УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.Е. Федоров
«_25_» _____06_____ 2021 г.

Рабочая программа дисциплины (модуля)*
Информационная безопасность и защита информации

Направление подготовки (специальность)

02.03.01 Математика и компьютерные науки

Направленность (профиль)

Топологические и аналитические методы исследования математических моделей

Присваиваемая квалификация (степень)

бакалавр

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 математического факультета

Протокол заседания № 13 от «24» 06 2021 г.

Председатель Ученого совета
математического факультета _____ Е.А. Сбродова

Секретарь Ученого совета
математического факультета _____ С.А. Никитина

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 обучающихся к деятельности, связанной с комплексным анализом возможных угроз и с постановкой конкретных задач заданной степени сложности в рамках обеспечения информационной безопасности, а также содействие развитию системного мышления.

Задачи дисциплины:

- изучение основных аспектов обеспечения информационной безопасности государства;
- изучение методологии создания систем защиты 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:

УК-2.1. Демонстрирует знание теоретических основ принятия решений в сфере управления проектами.

УК-2.2. Выявляет и анализирует различные способы решения задач в рамках цели проекта и аргументирует их выбор.

УК-2.3. Демонстрирует способность проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.

УК-10.1. Понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике.

УК-10.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.17

2.1 Требования к предварительной подготовке обучающегося:

Изучение данной дисциплины базируется на следующих курсах общей и специальной подготовки:

Современные технологии поиска и обработки информации

Информатика

Правоведение

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

Освоение данной дисциплины является предшествующим для дисциплин, связанных с разработкой проектов и дисциплин, связанных с защитой информации.

Управление IT-проектами

Теория передачи информации (научный семинар)

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

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Знать:

- действующие правовые нормы и ограничения;
- имеющиеся в организации ресурсы для решения поставленных задач.

Уметь:

- грамотно формулировать цель проекта;
- исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели;
- использовать организационно-правовые методы обеспечения информационной безопасности;
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

Владеть:

- навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели;

- навыками использования профессиональной терминологии в области информационной безопасности;
- профессиональной терминологией в области информационной безопасности;
- навыками математического моделирования угроз безопасности автоматизированных информационных систем.

УК-10: Способен формировать нетерпимое отношение к коррупционному поведению
Знать:
- базовые принципы функционирования экономики и экономического развития; - основные термины и понятия гражданского права, используемые в антикоррупционном законодательстве; - действующее антикоррупционное законодательство и практику его применения.
Уметь:
- правильно толковать гражданско-правовые термины, используемые в антикоррупционном законодательстве; - давать оценку коррупционному поведению и применять на практике антикоррупционное законодательство.
Владеть:
- навыками правильного толкования гражданско-правовых терминов, используемых в антикоррупционном законодательстве; - навыками применения на практике антикоррупционного законодательства, правовой квалификацией коррупционного поведения и его пресечения.

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;
3.1.3	– 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 защищаемую информацию по видам тайны и степеням конфиденциальности.
3.3	**Владеть:**
3.3.1	– использования профессиональной терминологии в области информационной безопасности;
3.3.2	– построения систем защиты информации.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**2 ЗЕТ**
Часов по учебному плану : 72 в том числе : аудиторные занятия : 36 самостоятельная работа : 36 :	Виды контроля в семестрах: зачеты 5

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. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
1.2	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
1.3	Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
	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/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
2.2	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
2.3	Организационная система обеспечения информационной безопасности Российской Федерации. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
2.4	Структура законодательства Российской Федерации в сфере обеспечения информационной безопасности. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
2.5	Уголовная и административная ответственность за правонарушения в информационной сфере. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
2.6	Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
	Раздел 3. Информационное противоборство, методы и средства его осуществления			
3.1	Понятие информационного противоборства. Информационные войны, методы и средства их ведения. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
3.2	Информационное оружие, его классификация и возможности. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
3.3	Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
	Раздел 4. Виды защищаемой информации ограниченного доступа.			
4.1	Государственная тайна. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
4.2	Коммерческая тайна. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
4.3	Персональные данные. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
4.4	Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
	Раздел 5. Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры			
5.1	Принципы и основные направления обеспечения информационной безопасности. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

5.2	Автоматизированная информационная система как объект защиты. Модели и стратегии обеспечения информационной безопасности автоматизированных информационных. систем. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.3	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.4	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.5	Понятие комплексного обеспечения информационной безопасности. Политика обеспечения информационной безопасности предприятия (организации). /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.6	Задачи и организационная структура подразделения обеспечения информационной безопасности предприятия (организации). /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.7	Проработка лекционного материала и литературы. Подготовка к тестированию, проверочной работе и сдаче зачета. /Ср/	5	12	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Итоговый тест (Зачет)

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для самостоятельной работы.
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.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Примеры теоретических вопросов к зачету
1. Административная ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
2. Базовые и частные модели угроз безопасности АИС
3. Виды защищаемой информации
4. Виды угроз безопасности информационных и телекоммуникационных систем.
5. Виды угроз информационной безопасности Российской Федерации.
6. Внешние источники угроз безопасности информационных систем.
7. Внутренние источники угроз безопасности информационных систем.
8. Должностные обязанности администратора безопасности АИС.
9. Должностные обязанности руководителя подразделения информационной безопасности.
10. Задачи подразделения информационной безопасности предприятия.
11. Интересы личности общества и государства в информационной сфере.
12. Интересы личности, общества и государства в информационной сфере. Понятие информационной безопасности
13. Информационная безопасность и информационное противоборство.
14. Информационное оружие, его классификация и возможности.
15. Использование террористическими организациями сети Интернет.
16. Источники угроз информационной безопасности Российской Федерации.
17. Классификация информационного оружия.
18. Компетенция федеральных и региональных органов государственной власти в сфере обеспечения информационной безопасности.
19. Конституция Российской Федерации о правах и обязанностях граждан в информационной сфере.
20. Конституция РФ о правах и обязанностях граждан в информационной сфере
21. Контроль и надзор в сфере обеспечения информационной безопасности.
22. Конфиденциальные документы: состав, сроки, реквизиты. Угрозы конфиденциальному документу.
23. Критерии оценки защищенности автоматизированных информационных систем.
24. Методика оценки актуальности угроз безопасности АИС.
25. Методы и средства обеспечения безопасности компьютерных систем.
26. Национальные интересы, угрозы национальной безопасности Российской Федерации.
27. Негативные последствия нарушения функционирования систем управления критически важных объектов.
28. Обеспечение защиты информации в ходе эксплуатации АСУ ТП.
29. Общие принципы и методы обеспечения информационной безопасности Российской Федерации.
30. Обязанности обладателя конфиденциальной информации по ее защите.
31. Обязанности обладателя по обеспечению защиты информации.
32. Обязанности пользователя автоматизированной информационной системы по обеспечению информационной безопасности.
33. Обязанности пользователя АИС по обеспечению информационной безопасности.
34. Обязанности руководителя подразделения информационной безопасности.
35. Обязанности системного администратора (администратора безопасности).
36. Определение требований к защите информации в АСУ ТП.
37. Основные положения государственной политики и организационная основа обеспечения информационной безопасности.
38. Основные задачи, решаемые подразделением обеспечения информационной безопасности.
39. Основные каналы утечки защищаемой информации.

40. Основные компоненты информационной войны.
41. Основные направления обеспечения информационной безопасности объектов информационной инфраструктуры государства
42. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
43. Основные требования по защите АИС.
44. Основные угрозы национальной безопасности России.
45. Основные этапы создания службы безопасности предприятия.
46. Перечень статей УК РФ, предусматривающих уголовную ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
47. Политика обеспечения информационной безопасности.
48. Понятие автоматизированной информационной системы.
49. Понятие и виды административной ответственности за нарушение требований информационной безопасности.
50. Понятие и основные виды терроризма.
51. Понятие и свойства информации.
52. Понятие и уровни защищенности автоматизированных информационных систем (АИС).
53. Понятие информационного оружия.
54. Понятие информационной безопасности, основные составляющие национальных интересов в информационной сфере.
55. Понятие информационной войны, цели и средства её ведения.
56. Понятие кибертерроризма
57. Понятие национальной безопасности Российской Федерации.
58. Понятие объекта, критически важного для обеспечения национальной безопасности государства, классификация критически важных объектов.
59. Правовая и организационная система обеспечения информационной безопасности Челябинской области.
60. Правовой режим зашиты персональных данных.
61. Правовой режим защиты государственной тайны.
62. Правовой режим защиты коммерческой тайны.
63. Принципы обеспечения информационной безопасности.
64. Процедура оценки обстановки на объекте защиты
65. Разработка и внедрение защиты АСУ ТП.
66. Режим конфиденциальности информации и порядок его введения, на примере режима коммерческой тайны
67. Роль информационных технологий в управлении критически важными объектами государства.
68. Состав и содержание организационных и технических мер по защите АИС
69. Способы совершения террористического акта в отношении объектов информационной инфраструктуры.
70. Структура законодательства в сфере обеспечения информационной безопасности.
71. Структура службы безопасности предприятия.
72. Уголовная ответственность за компьютерные преступления.
73. Угрозы уязвимости информационной инфраструктуры критически важных объектов.
74. Факторы, способствующие повышению роли информационной безопасности в системе национальной безопасности.
75. Федеральные органы, осуществляющие контрольные функции в сфере обеспечения информационной безопасности.
76. Характеристика основных видов угроз информационной безопасности.
77. Элементы обстановки на объекте защиты, процедура оценки обстановки.
78. Этапы создания и структура службы безопасности предприятия.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
Зачет проходит в виде теста в системе электронного обучения MOODLE.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Зачет	100
Итого		100

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/51-69 баллов
Неудовлетворительно/не зачтено/0-50 баллов

При подведении итогов учитываются результаты текущей аттестации.
0-50 баллов - не зачтено;
51-100 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
Л1.1	Рытенкова О.	Информационная безопасность: журнал (https://biblioclub.ru/index.php?page=book&id=230502)	Москва : ГРОТЕК, 2014	ЭБС
Л1.2	Мельников В.П., Куприянов А.И.	Информационная безопасность: учебник (https://www.book.ru/book/924214)	Москва : КноРус, 2018	ЭБС
Л1.3	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (http://znanium.com/catalog/document?id=353520)	Москва : Издательство "ФОРУМ", 2020	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 Раздел «Официальное опубликование правовых актов» в электронном виде» http://publication.pravo.gov.ru/
Э2	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
Э3	Кодексы и законы РФ - правовая справочно-консультационная система http://kodeks.systecs.ru

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

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 и самостоятельная работа студента.На лекционных занятиях преподаватель излагает основное содержание тем программы и тестирование по материалам предыдущей лекции. По окончании темы проводится проверочная работа. 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.
Студенту желательно проявлять активное участие на 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.