Рабочая программа дисциплины (модуля)*
Защита в операционных системах

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 2025г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями изучения дисциплины являются:

– обучение студентов принципам построения систем защиты информации в операционных системах (ОС).

Задачами изучения дисциплины являются:

– ознакомление с основами принципов построения подсистем защиты в ОС различной архитектуры,

– ознакомление со средствами и методами несанкционированного доступа к ресурсам ОС;

– изучение принципов функционирования современных систем идентификации и аутентификации.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных.

ОПК-9.2 Умеет осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты.

ОПК-13.1 Знает средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем.

ОПК-13.2 Умеет формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.

ОПК-13.3 Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.О.29

2.1 Требования к предварительной подготовке обучающегося:

Основы информационной безопасности

Операционные системы

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

Знания и практические навыки, полученные в курсе «Защита в операционных системах», расширяют профессиональный кругозор, используются обучающимися при разработке курсовых и дипломных работ.

Научно-исследовательская работа

Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

Знать:

– основные понятия операционных систем и их защиты;
– основные понятия, основные алгоритмы хранения и обработки данных ОС;
– основные стандарты и алгоритмы передачи данных;
– основные понятия защищенных операционных систем, баз данных и компьютерных сетей;
– основные актуальные модели атак;
– понятие защиты информации, системы защиты;
– аппаратно-программные средства защиты информации:

– средства обеспечения конфиденциальности данных;
– средства аутентификации электронных данных и средства управления ключевой информацией;
– цели и концептуальные основы защиты информации;
– основные виды угроз безопасности информации и их классификацию.

Уметь:

– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;
– оценивать угрозы безопасности клиентским ОС осуществлять проверку защищенности клиентских ОС;
– осуществлять проверку защищенности серверных ОС;
– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;
– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;
– использовать алгоритмы генерации, хранения и распределения ключей;
– проектировать и использовать системы электронной цифровой подписи;
– применять на практике алгоритмы управления открытыми ключами.

Владеть:

– 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;
– 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.

ОПК-13: Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;

Знать:

– цели и концептуальные основы защиты информации;
– основные виды угроз безопасности информации и их классификацию;
– программно-аппаратные средства защиты информации:
– средства обеспечения конфиденциальности данных;
– средства аутентификации электронных данных и средства управления ключевой информацией;
– требования к криптографическим системам защиты информации;
– понятие и виды криптографических атак.

Уметь:

– оценивать угрозы безопасности клиентским ОС;
– проектировать и использовать системы электронной цифровой подписи;
– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;
– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;
– использовать алгоритмы генерации, хранения и распределения ключей;
– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;
– осуществлять проверку защищенности клиентских ОС;
– осуществлять проверку защищенности серверных ОС.

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.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– основные понятия операционных систем и их защиты, понятие хеш-функций; понятие защиты информации и основные актуальные модели атак.
3.2	**Уметь:**
3.2.1	– формулировать, разрабатывать и настраивать политику безопасности основных операционных систем;
3.2.2	– пользоваться в своей профессиональной деятельности основными методами и средствами обеспечения информационной безопасности с учетом угроз безопасности информации и требований по защите информации;
3.2.3	– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем.
3.3	**Владеть:**
3.3.1	– навыками проведения экспериментальных исследований с применением стандартов и политики безопасности ОС;
3.3.2	– навыками оценки степени безопасности ОС;
3.3.3	– навыками настройки политики безопасности учетных записей ОС, оценки степени защищенности клиентских ОС;
3.3.4	– навыками администрирования протокольных средств обеспечения безопасности ОС;
3.3.5	– навыками администрирования прав пользователей и аудита доступа к ресурсам ОС.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**6 ЗЕТ**
Часов по учебному плану : 216 в том числе : аудиторные занятия : 100 самостоятельная работа : 74,7 часов на контроль : 27 контактная работа: 114,3 ИКР: 14,3	Виды контроля в семестрах: экзамены 9 зачеты 8

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/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
1.2	Создание бюджетов пользователя в ОС Windows, UNIX /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
1.3	Использование списков доступа в ОС Windows, UNIX /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
1.4	Аудит в Windows, UNIX /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3

1.5	Создание бюджетов пользователя в ОС Windows, UNIX. Использование списков доступа в ОС Windows, UNIX. Аудит в Windows, UNIX. /Ср/	8	15	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	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/	8	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
2.2	Оценка защищенности заданной конфигурации Windows: файловая система, реестр /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
2.3	Оценка защищенности заданной конфигурации Windows: список пользователей, политика безопасности в области паролей /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
2.4	Оценка защищенности заданной конфигурации Windows: файловая система, реестр. Оценка защищенности заданной конфигурации Windows: список пользователей, политика безопасности в области паролей. Поиск программных закладок в заданной консультации Windows. /Ср/	8	10	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	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/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
3.2	Интеграция сетей Microsoft и UNIX с использованием сервера Samba /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
3.3	Изучение средств защиты сетевого взаимодействия Unix. /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
3.4	Интеграция сетей Microsoft и UNIX с использованием сервера Samba /Ср/	8	9,7	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	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/	8	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
4.2	Поиск программных закладок в заданной консультации Windows. Использование возможностей файловой системы ОС Windows для шифрования файлов. /Лаб/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
4.3	Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ. /Ср/	8	2	Л1.1 Л1.3 Л1.4Л2.3
	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. /Лек/	8	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 6. Зачет			
6.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	8	3,3	Л1.1 Л1.3 Л1.4Л2.3
	Раздел 7. Инфраструктура открытых ключей PKI			

7.1	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/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
7.2	Изучение инфраструктуры открытых ключей /Лаб/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
7.3	Изучение создания смарт-карт в инфраструктуре открытых ключей. /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
7.4	Создание сертификатов в PKI /Ср/	9	5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
7.5	Создание смарт-карт в PKI /Ср/	9	5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 8. Службы сертификации в ОС Windows			
8.1	Службы сертификации в ОС Windows. Основные действия необходимые для установки и базовой настройки службы сертификации ActiveDirectory® (AD CS) в тестовой среде. /Лек/	9	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
8.2	Изучение защиты конфигурации ADCS. /Лаб/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
8.3	Создание репозитория сертификатов и восстановление ЦС /Ср/	9	7	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 9. Служба управления правам ADRMS			
9.1	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/	9	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
9.2	Изучение службы управление правами. /Лаб/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
9.3	Изучение основных настроек службы управления правами. /Лаб/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
9.4	Создание шаблонов RMS для защиты офисных документов /Ср/	9	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 10. Безопасность ОС Windows на серверном уровне			
10.1	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/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
10.2	Изучение физической безопасности сервера. /Лаб/	9	4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3

10.3	Изучение физической безопасности сервера. Изучение дополнительных мер безопасности. /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
10.4	Изучение службы обновления WindowsServer /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
10.5	Создание дополнительных сценариев резервного копирования. /Ср/	9	5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 11. Шифрование IPsec в ОС Windows			
11.1	Шифрование IPsec в ОС Windows. Рассмотрение шифрования IPsec в WindowsServer 2008R2. Принципы работы IPsec. Основные возможности IPsec. NATTraversal в IPsec. /Лек/	9	6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
11.2	Изучение компонентов NAP. /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
11.3	Изучение протокола RADIUS. /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
11.4	Развертывание и внедрение виртуальной частной сети. /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
11.5	Создание политик сетевого доступа /Ср/	9	5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 12. Сервер сетевых политик, защита и маршрутизация сетевого доступа и дистанционный доступ			
12.1	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/	9	8	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
12.2	Внедрение параметров политики с помощью сервера сетевых политик. /Лаб/	9	2	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
12.3	Создание дополнительных верификаторов. /Ср/	9	5	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
	Раздел 13. Экзамен			
13.1	/Экзамен/	9	27	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3
13.2	Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/	9	11	Л1.1 Л1.3 Л1.4Л2.3

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Устный опрос.
Самостоятельная работа.
Лабораторная работа.
Перечень вопросов к зачету. (8 семестр)
Перечень вопросов к экзамену. (9 семестр)

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для устного опроса для текущей аттестации
1. Типовые модели управления доступом.
2. Дискреционное управление доступом.
3. Изолированная программная среда.
4. Мандатное управление доступом.
5. Архитектура безопасности ОС Windows.
6. Security accounts manager.
7. LM, NTLM, NTLM2, NTLMv2.
8. Kerberos.
9. Реестр ОС Windows.
10. Microsoft Management Console.
11. Подсистема защиты информации в ОС UNIX.
12. Passwd и shadow файлы.
13. Основные компоненты подсистем защиты UNIX.
14. Права доступа к элементам файловой системы.
15. Управление процессами.
16. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах.
17. Аудит событий.
18. Бюджет пользователя в ОС Windows.
19. Список доступа в ОС Windows.
20. Аудит в Windows, UNIX.
21. Подсистема защиты информации в ОС Windows.
22. Основные компоненты подсистем защиты Windows.
23. Политики безопасности.
24. Понятие домена.
25. Основы взаимодействия элементов гетерогенных сетей.
26. Шлюзы NFS.
27. Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ.
28. Методы и средства ограничения доступа к компонентам ПЭВМ.
29. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
30. Методы и средства хранения ключевой информации.
31. Программная закладка.
32. Инфраструктура открытых ключей PKI.
33. Основные компоненты PKI.
34. Функции удостоверяющего и регистрационного центров, репозитория, архива сертификатов, серверных компонентов PKI.
35. Службы сертификации в ОС Windows.
36. Основные действия необходимые для установки и базовой настройки службы сертификации ActiveDirectory® (AD CS) в тестовой среде.
37. Служба управления правам ADRMS.
38. Шифрование IPsec в ОС Windows.
39. NATTraversal в IPsec.
40. Компоненты NAP.
41. Протокол RADIUS.
42. Сервер сетевых политик.
43. Сетевая система обнаружения и предотвращения вторжений.
44. Выявление вторжений.
45. Методы предотвращения вторжений.
46. Способы обхода системы обнаружения вторжений.
47. Хостовая система обнаружения вторжений.
48. Мониторинг файловой системы.
49. Обнаружение rootkit.
50. Honeypot. Виды, классификация.
51. Обнаружение Honeypot.
52. Security Information and Event Management.
53. Log Management System
54. Security Log/Event Management
55. Security Information Management
56. Security Event Correlation

57. Security Information and Event Management.
58. Функции SIEM

Перечень самостоятельных работ
1. Создание бюджетов пользователя в ОС Windows, UNIX.
2. Использование списков доступа в ОС Windows, UNIX.
3. Аудит в Windows, UNIX.
4. Оценка защищенности заданной конфигурации Windows.
5. Создание сертификатов в PKI.
6. Создание смарт-карт в PKI.
7. Создание репозитория сертификатов и восстановление ЦС.
8. Создание шаблонов RMS для защиты офисных документов.
9. Создание дополнительных сценариев резервного копирования.
10. Создание политик сетевого доступа.

Перечень лабораторных работ
1. Изучение систем безопасности ОС Windows, UNIX. Создание бюджетов пользователя. Использование списков доступа.
2. Аудит событий в ОС Windows, UNIX.
3. Оценка защищенности заданной конфигурации Windows: файловая система, реестр, список пользователей, политика безопасности в области паролей.
4. Интеграция сетей Microsoft и UNIX с использованием сервера Samba.
5. Изучение средств защиты сетевого взаимодействия Unix.
6. Поиск программных закладок в заданной консультации Windows.
7. Использование возможностей файловой системы ОС Windows для шифрования файлов BitLocker, EFS.
8. Изучение инфраструктуры открытых ключей. Создание смарт-карт. Защита конфигурации ADCS.
9. Изучение дополнительных мер безопасности (резервное копирование, работа со службой обновления).
10. Изучение протокола RADIUS.
11. Развертывание и внедрение виртуальной частной сети.
12. Внедрение параметров политики с помощью сервера сетевых политик.
13. Настройка и разработка правил для NIPS/NIDS Snort.
14. Настройка и разработка правил для HIDS OSSEC.
15. Настройка системы Honeypot и интеграция с SIEM.
16. Отправка уведомлений OSSEC.
17. SIEM Splunk.

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

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к зачету (8 семестр)
1. Подсистема защиты информации в ОС UNIX.
2. Passwd и shadow файлы.
3. Основные компоненты подсистем защиты UNIX.
4. Права доступа к элементам файловой системы.
5. Управление процессами.
6. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах.
7. Аудит событий.
8. Бюджет пользователя в ОС Windows.
9. Список доступа в ОС Windows.
10. Аудит в Windows, UNIX.
11. Подсистема защиты информации в ОС Windows.
12. Основные компоненты подсистем защиты Windows.
13. Политики безопасности.
14. Понятие домена.
15. Основы взаимодействия элементов гетерогенных сетей.
16. Шлюзы NFS.
17. Программно-аппаратные методы и средства ограничения доступа к ресурсам ПЭВМ.
18. Методы и средства ограничения доступа к компонентам ПЭВМ.
19. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим

носителям.
20. Методы и средства хранения ключевой информации.
21. Программная закладка.
22. Инфраструктура открытых ключей PKI.
23. Основные компоненты PKI.
24. Функции удостоверяющего и регистрационного центров, репозитория, архива сертификатов, серверных компонентов PKI.
25. Службы сертификации в ОС Windows.
26. Основные действия необходимые для установки и базовой настройки службы сертификации ActiveDirectory® (AD CS) в тестовой среде.
27. Служба управления правам ADRMS.
28. Шифрование IPsec в ОС Windows.
29. NATTraversal в IPsec.
30. Компоненты NAP.
31. Протокол RADIUS.
32. Сервер сетевых политик.

Перечень вопросов к экзамену (9 семестр)
1. Типовые модели управления доступом.
2. Дискреционное управление доступом.
3. Изолированная программная среда.
4. Мандатное управление доступом.
5. Архитектура безопасности ОС Windows.
6. Security accounts manager.
7. LM, NTLM, NTLM2, NTLMv2.
8. Kerberos.
9. Реестр ОС Windows.
10. Microsoft Management Console.
11. Архитектура безопасности ОС Unix.
12. Базовая файловая структура.
13. Права доступа к файлам и директориям.
14. Passwd и shadow файлы.
15. Аудит событий.
16. Аудит в ОС Windows.
17. Аудит в ОС Unix.
18. Сетевая система обнаружения и предотвращения вторжений.
19. Выявление вторжений.
20. Методы предотвращения вторжений.
21. Способы обхода системы обнаружения вторжений.
22. Хостовая система обнаружения вторжений.
23. Мониторинг файловой системы.
24. Обнаружение rootkit.
25. Honeypot. Виды, классификация.
26. Обнаружение Honeypot.
27. Security Information and Event Management.
28. Log Management System
29. Security Log/Event Management
30. Security Information Management
31. Security Event Correlation
32. Security Information and Event Management.
33. Функции SIEM.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
Часть 1 (8 семестр)
В течение семестра студент должен выполнить двенадцать лабораторных работ, каждая из которых оценивается в 5 баллов.
Максимальный балл за лабораторную работу – 5 баллов.
Максимальный балл за лабораторные работы в 8 семестре 60 баллов.
В течение семестра студент должен выполнить четыре самостоятельных работы, каждая из которых оценивается в 5

баллов.
Допуском до проведения зачета являются сданные студентом лабораторные и самостоятельные работы в течение семестра.
Зачет проводится в один этап, на котором студент отвечает один теоретический вопрос и выполняет одно практическое задание из списка лабораторных и самостоятельных работ. Продолжительность – 30 минут.
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Максимальный балл за практическую часть зачета – 10 баллов.

Сводная таблица рейтинга успеваемости (8 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-12	12x5=60
2	Самостоятельная работа № 1-4	4x5=20
3	Зачет (теоретический вопрос)	10
4	Зачет (практическая часть)	10
Итого		100

Часть 2 (9 семестр)
В течение семестра студент должен выполнить пять лабораторных работ, каждая из которых оценивается в 5 баллов.
Максимальный балл за лабораторную работу – 5 баллов.
Максимальный балл за лабораторные работы в 9 семестре – 25 баллов.
В течение семестра студент должен выполнить шесть самостоятельных работы, каждая из которых оценивается в 5 баллов.
Допуском до проведения экзамена являются сданные студентом лабораторные и самостоятельные работы в течение семестра.
Экзамен проводится в один этап, на котором студент отвечает на два теоретических вопроса и выполняет одно практическое задание из списка лабораторных и самостоятельных работ. Продолжительность – 30 минут.
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Максимальный балл за практическую часть экзамена – 20 баллов.

Сводная таблица рейтинга успеваемости (8 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-5	5x5=25
2	Самостоятельная работа № 1-6	6x5=30
3	Посещаемость (все занятия)	5
3	Экзамен (теоретический вопрос)	2x10=20
4	Экзамен (практическая часть)	20
Итого		100

Критерии оценивания теоретического вопроса зачета и экзамена
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом. 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.

Критерии оценивания практической части (практического задания) зачета
Максимальный балл за ответ на теоретический вопрос – 10 баллов.
Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом. 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.

Критерии оценивания практической части (практического задания) экзамена
Максимальный балл за практическую часть экзамена – 20 баллов.
Отлично/зачтено/17-20 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов и названий. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/13-16 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения, грамотно изъясняется с использованием точных терминов и названий. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/8-12 баллов - Обучающийся знаком с материалом, но допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-8 баллов - 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, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
4 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
3 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
2 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
1 балл – при выполнении лабораторной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.
0 баллов – не выполнена лабораторная работа.

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

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.
В течении семестра проводится лабораторные работы, проверяются самостоятельные работы по одному из рассматриваемых разделов, которые осуществляют срез знаний по основным понятиям, определениям и задачам.
Для зачета:
0–60 баллов – выставляется «не зачтено»
от 61 баллов и выше – выставляется «зачтено»
Для экзамена:
0-60 баллов – неудовлетворительно (2);

61-74 баллов – удовлетворительно (3);
75-90 баллов – хорошо (4);
91-100 баллов – отлично (5).

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Бражук А. И.	Сетевые средства Linux: курс лекций (https://biblioclub.ru/index.php?page=book&id=428794)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л1.2	Проскурин В. Г., Крутов С. В., Мацкевич И. В.	Защита в операционных системах: программно-аппаратные средства обеспечения информационной безопасности : учебное пособие для вузов	Москва : Радио и связь, 2000	
Л1.3	Гарькушев А.Ю., Липис А.В., Карпова И.Л.	Основы обеспечения безопасности операционных систем: учебное пособие (https://znanium.ru/catalog/document?id=451739)	Вологда : Инфра-Инженерия, 2024	ЭБС
Л1.4	Окороков В. А.	Безопасность операционных систем: учебное пособие для вузов (https://e.lanbook.com/book/367472)	Санкт- Петербург : Лань, 2024	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
Л2.3	Баланов А. Н.	Комплексная информационная безопасность: учебное пособие для вузов (https://e.lanbook.com/book/414947)	Санкт- Петербург : Лань, 2024	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Reader

Notepad++

Visual Studio

VirtualBox

Ubuntu Linux

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 рассматриваются вопросы организации аудита доступа к объектам файловой системы, оценки защищенности заданной конфигурации ОС, создание локальной политики паролей и проч. 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 «Защита в операционных системах»
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