиотека	http://www.rsl.ru
2.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
3.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
4.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
5.	Научная электронная библиотека	http://elibrary.ru
6.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
7.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение учебной дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);
– мультимедийный проектор с дистанционным управлением
– настенный экран;
– интерактивная доска SMART;

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11.Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. Основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании расчетно-графической работы.

Формы организации студентов на лабораторных работах и практических занятиях: фронтальная и индивидуальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу. При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.