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
«Управление информационной безопасностью»

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

Дисциплина направлена на изучение комплексного подхода к обеспечению информационной безопасности в организациях и состоит в изучении способов управления методами и средствами защиты информации, а так же приемов их интеграции в инфраструктуру предприятия.

Основными задачами дисциплины являются:

- контроль реализации политики информационной безопасности;
- организационно-методическое обеспечение информационной безопасности автоматизированных систем.

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

Дисциплина «Управление информационной безопасностью» относится к числу дисциплин базовой части профессионального цикла. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Системное программное обеспечение», «Безопасность операционных систем», «Основы информационной безопасности».

Дисциплина является предшествующей для дисциплин: «Безопасность сетей ЭВМ» и написания выпускной квалификационной работы.

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 участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

– способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

– способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

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

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

знать:

– устройство системы управления информационной безопасностью автоматизированной системы (З1);

– нормы и основные положения лучших практик в области информационной безопасности (З2);

– принципы, состав и структуру политик информационной безопасности (З3);

– теоретические, нормативные, организационные и технические способы обеспечения информационной безопасности (З4);

– принципы и способы управления информационной безопасностью (З5);

– основные нормативные правовые акты в области информационной безопасности (З6);

уметь:

– управлять процессами обеспечения информационной безопасностью (У1);

– проводить сравнение системы управления информационной безопасностью с требованиями стандартов (У2);

– разрабатывать политику информационной безопасности (У3);

– формировать комплексную систему защиты безопасности организации (У4);

– применять методы и средства для управления информационной безопасностью (У5);

– находить, классифицировать и интерпретировать нормативно-правовые акты в области информационной безопасности (У6);

владеть:

– стандартизированными методиками построения системы управления информационной безопасностью автоматизированной системы (Н1);

– навыками составления и аргументирования предложений по управлению информационной безопасностью (Н2);

– реализации положений политики информационной безопасности (Н3);

– способами администрирования средств защиты информации (Н4);

– навыками обеспечения непрерывной работы системы управления информационной безопасностью (Н5);

– навыками выполнения требований нормативно-правовых актов (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 (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, 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. Планирование СУИБ.	ПК-27, ПК-28	З4, З5,У4, У5
Тема 1.1. Архитектура системы управления информационной безопасностью (СУИБ).		
Тема 1.2. Политика безопасности СУИБ.		
Тема 1.3. Оценка рисков ИБ.		
Раздел 2. Реализация СУИБ.	ПК-12, ПК-19, ОПК-6, ПК-22	З1, З2, З3, У1, У2, У3
Тема 2.1. Технические меры обеспечения ИБ.		
Тема 2.2. Организационно-режимные меры обеспечения ИБ.		
Раздел 3. Тестирование СУИБ.	ПК-12, ПК-19, ОПК-6, ПК-22	З1, З2, З3, Н1, Н2, Н3
Тема 3.1. Проверка ИБ.		
Раздел 4. Совершенствование СУИБ.	ПК-12, ПК-19, ОПК-6, ПК-22, ПК-27, ПК-28	З3, З4, З5, Н3, Н4, Н5, Н6
Тема 4.1. Оценка СУИБ.		
Тема 4.2. Сопровождение СУИБ.		

Зачет	ПК-12, ПК-19, ОПК-6, ПК-22, ПК-27, ПК-28	З1-З6, У1-У5, Н1-Н6

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	КСР			
Раздел 1. Планирование СУИБ.							
Тема 1.1. Архитектура системы управления информационной безопасностью (СУИБ).	10	4	4		2	2	
Тема 1.2. Политика безопасности СУИБ.	14	4	4		6	2	
Тема 1.3. Оценка рисков ИБ.	20	6	6		8	2	
Раздел 2. Реализация СУИБ.							
Тема 2.1. Технические меры обеспечения ИБ.	14	4	4		6	2	
Тема 2.2. Организационно-режимные меры обеспечения ИБ.	14	4	4		6	2	
Раздел 3. Тестирование СУИБ.							
Тема 3.1. Проверка ИБ.	11	4	2		5	2	
Раздел 4. Совершенствование СУИБ.							
Тема 4.1. Оценка СУИБ.	16	4	8		4	2	
Тема 4.2. Сопровождение СУИБ.	5	2			3	2	
Зачет	4			2	2		
Итого	108 3 з.е.	32	32	2	42	16	0

5. Содержание разделов дисциплины

5.1. Лекции

Раздел 1. Планирование СУИБ

Тема 1.1. Архитектура системы управления информационной безопасностью (СУИБ).

Лекция 1. Модель организации.

1. Модели организации и бизнес-процессов.
2. Требования и приоритеты ИБ.
3. Структура СУИБ.

Лекция 2. Границы организации

1. Физические и организационные границы организации.
2. Область инфраструктуры организации.
3. Определение области действия СУИБ.

Тема 1.2. Политика безопасности СУИБ.

Лекция 3. Разработка политики СУИБ.

1. Цели и сценарии использования СУИБ.
2. Принципы безопасности.
3. План построения СУИБ.

Лекция 7. План непрерывности.

1. Анализ влияния на бизнес (BIA).
1. Способы реагирования и восстановления бизнес-процессов.
2. Планирование мер непрерывности.

Тема 1.3. Оценка рисков ИБ.

Лекция 4. Анализ требований.

1. Категорирование активов.
2. Оценка активов.
3. Критерии оценки риска.

Лекция 5. Анализ рисков.

1. Модели угроз и уязвимостей.
2. Определение вероятностей инцидентов и величин ущерба.

Лекция 6. Управление рисками.
1. Категорирование рисков.
2. Способы обработки рисков.

Раздел 2. Реализация СУИБ

Тема 2.1. Технические меры обеспечения ИБ.

Лекция 7. Средства защиты информации.
1. Классификация средств защиты информации.
2. Выполнение требований ИБ.
3. Выбор средств защиты информации.

Лекция 8. Средства администрирования СУИБ.
1. Средства инвентаризации и учета.
2. Средства централизованного управления СЗИ.
3. Средства обнаружения и предотвращения инцидентов.

Тема 2.2. Организационно-режимные меры обеспечения ИБ.

Лекция 9. Управление персоналом.
1. Распределение ролей и ответственности сотрудников.
2. Взаимодействие с внешней средой.
3. Обучение сотрудников.

Лекция 10. Управление инфраструктурой организации.
1. Правила использования инфраструктурой организации.
2. Правила применения средств защиты информации.
3. Правила изменения инфраструктуры организации.

Раздел 3. Тестирование СУИБ

Тема 3.1. Проверка ИБ.

Лекция 12. Мониторинг ИБ.
1. Показатели измерения.
2. Категорирование событий.
3. Планирование проверок.

Лекция 13. Аудит СУИБ.
1. Стандарты оценки СУИБ.
2. Процедура оценки СУИБ.
3. Документирование СУИБ.

Раздел 4. Совершенствование СУИБ

Тема 4.1. Оценка СУИБ.

Лекция 14. Зрелость СУИБ.
1. Выявление недостатков СУИБ.
2. Модели оценки зрелости.
3. Оценка зрелости процессов обеспечения информационной безопасности.

Лекция 15. Сертификация СУИБ.
1. Международные стандарты в области информационной безопасности.
2. Требования к сертификации.
3. Процедура сертификации.

Тема 4.2. Сопровождение СУИБ.

Лекция 16. Сопровождение СУИБ.
1. Жизненный цикл СУИБ.
2. Оценка текущего состояния.
3. Реагирование на появление новых угроз.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторная работа 1. Построение модели предприятия.	2
Лабораторная работа 2. Определение области действия СУИБ.	2
Лабораторная работа 3. Разработка политики СУИБ.	2
Лабораторная работа 4. Составление плана непрерывности.	2
Лабораторная работа 5. Оценка рисков ИБ.	6
Лабораторная работа 6. Технические меры обеспечения ИБ.	4
Лабораторная работа 7. Организационно-режимные меры обеспечения ИБ.	4
Лабораторная работа 8. Составление плана мониторинга.	2
Лабораторная работа 9. Моделирование атак злоумышленника.	4
Лабораторная работа 10. Проведение аудита СУИБ.	4
Итого	32

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

Раздел 1. Планирование СУИБ.
1. Модель предприятия
2. Политика безопасности

Раздел 2. Реализация СУИБ.
1. Средства защиты
2. Средства контроля
3. План непрерывности бизнес процессов ИС.

Раздел 3. Тестирование СУИБ.
1. Идентификация уязвимостей и угроз
2. Оценка рисков
3. Тестирование и оценка реакции на инциденты.

Раздел 4. Совершенствование СУИБ.
1. Класс защищенности
2. Показатель защищенности от несанкционированного доступа
3. Класс доверия

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, частично-поисковой, репродуктивной, творческой и пр.).

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.;

– 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: аннотирование и конспектирование литературы по теме, составление вопросов и тестов к теме, подготовка к лабораторным работам, разработка проекта.

Формами контроля самостоятельной работы выступают: проверка письменных отчётов по результатам выполненных заданий и лабораторных работ, защита проектной 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 преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Требования СУИБ и политика безопасности
2. Методы анализа и оценки риска
3. Риск-менеджмент
4. Характеристики средств защиты
5. Анализ влияния на бизнес (BusinessImpactAnalysis)
6. Порядок расследования инцидентов
7. Требования к проведению аудита
8. Модель предприятия.
9. Цели и принципы, область действия ИБ
10. Стандарты и требования ИБ.
11. Средства защиты и управления, правила безопасности
12. Регламенты применения защитных мер
13. План непрерывности: процедуры, средства, контроль.
14. Требования соответствия ISO/IEC 27001.
15. Показатели и методы измерения (ISO/IEC 27004. Измерения)
16. Достоинства и недостатки организационно-режимных мер.
17. Проект и план ИС.
18. Концепция СУИБ.
19. Что входит в ядро (минимальный набор) политики безопасности.
20. Виды правил безопасности ISO/IEC 27002.
21. Статистика нарушений ИБ персоналом.
22. Что нужно для проведения аудита СУИБ?

23. Этика службы безопасности.
24. Права и ограничения службы безопасности.
25. Переход от проекта СМИБ к плану его построения.
26. Способы обеспечения ИБ?
27. ГОСТ Р ИСО/МЭК 27000.
28. Жизненный цикл СУИБ.
29. Host-based Intrusion Prevention System(HIPS).
30. Data Leak Prevention(DLP).
31. Мониторинг и аудит.
32. Классификация средств защиты информации.

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.

Оценивание результатов зачета осуществляется в соответствии с полнотой и качеством выполнения задания на работу, качеством защиты работы (ответы на вопросы, и др.). Оценка работы отражает уровень сформированности соответствующих компетенций.

– «отлично» - работа выполнена в соответствии с утвержденным планом и заданием, полностью раскрыто содержание каждого вопроса; студентом сформулированы собственные аргументированные выводы по теме работы; оформление работы соответствует предъявляемым требованиям; при защите работы обучающийся демонстрирует свободное владение материалом и верно отвечает на поставленные вопросы;

– «хорошо» - работа выполнена в соответствии с утвержденным планом и заданием; полностью раскрыто содержание каждого вопроса; имеются незначительные замечания к оформлению работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает на ряд поставленных вопросов не в достаточно полном объеме;

– «удовлетворительно» - работа выполнена в соответствии с утвержденным планом и заданием, но не полностью раскрыто содержание каждого вопроса; обучающимся не сделаны собственные выводы по теме работы; допущены существенные недостатки в оформлении работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает не на все поставленные вопросы, либо не в достаточно полном объеме;

– «неудовлетворительно» - если работа не выполнена в соответствии с утвержденным планом и заданием, не раскрыто содержание каждого вопроса; обучающимся не сделаны выводы по теме работы, имеются существенные недостатки в оформлении работы; при защите работы обучающийся не демонстрирует владение материалом, не отвечает на поставленные вопросы.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания и лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно». Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания и лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

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.	Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 c. Режим доступа: http://www.iprbookshop.ru/52182.html
2.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.

8.2. Рекомендуемая дополнительная литература

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

№ п/п	Наименование
1.	Астахов А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 312 c. — 978-5-4488-0079-5. — Режим доступа: http://www.iprbookshop.ru/63803.html
2.	Системы защиты информации в ведущих зарубежных странах [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков [и др.]. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 224 c. — 978-89838-488-3. — Режим доступа: http://www.iprbookshop.ru/7007.html
3.	Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 c. Режим доступа: http://www.iprbookshop.ru/6991.html
4.	Заляжных В.А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем [Электронный ресурс] / В.А. Заляжных, А.В. Гирик. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 139 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/65733.html

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
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Arch linux	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community
4.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
5.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
6.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
7.	360 Total Security	https://www.360totalsecurity.com/ru/

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 +	

3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
3.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
4.	Xgu.ru.	http://xgu.ru/wiki/
5.	Российская Государственная Библиотека	http://www.rsl.ru
6.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
7.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
8.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
9.	Научная электронная библиотека	http://elibrary.ru
10.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
11.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.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».

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 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. 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: фронтальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

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 №		