УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.Е. Федоров
«25» июня 2021 г.

Рабочая программа дисциплины (модуля)*
Основы информационной безопасности

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

специализация № 4 "Безопасность автоматизированных систем критически важных объектов"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2021

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2021 г.

Рабочая программа дисциплины (модуля) принята:
Ученым советом физического факультета

Протокол заседания № 11 от «27» мая 2021 г.

Председатель Ученого совета физического факультета _____ Д.А. Захарьевич

Секретарь Ученого совета физического факультета _____ М.А. Эбель

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой компьютерной безопасности и прикладной алгебры.

Протокол заседания № 10 от «04» 06 2021 г.

Заведующий кафедрой _____ А.Н. Ручай

Автор (составитель):
Зав.кафедрой, канд.физ.-мат. наук, доцент _____ А.Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления.

Задачи дисциплины:

– изучение основных аспектов обеспечения информационной безопасности государства;

– изучение методологии создания систем защиты информации;

– изучение процессов сбора, передачи и накопления информации;

– изучение основных элементов теории компьютерной безопасности;

– изучение математических основ моделей безопасности;

– изучение вопросов оценки защищенности и обеспечения безопасности компьютерных систем.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-1.1. Имеет представление об объективных потребностях личности, общества и государства в информационных технологиях и информационной безопасности.

ОПК-1.2. Обладает навыками оценивать роль и значение информации, информационных технологий и информационной безопасности в современном обществе.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.20

2.1 Требования к предварительной подготовке обучающегося:

Правоведение

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Организационное и правовое обеспечение информационной безопасности

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

Знать:

Для достижения индикатора ОПК-1.1: Знать основные термины по проблематике информационной безопасности; цели, задачи, принципы и основные направления обеспечения информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; содержание информационной войны, методы и средства ее ведения; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

Уметь:

Для достижения индикатора ОПК-1.2: Уметь пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

Владеть:

Для достижения индикатора ОПК-1.2: Владеть навыками использования профессиональной терминологии в области информационной безопасности.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
3.1.2	основы государственной информационной политики, стратегию развития информационного общества в России.
3.2	**Уметь:**
3.2.1	пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;

3.2.2	классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.
3.3	**Владеть:**
3.3.1	навыками использования профессиональной терминологии в области информационной безопасности;
3.3.2	навыками построения систем защиты информации.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану: 144 в том числе: аудиторные занятия: 54 самостоятельная работа: 54 часов на контроль: 36	Виды контроля в семестрах: экзамены 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации			
1.1	Понятие национальной безопасности Российской Федерации. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
1.2	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
1.3	Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче зачета. /Ср/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 2. Основы государственной политики Российской Федерации в области информационной безопасности			
2.1	Национальные интересы Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.2	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Организационная система обеспечения информационной безопасности Российской Федерации. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.3	Национальные интересы Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности Российской Федерации. Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Организационная система обеспечения информационной безопасности Российской Федерации. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.4	Структура законодательства Российской Федерации в сфере обеспечения информационной безопасности. Уголовно- процессуальная характеристика компьютерных преступлений. /Лек/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.5	Структура законодательства Российской Федерации в сфере обеспечения информационной безопасности. Уголовно- процессуальная характеристика компьютерных преступлений. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.6	Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче зачета. /Ср/	7	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 3. Информационное противоборство, методы и средства его осуществления			

3.1	Понятие информационного противоборства. Информационные войны, методы и средства их ведения. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
3.2	Информационное оружие, его классификация и возможности. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
3.3	Понятие информационного противоборства. Информационные войны, методы и средства их ведения. Информационное оружие, его классификация и возможности. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
3.4	Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче зачета. /Ср/	7	14	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 4. Виды защищаемой информации ограниченного доступа.			
4.1	Виды защищаемой информации ограниченного доступа. Государственная тайна. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.2	Виды защищаемой информации ограниченного доступа. Коммерческая тайна. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.3	Виды защищаемой информации ограниченного доступа. Персональные данные. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.4	Виды защищаемой информации ограниченного доступа. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.5	Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче зачета. /Ср/	7	15	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 5. Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры			
5.1	Стратегические цели и основные направления. принципы и общие методы обеспечения обеспечения информационной безопасности. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.2	Автоматизированная информационная система как объект защиты. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.3	Стратегические цели и основные направления. принципы и общие методы обеспечения обеспечения информационной безопасности. Автоматизированная информационная система как объект защиты. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.4	Понятие комплексного обеспечения информационной безопасности. Политика обеспечения информационной безопасности предприятия (организации). /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.5	Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.6	Понятие комплексного обеспечения информационной безопасности. Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем. /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

5.7	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.8	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.9	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общая характеристика методов и средств защиты информации в автоматизированных информационных системах /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.10	Задачи и организационная структура подразделения обеспечения информационной безопасности предприятия (организации) /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.11	Задачи и организационная структура подразделения обеспечения информационной безопасности предприятия (организации). /Пр/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.12	Проработка лекционного материала и литературы. Подготовка выступлений на практических занятиях. Подготовка к сдаче зачета. /Ср/	7	15	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Устный опрос на практических занятиях.
Итоговый тест (Зачет).

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для устного опроса на практических занятиях.

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы, угрозы национальной безопасности Российской Федерации.
3. Понятие информационной безопасности, основные составляющие национальных интересов в информационной сфере.
4. Факторы, способствующие повышению роли информационной безопасности в системе национальной безопасности.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности.
6. Компетенция федеральных и региональных органов государственной власти в сфере обеспечения информационной безопасности.
7. Правовая и организационная система обеспечения информационной безопасности Челябинской области.
8. Интересы личности общества и государства в информационной сфере.
9. Характеристика основных видов угроз информационной безопасности.
10. Принципы обеспечения информационной безопасности.
11. Понятие информационной войны, цели и средства её ведения.
12. Основные компоненты информационной войны.
13. Понятие информационного оружия.
14. Классификация информационного оружия.
15. Понятие и свойства информации.
16. Виды защищаемой информации.
17. Обязанности обладателя по обеспечению защиты информации.
18. Режим конфиденциальности информации и порядок его введения, на примере режима коммерческой тайны
19. Конституция Российской Федерации о правах и обязанностях граждан в информационной сфере.
20. Структура законодательства в сфере обеспечения информационной безопасности.
21. Перечень статей УК РФ, предусматривающих уголовную ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
22. Федеральные органы, осуществляющие контрольные функции в сфере обеспечения информационной безопасности.
23. .Административная ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
24. Понятие автоматизированной информационной системы.
25. Виды угроз безопасности информационных и телекоммуникационных систем.
26. Основные каналы утечки защищаемой информации.
27. Внешние источники угроз безопасности информационных систем.
28. Внутренние источники угроз безопасности информационных систем.
29. Элементы обстановки на объекте защиты, процедура оценки обстановки.
30. Критерии оценки защищенности автоматизированных информационных систем.
31. Структура службы безопасности предприятия.
32. Основные этапы создания службы безопасности предприятия.

33. Основные задачи, решаемые подразделением обеспечения информационной безопасности.
34. Обязанности руководителя подразделения информационной безопасности.
35. Обязанности системного администратора (администратора безопасности).
36. Обязанности пользователя автоматизированной информационной системы по обеспечению информационной безопасности.
37. Понятие и основные виды терроризма.
38. Роль информационных технологий в управлении критически важными объектами государства.
39. Способы совершения террористического акта в отношении объектов информационной инфраструктуры.
40. Использование террористическими организациями сети Интернет.
41. Понятие объекта, критически важного для обеспечения национальной безопасности государства, классификация критически важных объектов.
42. Угрозы уязвимости информационной инфраструктуры критически важных объектов.
43. Негативные последствия нарушения функционирования систем управления критически важных объектов.
44. Определение требований к защите информации в АСУ ТП.
45. Разработка и внедрение защиты АСУ ТП.
46. Обеспечение защиты информации в ходе эксплуатации АСУ ТП.

База тестовых вопросов

Пример:

1 В каком году утверждена действующая Доктрина информационной безопасности РФ: а) 2010 г.; б) 2016 г.;в) 2015 г.

2 Сколько групп национальных интересов в информационной сфере сформулировано в действующей Доктрине информационной безопасности РФ: а) 3; б) 4;в) 5.

3 Какая группа национальных интересов в информационной сфере отсутствовала в предыдущей Доктрине информационной безопасности РФ: а) содействие формированию системы международной информационной безопасности; б) доведение до российской и международной общественности достоверной информации о государственной политике РФ; в) обеспечение и защита прав и свобод человека и гражданина в информационной сфере.

4 Фраза «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» содержится в: а) статье Конституции РФ; б) статье Уголовного Кодекса РФ;в) статье Гражданского Кодекса РФ.

5 Какая статья Конституции РФ разрешает на законном основании ограничивать права и свободы граждан РФ в информационной сфере:а) статья 23; б) статья 33; в) статья 55.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Теоретические вопросы к зачету.

1. Понятие национальной безопасности. Основные угрозы национальной безопасности России.
2. Интересы личности, общества и государства в информационной сфере. Понятие информационной безопасности
3. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
4. Виды угроз информационной безопасности Российской Федерации.
5. Источники угроз информационной безопасности Российской Федерации.
6. Информационная безопасность и информационное противоборство.
7. Понятие информационной войны, цели и средства её ведения
8. Информационное оружие, его классификация и возможности.
9. Понятие кибертерроризма
10. Основные направления обеспечения информационной безопасности объектов информационной инфраструктуры государства
11. Общие принципы и методы обеспечения информационной безопасности Российской Федерации.
12. Конституция РФ о правах и обязанностях граждан в информационной сфере
13. Виды защищаемой информации
14. Правовой режим защиты государственной тайны.
15. Правовой режим защиты коммерческой тайны.
16. Правовой режим зашиты персональных данных.
17. Уголовная ответственность за компьютерные преступления.
18. Понятие и виды административной ответственности за нарушение требований информационной безопасности.
19. Методы и средства обеспечения безопасности компьютерных систем.
20. Обязанности обладателя конфиденциальной информации по ее защите.
21. Политика обеспечения информационной безопасности.
22. Конфиденциальные документы: состав, сроки, реквизиты. Угрозы конфиденциальному документу.

23. Контроль и надзор в сфере обеспечения информационной безопасности.
24. Понятие и уровни защищенности автоматизированных информационных систем (АИС).
25. Основные требования по защите АИС
26. Состав и содержание организационных и технических мер по защите АИС
27. Процедура оценки обстановки на объекте защиты
28. Базовые и частные модели угроз безопасности АИС
29. Методика оценки актуальности угроз безопасности АИС.
30. Этапы создания и структура службы безопасности предприятия.
31. Задачи подразделения информационной безопасности предприятия.
32. Должностные обязанности руководителя подразделения информационной безопасности.
33. Должностные обязанности администратора безопасности АИС.
34. Обязанности пользователя АИС по обеспечению информационной безопасности.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
В течении семестра на практических занятиях проводится регулярный устный опрос. По учебному плану предусмотрены 18 академических часов, или 9 практических занятий.
Набранные баллы на практических занятиях являются допуском к зачету.
Максимальный балл за один устный опрос – 10 баллов.
Максимальный балл за все устные опросы – 90 баллов.
Более 50 баллов, набранных в семестре, – допуск к промежуточной аттестации, менее 50 – недопуск.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Устный опрос на практических занятиях	9x10=90
Итого:		
Допуск к промежуточной аттестации		Более 50
Недопуск к промежуточной аттестации		Менее 50
2	Зачет	100
Итого		100

Критерии оценивания устного опроса на практических занятиях
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-4 балла - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

Критерии оценивания теста на зачете
Тест формируется в системе электронного обучения MOODLE.
Максимальный балл за тест – 100 баллов.
Отлично/зачтено/91-100 баллов
Хорошо/зачтено/70-90 баллов
Удовлетворительно/зачтено/50-69 баллов
Неудовлетворительно/не зачтено/0-49 баллов

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:
0-49 баллов - не зачтено;
50-100 баллов - зачтено.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Рытенкова О.	Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=230502)	Москва : ГРОТЕК, 2014	ЭБС
Л1.2	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (http://znanium.com/catalog/document?id=364624)	Москва : Издательство "ФОРУМ", 2021	ЭБС
Л1.3	Мельников В.П., под ред., Куприянов А.И.	Информационная безопасность: учебник (https://www.book.ru/book/939292)	Москва : КноРус, 2021	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Кармановский Н. С., Михайличенко О. В., Прохожев Н. Н.	Организационно-правовое и методическое обеспечение информационной безопасности (https://e.lanbook.com/book/91449)	Санкт- Петербург : НИУ ИТМО, 2016	ЭБС
Л2.2	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций: учебное пособие (https://biblioclub.ru/index.php?page=book&id=362895)	Москва, Берлин : Директ-Медиа, 2015	ЭБС
Л2.3		Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: практикум (https://biblioclub.ru/index.php?page=book&id=458012)	Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Официальный интернет-портал правовой информации. Государственная система правовой информации http://pravo.gov.ru БД «Информационно-правовая система «Законодательство России» http://pravo.gov.ru/proxy/ips/?start_search&fattrib=1
Э2	Кодексы и законы РФ - правовая справочно-консультационная система http://kodeks.systecs.ru

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

Adobe Reader

LMS Moodle

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронныйресурс] : база данных / Челяб. гос.ун-т. – Челябинск, 1992 .

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион.центр правовой информ. Информправо.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа студента.
На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.

На практических занятиях рассматриваются основные понятия, принципы, уровни и угрозы информационной безопасности. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на практических и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, видеохостинг YouYube, форумы, электронная почта и др.).

Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.

Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.

2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.

3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.

Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.