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

Рабочая программа дисциплины (модуля)*

Безопасность операционных систем

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

специализация N 4 "Безопасность автоматизированных систем критически важных объектов"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год набора 2021

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

Челябинск 2021 г.

Рабочая программа дисциплины (модуля) принята:

Ученым советом физического факультета

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

Председатель Ученого совета физического факультета _____ Д.А. Захарьевич

Секретарь Ученого совета физического факультета _____ М.А. Эбель

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой

Радиофизики и электроники

Протокол заседания № 10 от «24» мая 2021 г.

И.о зав. кафедрой _____ А.В. Бутаков

Автор (составитель) _____ к.ф.-м.н., доцент, доцент кафедры радиофизики и электроники М.А. Загребин

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

Цель - обучение студентов принципам построения систем защиты информации в операционных системах. Задачи: ознакомление с основами принципов построения подсистем защиты в операционных системах различной архитектуры; ознакомление со средствами и методами несанкционированного доступа к ресурсам операционных систем; изучение принципов функционирования современных систем идентификации и аутентификации.

Индикаторы достижения компетенций:

ОПК-11.1. Имеет представление о компонентах систем защиты информации автоматизированных систем.

ОПК-11.2. Имеет практический опыт разрабатывать компоненты систем защиты информации автоматизированных систем.

ОПК-12.1. Обладает базовыми знаниями в области безопасности вычислительных сетей, операционных систем и баз данных.

ОПК-12.2. Демонстрирует умения применять при разработке автоматизированных систем знания в области безопасности вычислительных сетей, операционных систем и баз данных.

ОПК-13.1. Обладает знаниями о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем.

ОПК-13.2. Демонстрирует умения организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем.

ОПК-13.3. Имеет практический опыт проводить анализ уязвимостей систем защиты информации автоматизированных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.17

2.1 Требования к предварительной подготовке обучающегося:

Операционные системы

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

Основы информационной безопасности

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-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем;

Знать:

Для достижения индикатора ОПК-11.1: Знать о компонентах систем защиты информации автоматизированных систем (основные определения и положения безопасности ОС, основные защитные механизмы клиентских ОС).

Уметь:

Для достижения индикатора ОПК-11.2: Уметь разрабатывать компоненты систем защиты информации автоматизированных систем (осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации).

Владеть:

Для достижения индикатора ОПК-11.2: Владеть навыками разработки компонентов систем защиты информации автоматизированных систем.

ОПК-12: Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

Знать:

Для достижения индикатора ОПК-12.1: Знать базовые понятия в области безопасности операционных систем.

Уметь:

Для достижения индикатора ОПК-12.2: Уметь применять при разработке автоматизированных систем знания в области безопасности операционных систем.

Владеть:

Для достижения индикатора ОПК-12.2: Владеть навыками применения при разработке автоматизированных систем знания в области безопасности операционных систем.

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

Знать:

Для достижения индикатора ОПК-13.1: Знать о диагностике, тестировании и анализе уязвимостей систем защиты информации автоматизированных систем (программно-аппаратные средства обеспечения информационной безопасности в типовых операционных систем, в системах управления базами данных, вычислительных сетях).

Уметь:

Для достижения индикатора ОПК-13.2: Уметь организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем (оценивать угрозы безопасности клиентским ОС, осуществлять проверку защищенности клиентских ОС, осуществлять проверку защищенности серверных ОС).

Владеть:

Для достижения индикатора ОПК-13.3: Владеть навыками проведения анализа уязвимостей систем защиты информации автоматизированных систем (навыками настройки политики безопасности и учетных записей ОС, оценки степени защищенности клиентских ОС, навыками оценки степени безопасности ОС, навыками администрирования протокольных средств обеспечения безопасности ОС, навыками администрирования прав пользователей и аудита доступа к ресурсам ОС).

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	основные определения и положения безопасности ОС;
3.1.2	основные защитные механизмы клиентских ОС;
3.1.3	особенности обеспечения безопасности клиентских ОС семейств Windows и Linux
3.1.4	программно-аппаратные средства обеспечения информационной безопасности в типовых операционных систем в системах управления базами данных, вычислительных сетях
3.2	**Уметь:**
3.2.1	осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;
3.2.2	оценивать угрозы безопасности клиентским ОС осуществлять проверку защищенности клиентских ОС;
3.2.3	осуществлять проверку защищенности серверных ОС
3.3	**Владеть:**
3.3.1	навыками настройки политики безопасности и учетных записей ОС оценки степени защищенности клиентских ОС;
3.3.2	навыками оценки степени безопасности ОС;
3.3.3	навыками администрирования протокольных средств обеспечения безопасности ОС;
3.3.4	навыками администрирования прав пользователей и аудита доступа к ресурсам ОС

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану: 144 в том числе: аудиторные занятия: 72 самостоятельная работа: 36 часов на контроль: 36	Виды контроля в семестрах: экзамены 6

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Подсистема защиты информации в ОС UNIX			
1.1	Подсистема защиты информации в ОС UNIX. Основные компоненты подсистем защиты UNIX. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Создание и удаление бюджетов пользователей. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах. /Лек/	6	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
1.2	Создание бюджетов пользователя в ОС Windows, UNIX. Использование списков доступа в ОС Windows, UNIX. Аудит в Windows, UNIX. /Лаб/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
1.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 2. Подсистема Защиты информации в ОС Windows			

2.1	Подсистема Защиты информации в ОС Windows. Основные компоненты подсистем защиты Windows. Политики. Понятие домена. Особенности установления доверительных отношений. Создание и удаление бюджетов пользователей /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
2.2	Оценка защищенности заданной конфигурации Windows: файловая система, реестр, список пользователей, политика безопасности в области паролей /Лаб/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
2.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Оценка защищенности заданной конфигурации Windows: список пользователей, политика безопасности в области паролей. Поиск программных закладок в заданной консультации Windows. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Защита информации при интеграции UNIX и Windows			
3.1	Защита информации при интеграции UNIX и Windows. Основы взаимодействия элементов гетерогенных сетей. Шлюзы NFS. SMB в UNIX. Использование сервера Samba для разделения доступа к сетевым ресурсам в домене Windows. /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
3.2	Интеграция сетей Microsoft и UNIX с использованием сервера Samba. Изучение средств защиты сетевого взаимодействия Unix. /Лаб/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
3.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 4. Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ			
4.1	Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ. Методы и средства ограничения доступа к компонентам ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации /Лек/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
4.2	Поиск программных закладок в заданной консультации Windows. Использование возможностей файловой системы ОС Windows для шифрования файлов. /Лаб/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
4.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 5. Подсистема защиты информации в ОС UNIX			
5.1	Подсистема защиты информации в ОС UNIX. Основы информационной безопасности. Концепции безопасности UNIX. Настройка системы безопасности /Лаб/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
5.2	Подготовка и оформление отчетов по практическим работам. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 6. Инфраструктура открытых ключей PKI			
6.1	Инфраструктура открытых ключей PKI. Основные компоненты PKI, описываются функции удостоверяющего и регистрационного центров, репозитория, архива сертификатов, серверных компонентов PKI, приводится краткая характеристика сервисов PKI и сервисов, базирующихся на PKI, обсуждаются криптографические и вспомогательные сервисы, сервисы управления сертификатами /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
6.2	Изучение инфраструктуры открытых ключей. Изучение создания смарт-карт в инфраструктуре открытых ключей. /Лаб/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
6.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Создание сертификатов в PKI. Создание смарт-карт в PKI. /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 7. Службы сертификации в ОС Windows			

7.1	Службы сертификации в ОС Windows. Основные действия необходимые для установки и базовой настройки службы сертификации ActiveDirectory® (AD CS) в тестовой среде /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
7.2	Изучение защиты конфигурации ADCS. Создание репозитория сертификатов и восстановление ЦС. /Лаб/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
7.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 8. Служба управления правами ADRMS			
8.1	Служба управления правам ADRMS. Рассмотрение основных возможностей компонента ОС WindowsServer 2008 R2, предназначенный для управления правами доступа к файлам в целях повышения уровня безопасности информационных активов /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
8.2	Изучение службы управление правами. Изучение основных настроек службы управления правами /Лаб/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
8.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Создание шаблонов RMS для защиты офисных документов /Ср/	6	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 9. Безопасность ОС Windows на серверном уровне			
9.1	Безопасность ОС Windows на серверном уровне. Рассмотрение обеспечения физической безопасности WindowsServer. Создание входящих и исходящих правил для брандмауэра. Доступ к системе с помощью смарт-карт. Рассмотрение дополнительных мер безопасности (Защита с помощью резервного копирования, работа со службой обновления) /Лек/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
9.2	Изучение физической безопасности сервера. Изучение дополнительных мер безопасности. Изучение службы обновления WindowsServer /Лаб/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
9.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Создание дополнительных сценариев резервного копирования /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 10. Шифрование IPsec в ОС Windows			
10.1	Шифрование IPsec в ОС Windows. Рассмотрение шифрования IPsec в WindowsServer 2008R2. Принципы работы IPsec. Основные возможности IPsec. NATTraversal в IPsec /Лек/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
10.2	Изучение компонентов NAP. Изучение протокола RADIUS. Развертывание и внедрение виртуальной частной сети. /Лаб/	6	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
10.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Создание политик сетевого доступа. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
	Раздел 11. Сервер сетевых политик, защита и маршрутизациия сетевого доступа и дистанционный доступ			
11.1	Сервер сетевых политик, защита и маршрутизация сетевого доступа и дистанционный доступ. Защита сетевого доступа (NAP) в WindowsServer 2008R2. Причины развертывания NAP. Обзор компонентов NAP.Концепция NPS. Туннели VPN. Протоколы PPTP, L2TP. Активизация VPN на сервере RRAS /Лек/	6	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
11.2	Внедрение параметров политики с помощью сервера сетевых политик /Лаб/	6	1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5
11.3	Проработка лекционного материала. Подготовка и оформление отчетов по практическим работам. Создание дополнительных верификаторов. /Ср/	6	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Собеседование и отчеты по лабораторным работам.
Экзамен

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Пример лабораторной работы:
Сценарий ADCS:
Вы работаете системным администратором в компании ABC, Ltd. Компания ABC развернула инфраструктуру AD CS и опубликовала сертификаты для множества пользователей. В частности, были опубликованы сертификаты подписи программного обеспечения, распространяемого среди клиентов. Эти сертификаты позволяют гарантировать, что данное программное обеспечение предоставлено компанией ABC. Клиентам ABC понравился такой поскольку он гарантирует подлинность программного обеспечения В ваши обязанности, в частности, входит еженедельный просмотр журналов событий на серверах. Поскольку компания использует WindowsServer 2008, в каждом центре сертификации в сети вы отконфигурировали пересылку событий. Это упростило процесс администрирования, поскольку отпала необходимость в ведении журналов на отдельных серверах для просмотра событий. Вам нужно проверять лишь одно центральное размещение журналов. Во время рутинной проверки вы заметили, что корневой CA в инфраструктуре AD CS пересылал события на центральный сервер ведения журналов. Это очень странно, поскольку корневой CA должен быть постоянно отключен от сети, за исключением крайне редких операций, связанных с технической поддержкой или выдачей сертификата новому подчиненному CA. Как системный администратор вы точно знаете, что в последнее время такие операции не выполнялись. Вы просмотрели пересланный список различных событий и выяснили, что приблизительно неделю назад данный CA был подключен к сети. В течение этого времени он сгенерировал два новых корневых сертификата с именем . К счастью, в конфигурации пересылки вы также включили ведение журнала. В журналах вы нашли перечень тех, кто входил на корневой CA. Поскольку для входа требуется смарт-карта, с помощью журналов событий можно определить, кто входил на сервер. К своему удивлению, вы обнаружили, что на сервер входили два сотрудника, уволенные на прошлой неделе. Они не должны иметь права доступа к данному серверу. Вы проверили данные Интернета и выяснили, что эти два корневых сертификата использовались для подписи стороннего программного обеспечения не от компании ABC. Оказалось, что в настоящее время эти двое бывших сотрудников торгуют сертификатами подписи программного обеспечения, используя имя ABC. Что нужно предпринять?

Типовые вопросы для собеседования по лабораторным работам:
1. Инфраструктура открытых ключей - основные подходы к реализации PKI.
2. Цель создания и основные компоненты инфраструктуры открытых ключей.
3. Понятие цифровой сертификат, его функции и версии? Возможные классы сертификатов? (Примеры)
4. Центр сертификации? Функции центра сертификации? Основные отличия автономного центра сертификации от центра сертификации предприятия?
5. Понятие регистрационный центр? Функции регистрационного центра
6. Понятие реестра сертификаторв? Функции реестра сертификатов?
7. Понятие архива сертификатов? Функции архива сертификатов?
8. Пользователи PKI. Требование предъявляемые к пользователям?
9. Сервер восстановления? Основная функция сервера восстановления? Практическая реализация?
10. Модель строгой иерархии удостоверяющих центров?
11. Понятие списка аннулированных сертификатов?
12. Понятие онлайновый протокол статуса сертификата (OCSP)?
13. Примеры компонентов клиентской стороны PKI? Описание функционала?
14. Возможные сценарии служб сертификации ActiveDirectory?
15. Службы AD CS в Windows Server? (Описание основных компонентов)
16. Описание основных различий AD CS в каждом выпуске WindowsServer?
17. Описание основных этапов установки AD CS в WindowsServer?
18. Служба NDES? Описание возможностей службы?
19. Использование смарт-карт в инфраструктуре открытых ключей?

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Вопросы к экзамену:
1. Понятие операционной системы (ОС): предназначение и функции.
2. Угрозы безопасности ОС.
3. Защищенная ОС: характеристики, способы построения.
4. Архитектура подсистемы защиты ОС: компоненты и их назначение.
5. Модели разграничения доступа в ОС: основные типы и их особенности.
6. Идентификация и аутентификации в ОС: основные способы и их характеристики.
7. Политика безопасности организации: понятие, адекватность политики, этапы создания.
8. Защита в ОС Windows: процесс загрузки ОС, вход в систему, реестр, учетные записи пользователей, файловая система.
9. Защита в ОС Linux: процесс загрузки ОС, учетные записи пользователей.

10. Реализация классических атак на ОС Windows, UNIX: сброс пароля пользователя, подбор пароля.
11. Шифрование в ОС Windows, UNIX.
12. Средства разграничения доступа в ОС Windows, UNIX.
13. Безопасные системы и угрозы безопасности. Роль операционных систем в обеспечении информационной безопасности.
14. Идентификация и аутентификация пользователя.
15. Авторизация и методы разграничения доступа.
16. Методы реализации дискреционной модели доступа.
17. Многоуровневый доступ.
18. Контроль повторного использования объектов. Анализ тайных каналов передачи информации. Аудит и протоколирование системы защиты.
19. Требования надежности систем безопасности.
20. Понятие классов безопасности.
21. Средства обеспечения безопасности современных операционных системах.

6.4. Критерии оценивания

Критерии оценивания собеседования и отчета по лабораторным работам:

В процессе выполнения лабораторной работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.

Лабораторная работа засчитывается студенту, если он представил правильно оформленный отчет, владеет методикой обработки данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.

Лабораторная работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Критерии оценивания экзамена:

Студент допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполненных и защищенных работ. В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдаётся экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается. Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

Оценка «хорошо» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» выставляется:

Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

Оценка «неудовлетворительно» выставляется:

1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.
2) Ответ на вопрос полностью отсутствует.
3) Отказ от ответа.

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	Курячий Г. В.	Операционная система UNIX: методическое пособие (https://biblioclub.ru/index.php?page=book&id=233108)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2004	ЭБС
Л1.2	Бражук А. И.	Сетевые средства Linux: курс лекций (https://biblioclub.ru/index.php?page=book&id=428794)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.3	Молочков В. П.	Операционная система ROSA: курс лекций (https://biblioclub.ru/index.php?page=book&id=429056)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.4		Операционная система Microsoft Windows XP: курс лекций (https://biblioclub.ru/index.php?page=book&id=429091)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Ложников П. С., Михайлов Е. М.	Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft: практикум (https://biblioclub.ru/index.php?page=book&id=233194)	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) |Бином. Лаборатория знаний, 2008	ЭБС
Л2.2	Царев Р. Ю., Прокопенко А. В., Князьков А. Н.	Программные и аппаратные средства информатики: учебник (https://biblioclub.ru/index.php?page=book&id=435670)	Красноярск : Сибирский федеральный университет (СФУ), 2015	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство Лань. - URL: http://e.lanbook.com/
Э2	Университетская библиотека онлайн [Электронный ресурс]: электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. - URL: http://biblioclub.ru/
Э3	Юрайт [Электронный ресурс]: электронно-библиотечная система (ЭБС) / издательство Юрайт. - URL: https://urait.ru/
Э4	Znanium.com [Электронный ресурс]: электронно-библиотечная система (ЭБС) / Научно-издательский центр ИНФРА-М. - URL: http://znanium.com/
Э5	eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. – URL: http://elibrary.ru/defaultx.asp

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader
Notepad++
VirtualBox
Ubuntu Linux
LMS Moodle
MS Office365
Adobe Connect Acrobat
Антивирус Касперского

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. APS JOURNALS. Physical Review Letters, Physical Review X, Physical Review, and Reviews of Modern Physics : журналы American Physical Society : сайт. – URL: http://journals.aps.org/about – Яз. англ. – Режим доступа: только из сети университета. – Текст : электронный.
3. Web of Science: мультидисциплинарная реферативная база данных / компания Thomson Reuters. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.
4. Scopus: реферативная база данных / Elsevier BV. – URL: http://www.scopus.com/ – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.
5. Springer Link: [сайт]. – URL: http://link.springer.com/ – Яз. англ. – Режим доступа: для зарегистрир. пользователей ЧелГУ. – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения - мультимедийным оборудованием (экран, ноутбук, проектор, колонки).

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно- наглядных пособий (мультимедийные презентации), различные формы наглядности (графики, таблицы, схемы и т.д)).

Практические занятия проходят в учебной лаборатории электроники и схемотехники, микропроцессорных систем (аудитория 221 учебный корпус №1). Материально - техническое обеспечение приведено в паспорте лаборатории.

Для самостоятельной работы студента используются аудитория №205 - читальный зал №3 (учебный корпус №1) и аудитория №206 - электронный читальный зал (специализированный медиацентр) (учебный корпус №1), оснащенные персональными компьютерами, мультимедийной аппаратурой. В аудиториях обеспечен доступ к различной справочной литературе, энциклопедиям, библиографическим и полнотекстовым базам данных, информационным ресурсам «Интернет».

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

Освоение содержания учебной дисциплины «Безопасность операционных систем» осуществляется на лекциях, лабораторных занятиях и в процессе самостоятельной учебной деятельности студентов.

Лекции составляют основу теоретической подготовки студентов с целью понимания ими сущности дисциплины. Лекционные занятия посвящены рассмотрению ключевых, базовых положений дисциплины и разъяснению учебных заданий, выносимых на самостоятельную проработку. В ходе лекционных занятий нужно конспектировать учебный материал, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений. Лекции должны активизировать познавательную деятельность обучающихся, вызывать интерес к поставленным проблемам и направлениям развития в профессиональной области, формировать их профессиональный кругозор, аналитические качества, творческий подход к изучению дисциплины, определять направления дальнейшего самостоятельного изучения и практического освоения в данной области. Изложение материала лекций должно носить проблемный, инновационный характер, способствующий формированию и развитию соответствующих компетенций. Преподавателю необходимо опираться на основную литературу, представленную в рабочей программе данной дисциплины, а также на учебные пособия, монографии, научные статьи и периодические издания известных специалистов в данной области.

Лабораторные занятия предназначены для приобретения опыта практической реализации полученных теоретических знаний. Указания к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется преподавателем перед проведением лабораторных занятий. На лабораторных занятиях студенты овладевают первоначальными профессиональными умениями и навыками, которые в дальнейшем закрепляются и совершенствуются в процессе прохождения производственной практики.

Самостоятельная работа студентов включает проработку лекционного курса, подготовку к практическим работам, выполнение всех заявленных в рабочей программе видов самостоятельной работы (выполнение домашних заданий). Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников. В ходе самостоятельной работы необходимо изучить основную литературу, ознакомиться с дополнительной литературой. Очень полезно дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой.

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, MS Office365, форумы, электронная почта и др.).

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.