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
«Защита ключевых систем информационной инфраструктуры»

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 обобщить знания и умения по обеспечению защиты основных элементов инфраструктуры.

Основными задачами дисциплины являются изучение:

– администрирование подсистем информационной безопасности автоматизированных систем;

– анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;

– разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем.

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

Дисциплина «Защита ключевых систем информационной инфраструктуры» относится к числу обязательных дисциплин вариативной части. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Основы информационной безопасности», «Программно-аппаратные средства защиты информации», «Безопасность операционных систем», «Безопасность систем баз данных», «Информационная безопасность web-ресурсов».

Дисциплина является предшествующей для дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», 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 участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способность управлять информационной безопасностью автоматизированной системы (ПК-28).

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

знать:

– принцип работы средств защиты информации (З1);

– принципы построения и функционирования ключевых систем (З2);

– правила, процедуры и методы защиты информации ограниченного доступа (З3)

– принципы организации и структуру подсистем защиты ключевых систем (З4);

– способы управления информационной безопасностью автоматизированной системы (З5);

уметь:

– эксплуатировать и обслуживать программные, и технические средства защиты информации (У1);

– оценивать эффективность и надежность компонентов ключевых систем (У2);

– выбирать подходящие правила, процедуры и методы информационной безопасности в зависимости от требований (У3);

– применять средства защиты информации (У4);

– контролировать и поддерживать информационную безопасность автоматизированной системы (У5);

владеть навыками:

– выбора, установки и настройки средств защиты информации (Н1);

– настройка информационных процессов ключевых системы (Н2);

– разработки комплекса мер для защиты информации ограниченного доступа (Н3);

– выполнения требований информационной безопасности (Н4);

– организации системы управления информационной безопасностью автоматизированной системы (Н5).

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. Средства защиты операционных систем	ОПК-8, ПК-22, ПК-23, ПК-24, ПК-28	З1-5, У1-5, Н1-5
Тема 1.1. Управление безопасность ОС.		
Раздел 2. Средства сетевой защиты	ОПК-8, ПК-22, ПК-23, ПК-24, ПК-28	З1-5, У1-5, Н1-5
Тема 2.1. Принципы сетевой безопасности.		
Тема 2.2. Сетевые экраны.		
Раздел 3. Защита web-ресурсов	ОПК-8, ПК-22, ПК-23, ПК-24, ПК-28	З1-5, У1-5, Н1-5
Тема 3.1. Угрозы web-ресурсам.		
Раздел 4. Защита баз данных.	ОПК-8, ПК-22, ПК-23, ПК-24, ПК-28	З1-5, У1-5, Н1-5
Тема 4.1. Угрозы базам данных.		
Зачет	ОПК-8, ПК-22, ПК-23, ПК-24, ПК-28	З1-5, У1-5, Н1-5

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. Средства защиты операционных систем								
Тема 1.1. Управление безопасность ОС.	28	4	4	4		16	2	
Раздел 2. Средства сетевой защиты								
Тема 2.1. Принципы сетевой безопасности.	14	2	2	2		8		
Тема 2.2. Сетевые экраны.	16	2	2	2		10	2	
Раздел 3. Защита web-ресурсов								
Тема 3.1. Угрозы web-ресурсам.	22	4	4	4		10	2	
Раздел 4. Защита баз данных.								
Тема 4.1. Угрозы базам данных.	22	4	4	4		10	2	
Зачет	6				2	4		
Итого	108/3 з.е.	16	16	16	2	58	8	0

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Средства защиты операционных систем

Тема 1.1. Управление безопасность ОС.

Лекция 1. Угрозы ОС.

1. Виды атак на ОС.
2. Классификация мер защиты.

Практическое занятие 1. Обнаружение уязвимостей ОС.

Лекция 2. Антивирусы.

1. Классификация зловредных программ.
2. Принципы и методы работы антивирусов.

Практическое занятие 2. Антивирус.

Раздел 2. Средства сетевой защиты

Тема 2.1. Принципы сетевой безопасности.

Лекция 3. Проблемы сетевой безопасности.

1. Проблемы и уязвимости сетевых протоколов.
2. Виды сетевых атак.

Практическое занятие 3. Сетевой полигон.

Тема 2.2. Сетевые экраны.

Лекция 4. Сетевые экраны.

1. Принцип работы.
2. Классификация сетевых экранов.
3. Демилитаризованная зона.

Практическое занятие 4. Iptables.

Раздел 3. Защита web-ресурсов

Тема 3.1. Угрозы web-ресурсам.

Лекция 5. Атаки на web-ресурсы

1. Атаки нарушения аутентификации и сеансов.
2. Инъекции вредоносного кода.
3. Фишинг.
4. Межсайтовый скриптинг.

Практическое занятие 5. Проверка web-ресурса на типичные уязвимости.

Лекция 6. Проблемы управления web-ресурсом.

1. Запрещённый контент.
2. Непроверенные переадресации и пересылки
3. Подмена формы (form spoofing).
4. Нелегальное копирование контента веб-сайта.

Практическое занятие 6. Сбор и анализ содержимого веб-ресурса.

Раздел 4. Защита баз данных.

Тема 4.1. Угрозы базам данных.

Лекция 7. Особенности защиты БД

1. Функционирование в доверенной среде.
2. Организация физической безопасности файлов данных.
3. Организация безопасной и актуальной настройки СУБД.
4. Безопасность пользовательского доступа.
5. Безопасная организация и работа с данными.

Практическое занятие 7. Безопасная настройка СУБД.

Лекция 8. Основные аспекты создания защищенных БД

1. Разработка комплексных методик обеспечения безопасности хранилищ данных на предприятии.
2. Оценка и классификация угроз и уязвимостей СУБД.
3. Разработка стандартных механизмов обеспечения безопасности.

Практическое занятие 8. Повышение защищенности базы данных.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторное занятие 1. Обнаружение уязвимостей ОС.	2
Лабораторное занятие 2. Антивирус.	2
Лабораторное занятие 3. Сетевой полигон.	2
Лабораторное занятие 4. Iptables.	2
Лабораторное занятие 5. Проверка web-ресурса на типичные уязвимости.	2
Лабораторное занятие 6. Сбор и анализ содержимого веб-ресурса.	2
Лабораторное занятие 7. Безопасная настройка СУБД.	2
Лабораторное занятие 8. Повышение защищенности базы данных.	2
Итого	16

5.3. Вопросы для самостоятельной работы студента.

Раздел 1. Средства защиты операционных систем

1. Хранения, генерации и оценки паролей.
2. Резервное копирования дисков.
3. Проверка состояния ОС.

Раздел 2. Средства сетевой защиты

1. Списки контроля доступа ACL сетевых устройств.
2. Настройка аппаратного межсетевого экрана
3. Аудит безопасности протокола SNMP.

Раздел 3. Защита web-ресурсов

1. Защита от запрещённого контента.
2. Особенности веб-сервера LAMP

Раздел 4. Защита баз данных.

1. Резервное копирование базы данных
2. Формат хранения баз данных

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. Результаты самостоятельной работы учитываются при оценке знаний на экзамене и 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. Способы обеспечения ИБ. Классификация средств защиты ОС.
2. Принципы проектирования защищенных систем.
3. Понятие защищенной операционной системы.
4. Административные меры защиты. Адекватная политика безопасности.
5. Методы работы антивирусов.
6. возможности современных антивирусов.
7. Классификация сетевых атак.
8. Архитектура системы обеспечения сетевой безопасности.
9. Виртуальные сети: назначение, виды, достоинства и недостатки.
10. Сетевые экраны: виды, принцип работы.
11. Программные и аппаратные сетевые экраны.
12. Настройка сетевого экран Netfilter.
13. Когда необходимо создавать резервную копию?
14. Как защитить контент от утечки?
15. Как проверить допустимость отправляемых пользователем данных?
16. Как защититься от инъекций вредоносного кода?
17. Опишите способы хранения и защиты файлов баз данных.
18. Какие права пользователей учитываются в базах данных?
19. Способы защиты удалённого доступа к СУБД.

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.	Тони Хаулет Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям [Электронный ресурс] : учебное пособие / Хаулет Тони. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 608 c. — 978-5-4487-0065-1. — Режим доступа: http://www.iprbookshop.ru/67392.html
2.	Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 192 с. — Режим доступа: https://e.lanbook.com/book/63241. — Загл. с экрана.

8.2. Рекомендуемая дополнительная литература

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

№ п/п	Наименование
1.	Алексеев В.А. Маршрутизация и защита сетевого трафика в сетях TCP/IP [Электронный ресурс] : методические указания к проведению лабораторных работ по курсу «Сетевые технологии» / В.А. Алексеев. — Электрон. текстовые данные. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2013. — 35 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/55104.html
2.	Веселкова Т.В. Эффективная эксплуатация сайта [Электронный ресурс] : практическое пособие / Т.В. Веселкова, А.С. Кабанов. — Электрон. текстовые данные. — М. : Дашков и К, Ай Пи Эр Медиа, 2011. — 176 c. — 978-5-394-01093-4. — Режим доступа: http://www.iprbookshop.ru/741.html
3.	Стасышин В.М. Проектирование информационных систем и баз данных [Электронный ресурс]: учебное пособие/ Стасышин В.М.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 100 c.— Режим доступа: http://www.iprbookshop.ru/45001.html.— ЭБС «IPRbooks»

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 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».

Учебная аудитория для лабораторных занятий в области защищенных автоматизированных систем, оснащена аппаратно-программными средствами управления доступом к данным, шифрования, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, источниками

бесперебойного и аварийного питания, средствами контроля и управления доступом в помещения, охранной и пожарной сигнализацией, климатическим контролем.

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.