УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.Е. Федоров
«25» 06 2021 г.

Рабочая программа дисциплины (модуля)*
Методы и стандарты оценки защищенности компьютерных систем

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 1 "Анализ безопасности компьютерных систем"

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 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
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
6.1. Перечень видов оценочных средств
6.2. Типовые контрольные задания и иные материалы для текущей аттестации
6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
7.1. Рекомендуемая литература
7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение российских и зарубежных методов и стандартов оценки защищенности компьютерных систем и применение их на практике.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК 1.1.1 Знает принципы построения защищенных компьютерных систем и сетей; требования основных стандартов по оценке защищенности компьютерных систем и сетей.

ОПК 1.1.2 Умеет определять уровень защищенности и доверия программно-аппаратных средств защиты информации; классифицировать информационные системы по требованиям защиты информации; определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе; выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия; проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.31.05

2.1 Требования к предварительной подготовке обучающегося:

Информатика

Аппаратные средства вычислительной техники

Учебно-лабораторный практикум

Операционные системы

Теория информации

Модели безопасности компьютерных систем

Системы управления базами данных

Сети и системы передачи информации

Компьютерные сети

Основы построения защищенных компьютерных сетей

Защита программ и данных

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

Технологическая практика

Преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

ОПК-1.1: Способен проводить анализ защищенности и осуществлять поиск уязвимостей компьютерной системы

Знать:

– российские и зарубежные стандарты в области информационной безопасности;
– современные критерии и стандарты для анализа безопасности компьютерных систем.

Уметь:

– оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности;
– применять современные критерии и стандарты для анализа безопасности компьютерных систем.

Владеть:

– практическими навыками оценки защищенности на соответствие стандартам информационной безопасности ЦБ РФ в области информационных систем, функционирующих в финансовой сфере;
– практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– методы и стандарты оценки защищенности;

3.1.2	– российские и зарубежные стандарты в области информационной безопасности;
3.1.3	– методику разработки и применения модели угроз безопасности информации.
3.2	**Уметь:**
3.2.1	– разрабатывать модели угроз безопасности информационных систем;
3.2.2	– проводить оценку защищенности компьютерных систем согласно российским и зарубежным стандартам.
3.3	**Владеть:**
3.3.1	– практические навыки разработки модели угроз безопасности информации и проведение оценки защищенности компьютерных систем согласно стандартам информационной безопасности.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**5 ЗЕТ**
Часов по учебному плану : 180 в том числе : аудиторные занятия : 54 самостоятельная работа : 90 часов на контроль : 36	Виды контроля в семестрах: экзамены 10

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Оценка угроз информационной безопасности			
1.1	ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ. /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.2	МОДЕЛЬ НАРУШИТЕЛЯ ПО РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.3	Способы реализации угроз безопасности информации. /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.4	ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ. /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.5	Определение потенциала нарушителя. /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.6	Модель угроз безопасности информации. /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.7	Оценка угроз информационной безопасности. Актуальные угрозы. Способы реализации угроз ИБ. Действия по реализации угроз ИБ. /Пр/	10	9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.8	Разработка модели нарушителя /Ср/	10	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
1.9	Разработка модели угроз безопасности /Ср/	10	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
	Раздел 2. Стандарты оценки угроз информационной безопасности			
2.1	Стандарты информационной безопасности /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.2	Стандарты оценки защищенности /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

2.3	Методы и стандарты оценки защищенности информационных систем в банковской сфере /Лек/	10	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.4	Стандарты оценки угроз ИБ. /Пр/	10	9	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.5	Minimum Security Requirements for Federal Information and Information Systems /Ср/	10	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.6	МЕТОДИКА ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ. /Ср/	10	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.7	Российские стандарты информационной безопасности. /Ср/	10	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5
2.8	Банковские стандарты информационной безопасности /Ср/	10	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Устный опрос.
Самостоятельная работа.
Экзамен

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для устного опроса для текущей аттестации
1. Информация.
2. Информационная система.
3. Угроза безопасноси информации.
4. Опередлние области применения оценки угроз информационной безопасности.
5. Характеристика угрозы информационной безопасности.
6. Источники угроз безопасности и их классификация.
7. Факторы, обуславливающие техногенные угрозы безопасности информации.
8. Идентификация угрозы безопасности информации в информационной системе.
9. Мониторинг и переоценка угроз безопасности информации.
10. Определение угроз безопасности информации в информационной системе.
11. Нарушитель информационной безопасности.
12. Оценка возможностей нарушителей.
13. Типы нарушителей.
14. Мотивации реализации нарушителями угроз безопасности информации в информационной системе.
15. Связи нарушителей.
16. Нарушители с базовым (низким) потенциалом.
17. Нарушители с базовым повышенным (средним) потенциалом.
18. Нарушители с высоким потенциалом.
19. Модель нарушителя по реализации угроз безопасности информации.
20. Способы реализации угроз безопасности информации.
21. Действия по реализации угроз информационной безопасности.
22. Реализация преднамеренных угроз безопасности информации.
23. Условия определения способов реализации угроз безопасности информационной системы.
24. Актуальная угроза безопасности информации.
25. Показатель актуальности угрозы.
26. Вероятность реализации угрозы.
27. Вербальные градации показателя вероятности реализации угрозы.
28. Возможность реализации угрозы безопасности информации.
29. Показатели, характеризующие проектную защищенность информационной системы.
30. Уровень проектной защищенности.
31. Уровень защищенности в ходе эксплуатации информационной системы.
32. Возможность реализации угрозы безопасности информации.
33. Исходные данные об угрозах безопасности информации.
34. Условия определения способов реализации угроз безопасности информационной системы.
35. Оценка степени возможного ущерба от реализации угрозы безопасности информации.

36. Определение актуальных угроз безопасности информации в информационной системе.
37. Потенциал нарушителя.
38. Классификация и виды нарушителей информационной безопасности.
39. Определение потенциала нарушителя.
40. Параметры экспертной оценки.
41. Техническая компетентность нарушителя.
42. Возможности нарушителя по доступу к информационной системе.
43. Оснащенность нарушителя.
44. Оценка потенциала нарушителя.
45. Модель угроз безопасности информации.
46. Структура модели нарушителя.
47. Структура модели угроз безопасности.
48. Стандарты информационной безопасности.
49. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (1983).
50. Политика безопасности.
51. Классы безопасности.
52. Распределение функций безопасности по уровням модели OSI.
53. Стандарт ISO/IEC 15408.
54. Классы функциональных требований.
55. Международный стандарт ISO 17799.
56. Международные стандарты информационной безопасности.
57. Российские стандарты информационной безопасности.
58. Стандарты оценки защищенности.
59. Методы и стандарты оценки защищенности информационных систем в банковской сфере.
60. Minimum Security Requirements for Federal Information and Information Systems
61. Методика определения угроз безопасности информации в информационных системах.
62. Банковские стандарты информационной безопасности.
63. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

Перечень самостоятельных работ
1. Разработка модели нарушителя.
2. Разработка модели угроз безопасности.
3. Сравнение методического документа "Minimum Security Requirements for Federal Information and Information Systems" с российскими аналогами.
4. Применение методики определения угроз безопасности информации в информационных системах.
5. Применение российских стандартов информационной безопасности.
6. Применение банковских стандарты информационной безопасности.

Полные тексты самостоятельных работ и задания выложены на сетевом диске кафедры компьютерной безопасности и прикладной алгебры DC1\doc\.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к экзамену
1. Источники угроз безопасности и их классификация.
2. Определение угроз безопасности информации в информационной системе.
3. Нарушитель информационной безопасности.
4. Модель нарушителя по реализации угроз безопасности информации.
5. Способы реализации угроз безопасности информации.
6. Актуальная угроза безопасности информации.
7. Определение актуальных угроз безопасности информации в информационной системе.
8. Потенциал нарушителя.
9. Классификация и виды нарушителей информационной безопасности.
10. Определение потенциала нарушителя.
11. Модель угроз безопасности информации.
12. Структура модели нарушителя.
13. Структура модели угроз безопасности.
14. Стандарты информационной безопасности.
15. Стандарты оценки защищенности.
16. Методы и стандарты оценки защищенности информационных систем в банковской сфере
17. Minimum Security Requirements for Federal Information and Information Systems
18. Методика определения угроз безопасности информации в информационных системах.
19. Российские стандарты информационной безопасности.
20. Банковские стандарты информационной безопасности..

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
Допуском до проведения экзамена являются сданные студентом самостоятельные работы в течение семестра. Экзамен проводится в два этапа. На первом студент отвечает на два вопроса. На втором студент решает практическую задачу по оценке защищенности компьютерной системы. Продолжительность – 90 минут.

Сводная таблица рейтинга успеваемости

№	Вид оценочного средства	Максимальное кол-во баллов
1	Устный опрос	2x5=10
2	Самостоятельная работа	6x5=30
3	Экзамен (теоретический вопрос)	2x15=30
4	Экзамен (практическая задача)	30
Итого		100

Критерии оценки устного опроса
На каждый устный опрос студенту предоставляются пять вопросов из списка по выбору преподавателя.
Максимальный балл за устный опрос – 5 баллов.
Максимальный балл за устный опрос за семестр – 10 баллов.

Характеристики ответа	Баллы
Правильно даны все пять ответов	5
Правильно даны четыре ответа	4
Правильно даны три ответа	3
Правильно даны два ответа	2
Правильно дан один ответ	1
Нет правильных ответов	0

Критерии оценки самостоятельной работы
Максимальный балл за самостоятельную работу – 5 баллов.
Максимальный балл за самостоятельные работы за семестр – 30 баллов.
5 баллов – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
4 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
3 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
2 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
1 балл – при выполнении самостоятельной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.
0 баллов – не выполнена самостоятельная работа.

Критерии оценивания теоретического вопроса экзамена
Максимальный баллы за ответ на теоретический вопрос – 15 баллов.
Максимальный баллы за ответы на зачете – 30 баллов.
Отлично/зачтено/12-15 баллов - Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.
Хорошо/зачтено/ 8-11 баллов - Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе.
Удовлетворительно/зачтено/5-7 баллов - Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа.
Неудовлетворительно/не зачтено/0-4 балла - Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием

темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Критерии оценивания практической задачи экзамена
Максимальный баллы за практическую задачу/практическое задание – 30 баллов.
Отлично/зачтено/25-30 баллов - Студентом верно определены границы оценки защищенности компьютерной системы, верно выбрана и применена методика оценки.
Хорошо/зачтено/15-24 баллов - Студентом верно определены границы оценки защищенности компьютерной системы, выбрана и применена методика оценки с небольшими неточностями.
Удовлетворительно/зачтено/8-14 баллов - Студентом верно определены границы оценки защищенности компьютерной системы, не верно выбрана и применена методика оценки.
Неудовлетворительно/не зачтено/0-7 балла - Студентом подготовлен ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области.

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.
Для экзамена:
0-59 баллов – неудовлетворительно (2);
60-74 баллов – удовлетворительно (3);
75-90 баллов – хорошо (4);
91-100 баллов – отлично (5).

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	Галатенко В. А., Бетелин В. Б.	Стандарты информационной безопасности: курс лекций (https://biblioclub.ru/index.php?page=book&id=233065)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006	ЭБС
Л1.2	Бекетнова Ю. М., Крылов Г. О., Ларионова С. Л.	Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие (https://biblioclub.ru/index.php?page=book&id=494850)	Москва : Прометей, 2018	ЭБС
Л1.3	Аверченков В. И.	Аудит информационной безопасности: учебное пособие для вузов: учебное пособие (https://biblioclub.ru/index.php?page=book&id=93245)	Москва : ФЛИНТА, 2016	ЭБС
Л1.4	Дубинин Е.А., Тебуева Ф.Б.	Оценка относительного ущерба безопасности информационной системы: монография (http://znanium.com/catalog/document?id=14007)	Москва : Издательский Центр РИОР, 2014	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Громов Ю. Ю., Мартемьянов Ю. Ф., Букурако Ю. К., Иванова О. Г., Однолько В. Г.	Организация безопасной работы информационных систем: учебное пособие (https://biblioclub.ru/index.php?page=book&id=277794)	Тамбов : Тамбовский государственный технический университет (ТГТУ), 2014	ЭБС
Л2.2	Кияев В., Граничин О.	Безопасность информационных систем: курс: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429032)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие (http://znanium.com/catalog/document?id=315651)	Москва : Издательский Центр РИОР, 2018	ЭБС
Л2.4	Васильков А.В., Васильков И. А.	Безопасность и управление доступом в информационных системах: учебное пособие (http://znanium.com/catalog/document?id=327909)	Москва : Издательство "ФОРУМ", 2019	ЭБС
Л2.5	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие (http://znanium.com/catalog/document?id=336219)	Москва : Издательский Центр РИОР, 2019	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader

Notepad++

VirtualBox

Visual Studio

7.3.2 Профессиональные базы данных и информационно-справочные системы

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

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

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

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.

Лабораторные занятия проходят в учебных лабораториях технических средств защиты информации и "Сетевой полигон" (ауд. 421, 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспортах лабораторий.

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 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.

Рекомендуется перед каждым лекционным занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие в 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.