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
«Аттестация объектов информатизации по требованиям безопасности информации»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) 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 №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В.Ильин
Старший преподаватель С.О. Иванов

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информационных систем
«30» августа 2017г., 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 и задачи обучения по дисциплине

Целью дисциплины «Аттестация объектов информатизации по требованиям безопасности информации» является обеспечение всестороннего анализа состояния информационной безопасности, методов и средств защиты данных для конкретного рабочего места (подразделения).

Основными задачами дисциплины являются изучение:

- выполнять анализ объектов защиты информации и угроз безопасности информации;
- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации аттестации автоматизированных систем.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Аттестация объектов информатизации по требованиям безопасности информации» относится к обязательным дисциплинам базовой части. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Моделирование и проектирование автоматизированных информационных систем», «Технические каналы утечки информации».

Дисциплина является предшествующей для дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Аудит информационных технологий и систем обеспечения информационной безопасности», прохождения производственных и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
- способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20).

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

знать:

- особенности информационных элементов и технических средств объектов информатизации (З1);
- способы обеспечения обеспечению безопасности автоматизированных систем (З2);
- технические каналы утечки информации и типы вредоносного воздействия (З3);
- особенности сертификации средств защиты информации автоматизированных систем (З4);

- особенности аттестации автоматизированных систем с учетом нормативных документов по защите информации (З5);
- требования информационной безопасности для автоматизированных систем (З6);

уметь:

- применять средства защиты информации (У1);
- анализировать защищенности объектов информатизации (У2);
- выявлять каналы утечки информации, источники вредоносных воздействий (У3);
- осуществлять экспериментально-исследовательские работы при сертификации средств защиты информации автоматизированных систем (У4);
- осуществлять экспериментально-исследовательские работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации (У5);
- выполнять требования информационной безопасности для автоматизированных систем (У6);

владеть навыками:

- выбора подходящих режимов работы средств защиты информации (Н1);
- по разработке и анализу проектных решения по обеспечению безопасности автоматизированных систем (Н2);
- оценки эффективности работы существующих средств защиты (Н3);
- по организации экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (Н4);
- по организации экспериментально-исследовательских работ при аттестации автоматизированных систем (Н5);
- по организации разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности (Н6).

4. Структура и содержание 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 (практические занятия, лабораторные работы), 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. Инвентаризация информационной системы	ПК-8, ПК-20	З2,З6, У2, У6
Тема 1.1. Классификация элементов информационной системы		
Тема 1.2. Аспекты информационной безопасности		
Раздел 2. Анализ защищенности данных в информационной системе	ПК-14, ПК-15, ПК-16	З3-З5, У3-У5, Н3-Н5
Тема 2.1. Выявление каналов утечки информации		
Тема 2.2. Классификация вредоносных действий		
Раздел 3. Инвентаризация методов и средств защиты информации	ОПК-8, ПК-8, ПК-20	З1, З2, З6, У1, Н1, Н2, Н6

Тема 3.1. Классификация методов и средств защиты информации		
Тема 3.2. Инвентаризация методов и средств защиты информации в информационной системе		
Зачет	ПК-8, ПК-14, ПК-15, ПК-16	З2-З5, У2-У5, Н2-Н5

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

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Инвентаризация информационной системы								
Тема 1.1. Классификация элементов информационной системы	18	2	4	6		6	4	
Тема 1.2. Аспекты информационной безопасности	16	4		4		8	4	
Раздел 2. Анализ защищенности данных в информационной системе								
Тема 2.1. Выявление каналов утечки информации	16	2	2	8		4	4	
Тема 2.2. Классификация вредоносных действий	18	2	4	4		8	4	
Раздел 3. Инвентаризация методов и средств защиты информации								
Тема 3.1. Классификация методов и средств защиты информации	16	4	2	4		6	4	
Тема 3.2. Инвентаризация методов и средств защиты информации в информационной системе	22	2	4	6		10	4	
Зачет	2				2			
Итого	108 3 з.е	16	16	32	2	42	24	0

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Инвентаризация информационной системы

Тема 1.1. Классификация элементов информационной системы

Лекция 1. Объекты защиты информации в телекоммуникационных системах.

1. Условия, определяющие характер функционирования телекоммуникационных систем

2. Объекты защиты информации в телекоммуникационных системах

3. Анализ основных закономерностей функционирования телекоммуникационных

Практическое занятие 1. Классификация элементов информационной системы.

Практическое занятие 2. Бизнес-процессы компании.

Тема 1.2. Аспекты информационной безопасности

Лекция 2. Аспекты информационной безопасности

1. Современное состояние проблемы контроля безопасности информации в телекоммуникационных системах

2. Проблема разграничения доступа и защиты от несанкционированного доступа

3. Проблема обеспечения информационной безопасности в территориально распределенной системе

4. Проблема обеспечения безопасности информации при реализации нетрадиционных видов информационных услуг

Практическое занятие 3. Активы и ресурсы компании

Практическое занятие 4. Идентификация обрабатываемой информации

Раздел 2. Анализ защищенности данных в информационной системе

Тема 2.1. Выявление каналов утечки информации

Лекция 3. Выявление каналов утечки информации

1. Особенности сигналов, обрабатываемых на объектах телекоммуникационных систем

2. Проблема специальных исследований на предмет наличия аппаратных и программных закладок

3. Проблема разведзащищенности системы (защиты от демаскирования)

Практическое занятие 5. Каналы утечки информации

Практическое занятие 6. Инвентаризация оборудования и ресурсов инфраструктуры.

Тема 2.2. Классификация вредоносных действий

Лекция 4. Классификация вредоносных действий

1. Описания вредоносных воздействий на данные. Матрицы U и V

2. Проблема защиты от преднамеренной перегрузки ресурсов системы и переадресации информации

3. Проблема ЗИ при выходе на международные сети

Практическое занятие 7. Угрозы компании.

Практическое занятие 8. Уязвимости компании.

Раздел 3. Инвентаризация методов и средств защиты информации

Тема 3.1. Классификация методов и средств защиты информации

Лекция 5. Классификация методов и средств защиты информации

1. Проблема комплексной защиты информации по всем компонентам

2. Проблема построения защищённой системы на основе принципиально открытой модели

3. Проблема аутентификации абонентов и абонентских установок

4. Проблема разработки оптимальных ключевых структур

Практическое занятие 9. Роли и группы пользователей

Практическое занятие 10. Классификация методов и средств защиты информации

Тема 3.2. Инвентаризация методов и средств защиты информации в информационной системе

Лекция 6. Инвентаризация методов и средств защиты информации в информационной системе

1. Проблема организации управления защитой информации

2. Проблема интегральной оценки защищенности информации при использовании различных средств комплексной защиты информации

3. Анализ степени перекрытия каналов утечки информации

4. Обоснование структуры системы комплексного контроля безопасности информации

Практическое занятие 11. Регламент работы СЗИ

Практическое занятие 12. Оценка ущерба от нарушений Конфиденциальности, Целостности, Доступности.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторная работа 1. Описание бизнес-процессов компании.	4
Лабораторная работа 2. Инвентаризация обрабатываемой информации	2
Лабораторная работа 3. Инвентаризация оборудования и ресурсов инфраструктуры.	4
Лабораторная работа 4. Описание ролей и групп пользователей	2
Лабораторная работа 5. Оценка ущерба от нарушений Конфиденциальности, Целостности, Доступности.	4

Итого	16

5.3. Вопросы для самостоятельной работы студента.

1. ГОСТ Р 51000.4-2011 «Общие требования к аккредитации испытательных лабораторий»
2. Требования к испытательным лабораториям (центрам) и порядок проведения их аккредитации.
3. Требования к органам по сертификации и порядок их аккредитации
4. Требования к экспертами и порядок их аккредитации.

6. Образовательные технологии

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

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской).

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: подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ; защита исследовательской работы. 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 преподавателем, читающим лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Какие элементы данных могут быть включены в список защищаемых?
2. Каковы цели инвентаризации элементов информационной системы?
3. Какие существуют способы инвентаризации элементов информационной системы?
4. В каком виде оформляются результаты инвентаризации?
5. Что такое Доступность, Целостность, Конфиденциальность как аспекты ИБ?
6. Что такое Доступность, Целостность, Конфиденциальность как основа классификации СЗИ?
7. Какие виды затрат включаются в сумму ущерба от вредоносного воздействия?
8. Что такое затраты на восстановление работоспособности?
9. Как формируется список элементов требующих обязательной защиты?
10. Что такое канал утечки?
11. Как оценить степень вредоносного воздействия?
12. Как рассчитывается приведённая матрица вредоносных воздействий V?
13. Какие методы защиты применимы для повышения Доступности, Целостности, Конфиденциальности?

7.2. 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 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 и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
2.	Демидов А.А. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Электронный ресурс] : учебное пособие / А.А. Демидов. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2015. — 70 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67555.html
3.	Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс] : учебное пособие / К.А. Паршин. — Электрон. текстовые данные. — М. :

	Учебно-методический центр по образованию на железнодорожном транспорте, 2015. — 96 c. — 978-5-89035-821-9. — Режим доступа: http://www.iprbookshop.ru/45291.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Аккредитация и аттестация [Электронный ресурс] : сборник нормативных актов и документов / . — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2015. — 77 c. — 978-5-905916-68-7. — Режим доступа: http://www.iprbookshop.ru/30281.html
2.	Герасимов, А.А. Обследование объектов информатизации: методические указания к выполнению лабораторной работы по курсу «Аттестация объектов информатизации» [Электронный ресурс] : метод. указ. / А.А. Герасимов, Е.В. Вайц. — Электрон. дан. — Москва : МГТУ им. Н.Э. Баумана, 2012. — 28 с. — Режим доступа: https://e.lanbook.com/book/62002. — Загл. с экрана.
3.	Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации.: Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.

8.3. Правовые нормативные акты и нормативно-методические документы ограниченного доступа (доступны на кафедре)

1. Руководящий документ. Защита информации. Комплектующие помехоподавляющие изделия электронной техники, радиоэкранирующие и радиопоглощающие материалы. Общие технические требования. Утвержден приказом Гостехкомиссии России от 31.08.2001 № 355.
2. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27.
3. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282.
4. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.
5. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.
6. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 № 119. Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.
7. Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. № 119.
8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.
9. Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
10. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

11. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

12. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

8.4. 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//*

8.4.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	SPID_AlgorithmPoC-0-4-6	https://sourceforge.net/projects/spid/files/
4.	Snort2_9_11_1	https://www.snort.org/
5.	Wireshark 2.6.3	https://www.wireshark.org/
6.	Zabbix	https://www.zabbix.com/download
7.	Clonezilla	https://clonezilla.org/downloads.php
8.	rsync	https://rsync.samba.org/
9.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
10.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
11.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
12.	360 Total Security	https://www.360totalsecurity.com/ru/
13.	Система обнаружения вторжений	Snort https://www.snort.org/
14.	Средства дублирования и восстановления данных	Clonezilla https://clonezilla.org/downloads.php, rsync https://rsync.samba.org/
15.	Средства мониторинга состояния автоматизированных систем	Zabbix https://www.zabbix.com/download

8.4.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)
2.	Консультант +	
3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

8.5. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Xgu.ru.	http://xgu.ru/wiki/
2.	Российская Государственная Библиотека	http://www.rsl.ru
3.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
4.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
5.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru

6.	Научная электронная библиотека	http://elibrary.ru
7.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
8.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
9.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
10.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
11.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru

9. Материально-техническое обеспечение 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.

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. 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 выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

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.

Лист актуализации

№ п/п	Наименование документа	Решение кафедры		Подпись	Должность, ФИО
		Дата	протокол №		