Рабочая программа дисциплины (модуля)*
Администрирование Windows

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2025

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

Челябинск 2025 г.

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

Целями изучения дисциплины являются:

- ознакомление студентов с принципами построения и архитектурой современных сетевых операционных систем, принципами администрирования корпоративных сетевых информационных систем, с принципами обеспечения реализации типичных бизнес-процессов, характерных для большинства современных предприятий;

- освоение студентами основ администрирования корпоративных сетевых операционных систем.

Задачами изучения дисциплины являются:

- формирование и развитие компетенций, знаний, практических навыков и умений по вопросам архитектуры современных сетевых операционных систем, настройки конкретной операционной системы для выполнения бизнес- задач, особенностей обеспечения безотказного режима работы системы 24/7.

Результаты обучения по дисциплине направлены на достижение индикаторов:

УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах).

УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном (ых) языке(ах)

УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке (ах).

ОПК-12.1 Знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей; основные принципы конфигурирования и администрирования операционных систем.

ОПК-12.2 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде.

ОПК-12.3 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	К.М.03.05

2.1 Требования к предварительной подготовке обучающегося:

Операционные системы

Сети и системы передачи информации

Компьютерные сети

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

Защита в операционных системах

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

УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Знать:

– основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий.

Уметь:

– составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов.

Владеть:

– иметь навыки вербальной коммуникации на техническом иностранном языке.

ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

Знать:

– основные понятия защищенных операционных систем, баз данных и компьютерных сетей;
– понятие защиты информации, системы защиты;
– основные виды угроз безопасности информации и их классификацию;
– основные понятия, основные алгоритмы хранения и обработки данных ОС;
– основные стандарты и алгоритмы передачи данных;
– основные актуальные модели атак;
– аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных;
– средства аутентификации электронных данных и средства управления ключевой информацией;
– требования к криптографическим системам защиты информации;
– понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows.

Уметь:

– использовать алгоритмы генерации, хранения и распределения ключей;
– проектировать и использовать системы электронной цифровой подписи;
– применять на практике алгоритмы управления открытыми ключами;
– разрабатывать и конфигурировать программно-аппаратные средства защиты информации, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

Владеть:

– основными методами администрирования и настройки ОС и сетей передачи;
– алгоритмами формирования хеш-функций;
– инструментами обеспечения безопасной работы в сети интернет;
– методологией применения безопасных публичных служб;
– методами управления ключами в системах с открытым ключом;
– инструментами обеспечения безопасной работы в сети интернет;
– основами конфигурирования и разработки программно-аппаратных средств защиты информации, системы управления базами данных; компьютерных сетей, системы антивирусной защиты, средств криптографической защиты информации в рамках администрирования и защиты публичных служб Windows.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;
3.1.2	– основные понятия защищенных операционных систем, баз данных и компьютерных сетей;
3.1.3	– понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows.
3.2	**Уметь:**
3.2.1	– пользоваться программными средствами, реализующими основные криптографические функции;
3.2.2	– разрабатывать программно-аппаратных средств защиты информации.
3.3	**Владеть:**
3.3.1	– навыками обеспечения безопасной работы на компьютере;
3.3.2	– средствами криптографической защиты информации в рамках администрирования и защиты публичных служб Windows.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**2 ЗЕТ**
Часов по учебному плану : 72 в том числе : аудиторные занятия : 50 самостоятельная работа : 16,9 : контактная работа: 55,1 ИКР: 5,1	Виды контроля в семестрах: зачеты 7

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Раздел 1. Основные понятия и определения.			
1.1	Основные понятия и определения. /Лек/	7	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	Локальные политики безопасности /Лек/	7	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Парольная защита Windows /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Использование средств защиты информации от несанкционированного доступа для усиления парольной защиты Windows /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Лабораторная работа № 1 - Парольная защита в Windows /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Основные понятия и определения. Парольная защита Windows /Ср/	7	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 2. Раздел 2. Аудит в операционных системах Windows			
2.1	Аудит в операционных системах Windows /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.2	Лабораторная работа № 2 - Аудит в операционных системах Windows /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
2.3	Аудит в операционных системах Windows /Ср/	7	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 3. Раздел 3. Microsoft Active Directory			
3.1	Microsoft Active Directory /Лек/	7	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.2	Лабораторная работа № 3 - Microsoft Active Directory /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.3	Microsoft Active Directory. Коллектор журналов /Лек/	7	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

3.4	Лабораторная работа № 4 - Microsoft Active Directory. Коллектор журналов /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
3.5	Microsoft Active Directory /Ср/	7	5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 4. Раздел 4. Positive Technologies MP SIEM			
4.1	Positive Technologies MP SIEM. Активация, основные функции, сбор событий /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.2	Лабораторная работа № 5 - Positive Technologies MP SIEM. Активация, основные функции, сбор событий /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.3	Positive Technologies MP SIEM. Анализ защищенности /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.4	Лабораторная работа № 6 - Positive Technologies MP SIEM. Анализ защищенности /Лаб/	7	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.5	Positive Technologies MP SIEM. Обработка событий /Лек/	7	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.6	Лабораторная работа № 7 - Positive Technologies MP SIEM. Обработка событий /Лаб/	7	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
4.7	Positive Technologies MP SIEM. /Ср/	7	5,9	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
	Раздел 5. Иная контактная работа			
5.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	7	5,1	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Лабораторная работа.
Перечень вопросов к зачету.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Лабораторная работа № 1 - Парольная защита в Windows
В виртуальной машине установить клиентскую операционную систему Windows.
С использованием локальных политик безопасности установить ограничения:
- минимальная длина пароля пользователя Windows – 14 символов;
- требование сложности пароля;
- блокировка учетной записи пользователя на 30 минут после пяти неудачных попыток авторизации.
Создать учетную запись пользователя Windows с паролем, удовлетворяющим установленным требованиям.
Сбросить пароль пользователя Windows с использованием предоставленного специализированного программного обеспечения.
Установить предоставленное средство защиты от несанкционированного доступа.
Сбросить пароль пользователя Windows на виртуальной машине с установленным средством защиты от несанкционированного доступа.
Настроить средство защиты от несанкционированного доступа для блокировки попыток сброса пароля специализированным ПО.
*Дистрибутивы, лицензии и специализированное программное обеспечение предоставляются преподавателем.

Лабораторная работа № 2 - Аудит в операционных системах Windows
Настроить журналирование событий Windows – создать систему разграничения доступа (минимум два пользователя Windows с разным уровнем полномочий: полный доступ и доступ только для чтения) и настроить аудит

использования привилегий для каталога на локальном диске и вложенных в него файлов, обеспечивающий регистрацию сведений:
- метод доступа к контролируемым файлам и каталогу;
- результат (успех, отказ) попытки использования привилегий;
- учетная запись пользователя, использующего привилегии;
- время события;
- регистрация сведений об удалённых файлах.

Воссоздать структуру сети, сценарии использования компьютеров в локальной сети по результатам анализа предоставленных журналов безопасности, содержащую следующую информацию:
- сетевые имена компьютеров, входящих в локальную сеть;
- учётные записи пользователей и их соответствие сетевым именам компьютеров, на которых эти ученые записи используются;
- режим эксплуатации (время, дни недели) компьютеров;
- наличие сетевого программного обеспечения;
- определение наличия и типа контроллера домена Windows;
- используемые сетевые протоколы;
- используемое прикладное программное обеспечение;
- приблизительная схема локальной сети.

*специально подготовленные журналы, содержащие исходные события, предоставляются преподавателем

Лабораторная работа № 3 - Microsoft Active Directory

На двух виртуальных машинах установить соответственно серверную (Windows 2008 Server или более новая) и клиентскую (Windows 7 или более новая) операционные системы.
Клонировать виртуальную машину с серверной операционной системой, изменив идентификатор (SID) операционной системы и сетевое имя.
Между созданными виртуальными машинами настроить виртуальную сеть, соответствующую требованиям:
- все виртуальные машины находятся в одном virtual lan;
- все виртуальные машины имеют различные сетевые имена и ip-адреса;
- все виртуальные машины доступны друг другу по широковещательным рассылкам (находятся в одной подсети);
- основным шлюзом и сервером имён является виртуальная машина с исходной (по отношению к клонированной виртуальной машине с серверной операционной системой).

Серверной операционной системе добавить роль контроллера домена Active Directory.
Сконфигурировать контроллер домена с настройками по умолчанию, ввести клиентскую операционную систему в состав контроллера домена (показатель успешности настройки – на клиентской машине появляется возможность авторизоваться с доменной учетной записью).
На клонированной виртуальной машине с серверной операционной системой настроить роль резервного контроллера домена (показатель успешности настройки – изменение структуры Active Directory на основном контроллере домена (добавление пользователей, компьютеров и т.д.) влечёт изменение структуры Active Directory на резервном контроллере домена.

Лабораторная работа № 4 - Microsoft Active Directory. Коллектор журналов
На двух виртуальных машинах установить соответственно серверную (Windows 2008 Server или более новая) и клиентскую (Windows 7 или более новая) операционные системы.
Настроить журналирование событий Windows – создать систему разграничения доступа (минимум два пользователя Windows с разным уровнем полномочий: полный доступ и доступ только для чтения) и настроить аудит использования привилегий для каталога на локальном диске и вложенных в него файлов, обеспечивающий регистрацию сведений:
- метод доступа к контролируемым файлам и каталогу;
- результат (успех, отказ) попытки использования привилегий;
- учетная запись пользователя, использующего привилегии;
- время события;
- регистрация сведений об удалённых файлах.

Между созданными виртуальными машинами настроить виртуальную сеть, соответствующую требованиям:
- все виртуальные машины находятся в одном virtual lan;
- все виртуальные машины имеют различные сетевые имена и ip-адреса;
- все виртуальные машины доступны друг другу по широковещательным рассылкам (находятся в одной подсети);
- основным шлюзом и сервером имён является виртуальная машина с серверной операционной системой.

Серверной операционной системе добавить роль контроллера домена Active Directory.

Сконфигурировать контроллер домена с настройками по-умолчанию, ввести клиентскую операционную систему в состав контроллера домена (показатель успешности настройки – на клиентской машине появляется возможность авторизоваться с доменной учетной записью).
Настроить коллектор (сборщик) журналов безопасности в серверной операционной системе для сбора событий из журнала безопасности клиентской операционной системы (показатель успешности выполнения задания - события по результатам аудита (в клиентской операционной системе, в журнале безопасности) доступа к каталогу, на основе созданной системы разграничения доступа, появляются в серверной операционной системе, в журнале коллектора (сборщика) журналов).

Лабораторная работа № 5 - Positive Technologies MP SIEM. Активация, основные функции, сбор событий
Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM. Активировать предоставленную лицензию, в соответствии с предоставленной документацией на Positive Technologies MP SIEM.
Создать задачу по сбору журналов из коллектора (сборщика) журналов Windows.
Создать задачу по сбору событий из базы данных Kaspersky Security Center.
Создать задачу по сбору событий по стандарту syslog.

Лабораторная работа № 6 - Positive Technologies MP SIEM. Анализ защищенности
Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM.
Провести поиск доступных хостов в сети. Выполнить задачу по сканированию доступных хостов на наличие уязвимостей в режиме PenTest (показатель успешности – обнаруженные уязвимости в результатах сканирования доступных хостов).
Проанализировать выявленные уязвимости рассмотреть, описать и принять меры по их устранению стандартными средствами Windows (закрытие портов, установка обновлений и т.д.).

Лабораторная работа № 7 - Positive Technologies MP SIEM. Обработка событий
Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM.
Написать произвольное правило нормализации.
Написать произвольное правило агрегации.
Написать произвольное правило обогащения.
Написать произвольное правило корреляции.
Написать произвольное правило локализации.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к зачёту
1. Модель OSI
2. Модель TCP/IP
3. Архитектура DNS
4. Протокол LDAP
5. MS Windows Server. Роли
6. MS Active Directory. Архитектура
7. MS Active Directory. Средства управления
8. Коллектор журналов событий Windows Server
9. Построение VPN сети средствами MS Windows Server
10. Настройка сервера удалённых рабочих столов RDP
11. Парольная защита Windows (локальная)
12. Система аудита Windows
13. RAID
14. UEFI/Legacy режимы загрузки Windows
15. SIEM-системы. Принципы построения и назначение
16. SIEM-системы. Формирование инцидентов и управление ими
17. SIEM-системы. Обработка событий
18. SIEM-системы. Настройка сбора событий

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
На зачёте студент получает билет. В билете два теоретических вопроса. На написание ответа дается 1 час. После этого происходит оценка ответа. Преподаватель может задавать вопросы по тексту ответа. Студент должен на них ответить.
Максимальный балл за ответ на теоретический вопрос - 10.
Максимальный балл за лабораторную работу - 10.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-7	7x10=70
2	Зачет (теоретический вопрос)	2x10=20
Итого		90

Критерии оценивания теоретического вопроса и лабораторной работы
Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, понимает терминологию на языке программирования PERL или Python . Обучающийся практически не допускает ошибок.
Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, понимает терминологию на языке программирования PERL или Python. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом, владеет терминологией объектно-ориентированного программирования. Обучающийся допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-4 балла - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

При подведении итогов учитываются результаты текущей аттестации. Промежуточная аттестация в целом выставляется по результатам лабораторных работ и ответа на билет на зачете.
Критерий оценивания результатов зачета:
0 – 55 баллов – не зачет;
56 – 90 баллов – зачет.

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	Власов Ю. В., Рицкова Т. И.	Администрирование сетей на платформе MS Windows Server: учебное пособие (https://biblioclub.ru/index.php?page=book&id=233291)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) |Бином. Лаборатория знаний, 2008	ЭБС
Л1.2	Айвенс К.	Администрирование Microsoft Windows Server 2003: практическое пособие (https://biblioclub.ru/index.php?page=book&id=233685)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2008	ЭБС
Л1.3	Элсенпитер Р., Велт Тоби Дж.	Администрирование сетей Microsoft Windows XP Professional: учебное пособие (https://biblioclub.ru/index.php?page=book&id=428821)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Хоружников С. Э., Прыгун В. В.	Администрирование сетей Windows: учебное пособие (http://e.lanbook.com/books/element.php?pl1_id=40727)	Санкт- Петербург : НИУ ИТМО, 2012	ЭБС

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.2	Айвенс К.	Внедрение, управление и поддержка сетевой инфраструктуры MS Windows Server 2003: практическое пособие (https://biblioclub.ru/index.php?page=book&id=233686)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2008	ЭБС
Л2.3	Таненбаум Э., Леонтьев А.	Современные операционные системы	Санкт- Петербург : Питер, 2005	

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader

Notepad++

VirtualBox

LibreOffice

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.

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 рассматриваются установка и настройка служб и базовых параметров. Рекомендуется перед каждым лабораторным занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения

материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, 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 информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и 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 с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.
Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.
При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности 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 предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. 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.

Специальность 10.05.01 Компьютерная безопасность
Специализация № 1 «Анализ безопасности компьютерных систем»
Рабочая программа дисциплины «Администрирование Windows»
2025 год набора, очная форма обучения

Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) А. Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1