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

Рабочая программа дисциплины (модуля)*
Модели безопасности 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

Целью изучения дисциплины «Модели безопасности компьютерных систем» является обучение специалистов принципам формального моделирования и анализа безопасности компьютерных систем (КС), реализующих управление доступом и информационными потоками, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-8.1 Знает основные методы научных исследований при разработке моделей безопасности компьютерных систем.

ОПК-8.2 Умеет применять методы научных исследований при проведении разработок моделей безопасности компьютерных систем.

ОПК-8.3 Владеет способами моделирования безопасности компьютерных систем.

ОПК-11.1 Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.

ОПК-11.2 Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.

ОПК-11.3 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.24

2.1 Требования к предварительной подготовке обучающегося:

Информатика

Языки программирования

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

Системное программирование

Защита программ и данных

Защита в операционных системах

Тестирование компьютерных систем на проникновения

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

ОПК-8: Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

Знать:

– виды и состав угроз информационной безопасности;
– принципы и общие методы обеспечения информационной безопасности;
– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;
– каналы и методы несанкционированного доступа к конфиденциальной информации;
– состав объектов защиты информации.

Уметь:

– определять состав конфиденциальной информации;
– определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию;
– определять возможные каналы и методы несанкционированного доступа;
– принимать решения при выборе средств защиты информации на основе анализа угроз и рисков;
– организовывать системное обеспечение защиты информации.

Владеть:

– навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий;
– навыками разработки основных политик безопасности;
– критериями, условиями и принципами отнесения информации к защищаемой;

– методологией построения систем защиты автоматизированных систем.

ОПК-11: Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

Знать:

– типовые модели политик безопасности КС, политик управления доступом и информационными потоками.

Уметь:

– самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований.

Владеть:

– методами разработки моделей политик безопасности, управления доступом и информационными потоками.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основные формальные модели политик безопасности, модели дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;
3.1.2	– виды и состав угроз информационной безопасности;
3.1.3	– принципы и общие методы обеспечения информационной безопасности;
3.1.4	– основы разработки систем защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы;
3.1.5	– методы выявления уязвимостей.
3.2	**Уметь:**
3.2.1	– самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности;
3.2.2	– определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию;
3.2.3	– определять возможные каналы и методы несанкционированного доступа;
3.2.4	– организовывать системное обеспечение защиты информации;
3.2.5	– самостоятельно разрабатывать системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы.
3.3	**Владеть:**
3.3.1	– методами разработки моделей политик безопасности, управления доступом и информационными потоками;
3.3.2	– навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий;
3.3.3	– навыками разработки основных политик безопасности;
3.3.4	– методами разработки системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану : 144 в том числе : аудиторные занятия : 54 самостоятельная работа : 72 часов на контроль : 18	Виды контроля в семестрах: экзамены 5

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основные понятия и определения. Угрозы безопасности информации			
1.1	Основные элементы теории компьютерной безопасности. Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени). /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

1.2	Модели ценности информации. Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Классификация угроз безопасности информации. Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Угрозы информационной безопасности: Решение ситуационных задач в группах на определение видов угроз информационной безопасности в заданной автоматизированной системе. /Лаб/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Основные понятия и определения. Угрозы безопасности информации. /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 2. Политика безопасности			
2.1	Основные виды политик управления. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Представление политик безопасности. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Представление политик безопасности. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Политика безопасности: –Решение ситуационных задач в группах по составлению неформальных политик безопасности для заданной автоматизированной системе. -Настройка элементов политики безопасности операционной системы Windows XP SP2. -Элементы политики безопасности в ОС семейства Unix /Лаб/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.4	Политика безопасности. /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 3. Нормативный подход к безопасности			
3.1	Классические стандарты информационной безопасности. /Лек/	5	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.2	Нормативные акты. Изучение нормативов ИБ. Рассмотрение политик безопасности. /Лаб/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.3	Нормативный подход к безопасности. /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 4. Модели компьютерных систем с дискреционным управлением доступом			
4.1	Политики дискреционного управления доступом. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.2	Модели компьютерных систем с дискреционным управлением доступом. Модели компьютерных систем с дискреционным управлением доступом. Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.3	Классическая модель распространения прав доступа Take-Grant /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

4.4	Модели безопасности: - Математические основы моделей безопасности. Элементы теории графов, теории автоматов. - Рассмотрение систем ХРУ. Выполнение задач на описание моделей ХРУ, ТМД. Модель ХРУ как основа дискреционной политики безопасности в ОС Windows. - Модель Take-Grant. Решение задач на определение свойств безопасности модели Take-Grant. /Лаб/	5	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.5	Модели компьютерных систем с дискреционным управлением доступом. /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 5. Модели компьютерных систем с мандатным управлением доступом			
5.1	Модели компьютерных систем с мандатным управлением доступом. Модели компьютерных систем с мандатным управлением доступом. Классическая модель Белла-ЛаПадулы. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.2	Классическая модель Белла-ЛаПадулы. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.3	Модель Белла-ЛаПадулы: -Модель Белла-ЛаПадулы. Решение задач на определение безопасности системы Белла-ЛаПадулы. -Модель Белла-ЛаПадулы в ОС Unix. /Лаб/	5	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
5.4	Модели компьютерных систем с мандатным управлением доступом /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 6. Модели безопасности информационных потоков и изолированной программной среды			
6.1	Классическая модель Белла-ЛаПадулы. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
6.2	Безопасность информационных потоков. Защита от угроз конфиденциальности и целостности информации. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
6.3	Информационные потоки: -Решение задач на определение свойств модели безопасности информационных потоков. -Решение задач на определение свойств безопасности модели изолированной программной среды. /Лаб/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
6.4	Модели безопасности информационных потоков и изолированной программной среды /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 7. Модели компьютерных систем с ролевым управлением доступом			
7.1	Модель администрирования ролевого управления доступом. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
7.2	Ролевое управление доступом: -Модель администрирования ролевого управления доступом. -Модель мандатного ролевого управления доступом. /Лаб/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
7.3	Модели компьютерных систем с ролевым управлением доступом. /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 8. Развитие формальных моделей безопасности компьютерных систем			

8.1	Развитие формальных моделей безопасности компьютерных систем. /Лек/	5	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
8.2	Развитие формальных моделей безопасности компьютерных систем. Проблема адекватности реализации модели безопасности в реальной КС. Развитие формальных моделей. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП- моделей) КС с дискреционным, мандатным или ролевым управлением доступом. /Лек/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
8.3	ДП-модели: Свойства семейства ДП-моделей /Лаб/	5	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
8.4	Развитие формальных моделей безопасности компьютерных систем. /Ср/	5	9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 9. Экзамен			
9.1	/Экзамен/	5	18	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Лабораторная работа.
Экзамен

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Пример лабораторной работы

Лабораторная работа №5
Реализовать криптографическую подсистему в системе управления доступом.
Сервер:
- протокол связи сервера с клиентом (выбор этого протокола)
- выработка общего ключа
- шифрование всех передаваемых сообщений
- хранение ключей шифрования
- шифрование ключевой системной информации

Клиент:
- выработка общего ключа
- обмен сообщениями по шифрованному каналу связи

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к экзамену.
1. Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени).
2. Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности.
3. Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС.
4. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками.
5. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Представление политик безопасности.
6. Политики дискреционного управления доступом.
7. Классические стандарты информационной безопасности.
8. Классические стандарты информационной безопасности.
9. Модели компьютерных систем с дискреционным управлением доступом. Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.
10. Классическая модель распространения прав доступа Take-Grant.
11. Модели компьютерных систем с мандатным управлением доступом. Классическая модель Белла-

ЛаПадулы.
12. Классическая модель Белла-ЛаПадулы.
13. Модели безопасности информационных потоков и изолированной программной среды.
14. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей.
15. Безопасность информационных потоков. Защита от угроз конфиденциальности и целостности информации.
16. Развитие формальных моделей безопасности компьютерных систем.
17. Развитие формальных моделей безопасности компьютерных систем.
18. Проблема адекватности реализации модели безопасности в реальной КС. Развитие формальных моделей. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом.

Пример экзаменационного билета:
Билет №3
1. Общие подходы к построению парольных систем. Основные компоненты парольной системы. Типы угроз безопасности парольных систем.
2. Стандарт оценки безопасности компьютерных систем TCSEC. Основные требования к системам защиты TCSEC. Классы защиты TCSEC.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
В течении семестра проводится пять лабораторных работ, которые осуществляют срез знаний по основным понятиям, определениям и задачам.
На экзамене студент получает билет. В билете два теоретических вопроса. На написание ответа дается 1,5 часа. После этого происходит оценка ответа. Преподаватель может задавать вопросы по тексту ответа. Студент должен на них ответить.
При подведении итогов баллы за экзамен суммируются с баллами за лабораторные работы в течении семестра.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа	5x5=25
2	Допуск к экзамену – 4 из 5 лаб.работ	
3	Экзамен (2 теоретических вопрос	2x5=10
Итого:		35

Критерии оценивания теоретического вопроса
Максимальный балл за ответ на теоретический вопрос – 5 баллов.
Отлично/зачтено/5 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/ 4 балла - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/3 балла - Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-2 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 оценки лабораторной работы
5 баллов – лабораторная работа выполнена полно и правильно в соответствии с заданием, проведено и представлено полное тестирование систем и функций; технически правильным языком, даны верные ответы на контрольные вопросы;
4 балла – лабораторная работа выполнена не полностью, при выполнении лабораторной работы обучающимся допущены существенные ошибки, не весь функционал отражен в тестах.
3 балла – выполнены отдельные части лабораторной работы, допущены грубые ошибки, на большинство контрольных вопросов даны неверные ответы.

Промежуточная аттестация в целом выставляется по результатам лабораторных работ и ответа на экзаменационный билет, при условии сдачи хотя бы четырех из пяти лабораторных работ. Если какая-то часть не сдана, то студенту предлагаются дополнительные вопросы по этой части.
Критерий оценивания результатов экзамена:
0-17 баллов – неудовлетворительно (2);
18-23 баллов – удовлетворительно (3);
24-28 баллов – хорошо (4);

29-35 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	Мэйволд Э.	Безопасность сетей (https://biblioclub.ru/index.php?page=book&id=429035)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.2	Шаньгин В. Ф.	Защита информации в компьютерных системах и сетях (http://e.lanbook.com/books/element.php? pl1_cid=25&pl1_id=3032)	Москва : ДМК Пресс, 2012	ЭБС
Л1.3		Методика построения модели безопасности автоматизированных систем: статья (http://znanium.com/catalog/document?id=59146)	Тверь : ЗАО Научно-исследовательский институт Центрпрограммсистем, 2012	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Лапонина О. Р.	Криптографические основы безопасности: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429092)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л2.2	Шаньгин В. Ф.	Защита компьютерной информации (http://e.lanbook.com/books/element.php? pl1_cid=25&pl1_id=1122)	Москва : ДМК Пресс, 2010	ЭБС
Л2.3	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: учебное пособие (http://znanium.com/catalog/document?id=358701)	Москва : Издательский Дом "ФОРУМ", 2020	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

Adobe Reader

Notepad++

Visual Studio

Ubuntu Linux

VirtualBox

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, лабораторные 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 лабораторных занятиях преподаватель знакомит студентов с типовыми задачами, с методами решения задач и контролирует выполнение лабораторных работ.

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.