УТВЕРЖДЕНО

решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 05 2024г., протокол №_5/24__
Председатель _____Волков М.А._
«_21_» ____05_ _____ 2024_ _____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Безопасность операционных систем**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4 - очная форма обучения

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Иванцов Андрей Михайлович	Кафедра информационной безопасности и теории управления	Доцент,Кандидат технических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Цели освоения дисциплины:

·приобретение общих представлений о реализации механизмов защиты информации в современных операционных системах;

·знакомство с основными концепциями организации безопасности на уровне операционных систем.

Задачи освоения дисциплины:

Задачи освоения дисциплины:

·изучение различных подходов реализации безопасности на уровне файловых систем и систем хранения данных;

·дать основы системного подхода к организации аутентификации и авторизации пользователей;

·дать основы системам проведения аудитов безопасности операционных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность операционных систем» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-12, ОПК-13, ОПК-15.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Безопасность систем баз данных, Безопасность вычислительных сетей, Научно-исследовательская работа, Подготовка к сдаче и сдача государственного экзамена, Программно-аппаратные средства защиты информации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных	**знать**: основные принципы обеспечения безопасности вычислительных сетей, операционных систем и баз данных

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
систем;	при разработке автоматизированных систем **уметь**: применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем **владеть**: навыками применения знаний в области безопасности вычислительных сетей, операционных систем и баз данных
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;	**знать**: порядок администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем **уметь**: осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем **владеть**: навыками администрирования и контроля функционирования средств и систем защиты информации автоматизированных систем, инструментального мониторинга защищенности автоматизированных систем
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	**знать**: порядок диагностики и тестирования систем защиты информации автоматизированных систем **уметь**: организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем **владеть**: навыками организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 5 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 180 часов

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)	
	Всего по плану	В т.ч. по семестрам
		7
1	2	3
Контактная работа обучающихся с	90	90

Вид учебной работы	**Количество часов (форма обучения очная)**	
	Всего по плану	**В т.ч. по семестрам**
		7
1	**2**	**3**
преподавателем в соответствии с УП		
Аудиторные занятия:	90	90
Лекции	36	36
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	36	36
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Экзамен (18)	Экзамен
Всего часов по дисциплине	180	180

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	**Всего**	**Виды учебных занятий**					**Форма текущего контроля знаний**
		Аудиторные занятия			**Занятия в интерактивной форме**	**Самостоятельная работа**	
		Лекции	**Практические занятия, семинары**	**Лабораторные работы, практикумы**			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Раздел 1. Защита информации в современных информационных системах							
Тема 1.1. Основные понятия и положения защиты инормации в информационных системах	4	2	0	0	0	2	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 1.2. Угрозы безопасности информации в информационно-вычислительных системах	8	2	2	0	0	4	Тестирование
Тема 1.3. Программно-технический уровень обеспечения информационной безопасности и его организация	8	2	2	0	0	4	Тестирование
Раздел 2. Подсистема безопасности в ОС семейства Windows							
Тема 2.1. Анализ подсистемы безопасности в ОС семейства Windows	12	4	0	4	0	4	Тестирование
Тема 2.2. Идентификация, аутентификация и авторизация в ОС семейства Windows	16	2	2	4	0	8	Тестирование
Тема 2.3. Аудит в ОС семейства	16	4	4	4	0	4	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Windows							
Тема 2.4. Возможности шифрования файлов в ОС семейства Windows	12	4	0	4	0	4	Тестирование
Тема 2.5. Прочие возможности подсистемы безопасности в ОС семейства Windows	4	2	0	0	0	2	Тестирование
Тема 2.6. Усиление подсистемы безопасности в ОС семейства Windows	14	4	2	4	2	4	Тестирование
Раздел 3. Подсистема безопасности в ОС семейства UNIX							
Тема 3.1. Анализ подсистемы безопасности в ОС семейства UNIX	18	4	2	6	6	6	Тестирование
Тема 3.2. Идентификация, аутентификация и авторизация в ОС	16	4	2	4	4	6	Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
семейства UNIX							
Тема 3.3. Аудит в ОС семейства UNIX	16	2	2	6	6	6	Тестирование
Итого подлежит изучению	144	36	18	36	18	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Защита информации в современных информационных системах

Тема 1.1. Основные понятия и положения защиты инормации в информационных системах

Предмет защиты информации. Понятия информации и информационных ресурсов. Достоверность, ценность и своевременность информации. Предмет защиты информации. Объект защиты информации. Понятия информационной системы. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности информационных систем. Трехэтапная разработка мер по обеспечению безопасности информационных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС). Положения по защите АС. Принципы, позволяющие реализовать положения по защите АС. Принцип системности. Принцип комплексности. Принцип непрерывной защиты. Разумная достаточность. Гибкость системы защиты. Открытость алгоритмов и механизмов защиты. Принцип простоты применения средств зашиты.

Тема 1.2. Угрозы безопасности информации в информационно-вычислительных системах

Понятие угрозы. Понятие атаки. Понятие злоумышленника. Источники угроз. Окно опасности. Критерии классификации угроз. Базовые признаки угроз информационной безопасности. Классификация угроз по природе возникновения. Классификация угроз по степени преднамеренности проявления. Классификация угроз по непосредственному источнику угроз. Классификация угроз по положению источника угроз. Классификация угроз по степени

зависимости от активности АС. Классификация угроз по степени воздействия на АС. Классификация угроз по этапам доступа пользователей или программ к ресурсам АС. Классификация угроз по способу доступа к ресурсам АС. Классификация угроз по текущему месту расположения информации, хранимой и обрабатываемой в АС. Доступность информации. Угроза доступности. Целостность информации. Угроза нарушения целостности. Конфиденциальность информации. Угроза нарушения конфиденциальности. Угроза раскрытия параметров АС. Методы обеспечения информационной безопасности. Структуризация методов обеспечения информационной безопасности. Уровни доступа к защищаемой информации. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников.

Тема 1.3. Программно-технический уровень обеспечения информационной безопасности и его организация

Подходы к обеспечению компьютерной безопасности. Сервис безопасности. Основные и вспомогательные сервисы безопасности. Понятие полного набора. Виды сервисов безопасности. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации. Проблема надежной аутентификации и пути ее решения. Средства и методы хранения эталонных копий аутентификационной информации. Протоколы передачи аутентификационной информации по каналам вычислительной сети. Криптографическое обеспечение аутентификации пользователей. Парольная аутентификация. Виды парольной аутентификации. Преимущества и недостатки парольной аутентификации. Повышение надежности парольной аутентификации. Средства и методы защиты от компрометации и подбора паролей. Биометрическая аутентификация. Общая схема биометрической аутентификации. Преимущества и недостатки биометрической аутентификации. Достоинства и недостатки различных схем биометрической аутентификации. Требования к защите компьютерной информации. Общие положения. Характеристики подходов к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к набору и параметрам механизмов защиты. Необходимые требования. Дополнительные требования. Формализованные требования к защите информации от несанкционированного доступа. Общие подходы к построению систем защиты компьютерной информации. Нормативные документы Гостехкомиссии РФ, регламентирующие защиту информации от несанкционированного доступа. Формализованные требования к защите компьютерной информации АС. Основные подсистемы и группы механизмов защиты АС. Требования к защите конфиденциальной информации. Требования к защите секретной информации. Различия требований и основополагающих механизмов защиты от несанкционированного доступа.

Раздел 2. Подсистема безопасности в ОС семейства Windows

Тема 2.1. Анализ подсистемы безопасности в ОС семейства Windows

Основные механизмы защиты в ОС семейства Windows. Принципиальные недостатки защитных механизмов ОС семейства Windows

Тема 2.2. Идентификация, аутентификация и авторизация в ОС семейства Windows

Возможности подсистемы безопасности в ОС семейства Windows. Модель безопасности для подсистемы безопасности в ОС семейства Windows. Механизм идентификации пользователей. Идентификатор защиты SID пользователей. Идентификаторы полномочий. Возможные значения идентификатора полномочий. Относительный идентификатор. Маркер доступа и привилегии пользователя. Просмотр привилегий пользователя. Команда whoami и ее параметры. Ограничивающие маркеры доступа. Команда runas и ее параметры. API функции для создания маркеров доступа. Защита объектов системы. Дескриптор безопасности SD. Атрибуты дескриптора безопасности. Парольная аутентификация в ОС семейства Windows. Механизм аутентификации. Средства управления параметрами аутентификации. Учетные записи пользователей. Локальные учетные записи пользователей. База данных SAM. Возможности получения доступа к SAM. Организация защиты SAM от несанкционированного доступа. Авторизация в ОС семейства Windows. Недостатки в организации разграничения доступа к файлам в ОС семейства Windows. Механизм авторизации в ОС семейства Windows. Маркеры доступа. Дескриптор безопасности. Формат дескрипторов безопасности. Список контроля доступа ACL. Системный (SACL) и пользовательский (DACL) списки управления доступом. Структура списков управления доступом. Возможность управления правами доступа с помощью API. Пример проверки прав доступа пользователя к объекту. Изменение прав доступа к объекту. Смена владельца объекта. Команда cacls и ее параметры.

Тема 2.3. Аудит в ОС семейства Windows

Подсистема аудита в ОС семейства Windows. Категории аудита. Оснастка gpedit.msc. Настройка списка SACL. API функции для работы с SACL. Просмотр событий аудита. Утилита Event Viewer. Оснастка eventvwr.msc. Журналы аудита. Типы регистрируемых событий в журналах аудита. Настройка журналов аудита. Типы записей в журналах событий. Определение набора подлежащих аудиту событий.

Тема 2.4. Возможности шифрования файлов в ОС семейства Windows

Шифрующая файловая система EFS. Возможности шифрующей файловой системы EFS. Принципы работы EFS. Используемые в EFS алгоритмы шифрования. Случайный ключ для шифрования файла FEK. Шифрование ключа FEK. Команда cipher и ее параметры. Понятие агента восстановления. Добавление агентов восстановления. Сертификаты агентов восстановления. Поле восстановления данных DRF. API функции для работы с EFS. Система шифрования дисков BitLocker. Основные возможности BitLocker. Поддерживаемые алгоритмы шифрования. Принцип работы. Механизмы проверки подлинности и расшифровки. Уязвимости BitLocker. Настройка BitLocker. Шифрование и дешифрование дисков при помощи BitLocker.

Тема 2.5. Прочие возможности подсистемы безопасности в ОС семейства Windows

Интерфейс CryptoAPI. Возможности CryptoAPI. Работа с поставщиками службы шифрования CSP. Типы CSP в ОС семейства Windows. Контроль учетных записей пользователей UAC. Предпосылки к появлению UAC. Принцип работы UAC. События, приводящие к срабатыванию UAC. Настройка UAC. Недостатки UAC. Шаблоны безопасности в ОС семейства Windows. Возможности шаблонов безопасности. Настройки шаблонов безопасности.

Тема 2.6. Усиление подсистемы безопасности в ОС семейства Windows

Использование систем криптографической защиты информации. Наиболее известные системы криптографической защиты информации и особенности их работы. Противодействие вирусным атакам в системе. Выбор антивируса. Организация антивирусной защиты.

Раздел 3. Подсистема безопасности в ОС семейства UNIX

Тема 3.1. Анализ подсистемы безопасности в ОС семейства UNIX

Основные механизмы защиты в ОС семейства UNIX. Особенности организации файловой системы в UNIX. Принципиальные недостатки защитных механизмов ОС семейства UNIX.

Тема 3.2. Идентификация, аутентификация и авторизация в ОС семейства UNIX

Особенности подсистемы безопасности в ОС семейства UNIX. Единая модель безопасности для ОС семейства UNIX. Парольная аутентификация в UNIX. Зарегистрированные пользователи системы. Учетный файл зарегистрированных пользователей /etc/passwd. Содержимое файла /etc/passwd. Подключаемые модули аутентификации PAM. Основы PAM. Настройка PAM. Механизм идентификации пользователей. Идентификаторы пользователей UID, RUID, EUID. Учетный файл зарегистрированных групп /etc/group. Идентификаторы групп пользователей GID, RGID, EGID. Суперпользователи и привилегированные группы. Возможности суперпользователей и привилегированных групп. Хранение паролей в других файлах в ОС семейства UNIX. Командные интерпретаторы в ОС семейства UNIX. Авторизация в ОС семейства UNIX. Особенности доступа к файлам в ОС семейства UNIX. Классы доступа к файлу. Список прав доступа к файлу. Различие возможных значений прав доступа для разных типов файлов. Изменение прав доступа к файлу утилитой chmod. Формат команд для утилиты chmod. Проверка прав доступа при обращении к файлам в ОС UNIX. Дополнительные права SUID, SGID, Sticky-бит. Применение дополнительных прав. Работа из-под root. Особенности работы из-под root. Выполнение операций от имени root. Команда su и утилита sudo. Файл sudoers. Редактирование файла sudoers с помощью утилиты visudo.

Тема 3.3. Аудит в ОС семейства UNIX

Подсистема аудита в UNIX. Централизованная система регистрации системных сообщений Syslog. Возможности системы Syslog. Компоненты Syslog. Работа системы Syslog. Файл конфигурации Syslog syslog.conf. Селекторы Syslog. Средства и уровни Syslog. Действия с сообщениями Syslog. Утилита newsyslog. Работа утилиты newsyslog. Файл конфигурации newsyslog.conf.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Защита информации в современных информационных системах

Тема 1.2. Угрозы безопасности информации в информационно-вычислительных системах

Вопросы к теме:

Очная форма

1. Понятия угрозы, атаки, злоумышленника. Источники угроз.
2. Классификация угроз.
3. Методы обеспечения информационной безопасности. Уровни доступа к защищаемой информации.
4. Основные направления и методы реализации угроз информационной безопасности.

Тема 1.3. Программно-технический уровень обеспечения информационной безопасности и его организация

Вопросы к теме:

Очная форма

1. Подходы к обеспечению компьютерной безопасности. Сервис безопасности.
2. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации.
3. Требования к защите компьютерной информации.
4. Общие подходы к построению систем защиты компьютерной информации.
5. Различия требований и основополагающих механизмов защиты от несанкционированного доступа.

Раздел 2. Подсистема безопасности в ОС семейства Windows

Тема 2.2. Идентификация, аутентификация и авторизация в ОС семейства Windows

Вопросы к теме:

Очная форма

1. Модель безопасности для подсистемы безопасности в ОС семейства Windows.
2. Механизм идентификации пользователей. Идентификатор защиты SID пользователей.
3. Парольная аутентификация в ОС семейства Windows. Механизм аутентификации.
4. Структура списков управления доступом. Возможность управления правами доступа с помощью API.

Тема 2.3. Аудит в ОС семейства Windows

Вопросы к теме:

Очная форма

1. Подсистема аудита в ОС семейства Windows. Категории аудита.
2. Просмотр событий аудита. Утилита Event Viewer.
3. Журналы аудита. Типы регистрируемых событий в журналах аудита. Настройка журналов аудита.
4. Определение набора подлежащих аудиту событий.

Тема 2.6. Усиление подсистемы безопасности в ОС семейства Windows

Вопросы к теме:

Очная форма

1. Использование систем криптографической защиты информации.
2. Противодействие вирусным атакам в системе. Выбор антивируса.
3. Организация антивирусной защиты.

Раздел 3. Подсистема безопасности в ОС семейства UNIX

Тема 3.1. Анализ подсистемы безопасности в ОС семейства UNIX

Вопросы к теме:

Очная форма

1. Основные механизмы защиты в ОС семейства UNIX.
2. Особенности организации файловой системы в UNIX.
3. Принципиальные недостатки защитных механизмов ОС семейства UNIX.
4. Сравнительный анализ механизмов защиты ОС семейства UNIX и Windows.

Тема 3.2. Идентификация, аутентификация и авторизация в ОС семейства UNIX

Вопросы к теме:

Очная форма

1. Особенности подсистемы безопасности в ОС семейства UNIX. Единая модель безопасности для ОС семейства UNIX.
2. Парольная аутентификация в UNIX. Зарегистрированные пользователи системы.
3. Учетный файл зарегистрированных пользователей /etc/passwd. Содержимое файла /etc/passwd.
4. Подключаемые модули аутентификации PAM. Основы PAM. Настройка PAM.
5. Механизм идентификации пользователей. Идентификаторы пользователей UID, RUID, EUID.
6. Суперпользователи и привилегированные группы. Возможности суперпользователей и привилегированных групп.
7. Дополнительные права SUID, SGID, Sticky-бит. Применение дополнительных прав.

Тема 3.3. Аудит в ОС семейства UNIX

Вопросы к теме:

Очная форма

1. Подсистема аудита в UNIX.
2. Централизованная система регистрации системных сообщений Syslog. Возможности системы Syslog. Компоненты Syslog.
3. Средства и уровни Syslog. Действия с сообщениями Syslog.
4. Утилита newsyslog. Работа утилиты newsyslog. Файл конфигурации newsyslog.conf.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Пользователи и группы
Цели: Изучение системы администрирования пользователей и групп в операционных системах. Изучение системы защиты информации файловых систем NTFS (MS Windows) и ext4fs (BaseAlt (Альт Рабочая станция, Альт сервер)). Реализация системы разграничение прав доступа к каталогам файловой системы и файлам. Разграничение прав доступа к файловой системе по сети. Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).
Содержание: • Разработать политику именования сотрудников организации. • Необходимо создать пользователей в ОС в соответствии с разработанной политикой: Корейко Александр Иванович Балаганов Шура Mr. Panikovskii Mikhail Samuelivich Остап Бендер • Необходимо создать группы пользователей в ОС: Руководство, Планово-финансовый отдел, Департамент инженерных решений. • Включить каждого пользователя в свою группу: Бендер -> Руководство, Балаганов -> Департамент инженерных решений, Panikovskii -> Планово-финансовый отдел. • Создать каталог ООО Рога и Копыта, в нем каталоги Общие документы, Финансовые отчеты, Поставщики. • Назначить права для данных каталогов в соответствии с матрицей доступа Руководство Планово-финансовый отдел Департамент инженерных решений Корейко Общие документы Ч,З Ч,З Ч,З - Финансовые отчеты Ч Ч,З - - Поставщики Ч - Ч,З - • В каталоге «Поставщики» создать файл Особой важности.txt предоставить доступ только к этому файлу для чтения членам «Планово-финансового отдел» • Предоставить общий доступ к папке Общие документы через сеть. • Предоставить доступ к папке Общие документы для Корейко, только для чтения. • Запретить пользователям Планово-финансового отдела хранить больше 1Мб информации в папке Общие документы.
Результаты: Изучены системы администрирования пользователей и групп в операционных системах. Изучены системы защиты информации файловых систем NTFS (MS Windows) и ext4fs (BaseAlt (Альт Рабочая станция, Альт сервер)). Реализованы системы разграничение прав доступа к каталогам файловой системы и файлам.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739

Массовая регистрация пользователей
Цели: Изучение системы администрирования пользователей при помощи стандартного API операционной системы. Изучение методов назначения прав доступа к объектам файловой системы из скриптовых языков. Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).
Содержание: В файле в формате csv создан список более 100 пользователей, содержащий ФИО сотрудников, которым необходимо предоставить доступ к компьютеру: Васисуалий Лоханкин, v.lohankin@roga-kopita.ru Зося Синицкая, z.sinickaya@roga-kopita.ru В соответствии с разработанной политикой именования сотрудников создать всех пользователей при помощи скрипта. Создать в каталоге ООО Рога и Копыта каталог Пользовательские данные Создать каталоги для каждого пользователя и назначить пользователей владельцем своего каталога. Запретить всем другим пользователям доступ к данному каталогу. Разрешить группе Руководство доступ к каталогу для чтения и записи.
Результаты: Изучены системы администрирования пользователей при помощи стандартного API операционной системы. Изучены методы назначения прав доступа к объектам файловой системы из скриптовых языков.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Политика безопасности
Цели: Изучение возможности управления групповой политики операционных систем семейства Microsoft Windows.
Содержание: Задание №1. Выполняется только под ОС Microsoft Windows 10 и Microsoft Windows Server. 1. Определите следующую политику паролей: 1.1. Установите количество запоминаемых паролей равное 10. 1.2. Установите срок действия паролей равным 10 дням. 1.3. Установите минимальный срок действия пароля равным 5 дням. 1.4. Потребуйте установку пароля, отвечающего требованиям сложности. 1.5. Установите длину пароля не менее 5 символов. 1.6. Отключите использование обратного шифрования при хранении паролей. 2. Задайте политику блокировки учетных записей: 2.1. Определите блокировку учетной записи через 3 неудачных попытки входа в систему. 2.2. Определите блокировку учетной записи после неудачных попыток входа на 10 мин. 2.3. Определите время в течение, которого подсчитываются неудачные попытки входа равным 15 мин. 3. Сделайте регистрацию следующих событий: 3.1. Вход в систему (успех). 3.2. Доступ к объектам (успех). 3.3. Доступ к службе каталогов (успех). 3.4. Изменение политики (успех). 3.5. Использование привилегий (успех). 3.6. Отслеживание процессов (успех). 3.7. Системные события (успех). 3.8. События входа в систему (успех). 3.9. Управление учетными записями (успех). Задание №2. Осуществите три неудачные попытки входа в систему. Продемонстрируйте работу системных журналов регистрации событий входа.
Результаты: Изучены возможности управления групповой политики операционных систем семейства Microsoft Windows.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Ограниченное использование программ
Цели: Изучение возможности изменения уровней безопасности операционной системы путем блокирования определённых приложений
Содержание: Задача. Выполнять только для ОС Microsoft Windows 10 и Microsoft Server. 1. Задайте политику безопасности по «белому списку». 2. Добавьте к исполняемым файлам, файлы с расширением «.isp». 3. Разрешите всем пользователям проверять сертификаты. 4. Запретите по хеш-значению запуск программы «Калькулятор». 5. Запретите установку программ, загруженных из Интернета.

Результаты: Изучены возможности изменения уровней безопасности операционной системы путем блокирования определённых приложений
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Взлом паролей пользователей
Цели: Взлом паролей Microsoft Windows 10.
Содержание: 1. Установить на виртуальную машину Windows 10. 2. Создать трех пользователей с именами ФИО-Низкий, ФИО-Средний, ФИО-Высокий, где ФИО-ваша фамилия имя отчество. Например: 3. КАЕ-Низкий, КАЕ-Средний, КАЕ-Высокий. 4. Установить для каждого пользователя свой пароль. 5. Для Низкий - 6 букв и цифр латинского алфавита. 6. Для Средний - 12 букв и цифр латинского алфавита. 7. Для Высокий - 15 символов включая заглавные и прописные буквы, цифры, спец. символы. 8. Сохранить все файлы в файл Lab3\pass.txt 9. Найти bootkey ОС Windows. 10. Выгрузить базу паролей SAM. 11. Взломать пароли используя любую утилиту Kali Linux. Например john.
Результаты: Осуществлён успешный взлом паролей Microsoft Windows 10.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Прозрачное шифрование файловой системы
Цели: Изучение возможностей применения «прозрачного» шифрования данных в файловых системах.
Содержание: Задача. Организация защиты исполняемого кода. Выполняется для ОС Windows Server и для BaseAlt (Альт Рабочая станция, Альт сервер). Возможно использование LUKS или LVM. • Установить WEB сервер apache или ngnix. Создать каталог www для хранения данных сайта в каталоге ООО Рога и Копыта. • Настроить отображение тестовой страницы index.html для данного сайта. • Создать пользователя web-www с правами только чтения и записи данных в каталог www. • Настроить шифрование файлов для каталога www и установить ключи шифрования для пользователя Остап Бендер и для web-www. • Все остальные пользователи не должны иметь доступ каталогу. • Проверить чтение файла index.html под другим пользователем.
Результаты: Изучены возможности применения «прозрачного» шифрования данных в файловых системах.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Шифрование и хеширование
Цели: Изучение методов контроля целостности и шифрования данных
Содержание: Задание №1. Выполняется для ОС Microsoft Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер). • В каталоге ООО Рога и Копыта\Финансовые отчеты создайте 1000 файлов отчетов с именами в следующем формате: yyyymmdd-report.txt, где yyyy-год, mm-месяц в виде числа, dd – день. Создание файлов реализовать скриптом начиная с текущей даты и назад в прошлое на 1000 дней. В файл записать текущее время в формате yyyymmddhhMMss. • Создать файл с контрольными суммами (hash) для всех файлов каталога. • Сгенерировать ключ шифрования данных для gpg. • Зашифровать все файлы отчетов каждый отдельно. • Заархивировать все зашифрованные файлы и файл с хеш суммами и передать его на другую ОС (с MS Windows 10 на BaseAlt (Альт Рабочая станция, Альт сервер) и наоборот). • Распаковать файлы и расшифровать их. Проверить все хеш суммы файлов. • Изменить один из файлов и продемонстрировать, что хеш суммы у файлов не совпадают. Задание №2. Выполняется для ОС Microsoft Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер). • Установить на виртуальные машины КриптоАРМ ГОСТ. Внимание! Программа будет работать только 14 дней. Используйте копии виртуальных машин. • Сформируйте тестовый квалифицированный сертификат электронной подписи в тестовом удостоверяющем центре КриптоПро. • Сформируйте квалифицированную электронную подпись для

архива отчетов. • Зашифруйте архив и передайте его на другую ОС. • Расшифруйте архив при помощи сертификата и проверьте электронную подпись документов. • Дополнительное задание. Сохраните закрытый ключ и сертификат ключа на отчуждаемом носителе (RuToken, Jacarta и т.д.). и выполните полностью задание №2.
Результаты: Изучены основные методы контроля целостности и шифрования данных
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Отказоустойчивость. RAID массивы
Цели: Изучение возможностей программных средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации
Содержание: Задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер). • Создать программный отказоустойчивый RAID0 массив в ОС состоящий из двух и более жестких дисков (флеш кард, независимых дисков). • Сформировать 100 файлов по 100 мегабайт данных. • Разработать скрипт копирующий данные на RAID массив и засекающий время копирования информации. • Считать данные с RAID массива и зафиксировать время чтения данных. • Повторить эксперимент не менее 25 раз. • Провести графический статистический анализ результатов быстродействия RAID массива. Повторить все шаги для RAID массивов уровня 1 и 5. Подготовить сравнительный анализ быстродействия каждого из типов RAID массивов в различных ОС. • Дополнительное задание. Провести тестирование аппаратных RAID контроллеров, встроенных в сервера лаборатории или ваши персональные компьютеры при наличии не менее двух независимых жестких дисков.
Результаты: Изучены возможности программных средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Домены
Цели: Изучение возможностей создания контура безопасности предприятия на основе доменной структуры. Применение групповых политик безопасности к пользователям и компьютерам предприятия
Содержание: Задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер). • Установить роль «Контролера домена» в ОС Microsoft Windows Server. • Включить в домен одну рабочую станцию на ОС Microsoft Windows 10. • Включить в домен одну рабочую станцию на ОС BaseAlt (Альт Рабочая станция, Альт сервер). • Выполнить Лабораторную работу №1 Пользователи и Группы для домена. • Продемонстрировать доступ к общим папкам со всех рабочих станций. • Дополнительное задание. Настроить единое хранилище профилей пользователя на сетевом диске сервера. Продемонстрировать миграцию профилей пользователя.
Результаты: Изучены возможности создания контура безопасности предприятия на основе доменной структуры. Применены групповые политики безопасности к пользователям и компьютерам предприятия
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739
Аудит событий
Цели: Изучение механизмов регистрации различных событий в ОС. Ознакомление с методами анализа событий по различным критериям
Содержание: Задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер). • Настроить политику регистрации событий входа в систему и ошибок входа в систему для домена. • Распространить политику на все компьютеры домена. • Написать скрипт на powershell получающий все журналы событий с компьютеров домена. • Провести анализ журналов событий с указанием всех отказов входа в систему для пользователя «Корейко». • Провести

локальный анализ журналов событий для ОС BaseAlt (Альт Рабочая станция, Альт сервер). Выделить все отказы входа в систему. Дополнительное задание. Выполняется для ОС Microsoft Windows Server и BaseAlt (Альт Рабочая станция, Альт сервер). • Создать каталог с файлами журналов удовлетворяющих маске: yyyymmddhhss.txt не менее 100 файлов. • Написать скрипт реализующий резервную копию данных файлов: • 1. Все файлы за прошлый месяц отправляются в архив yyyymm.zip • 2. Все файлы за прошлую неделю отправляются в архив yyyymmKW.zip KW - номер недели в году. • 3. Все файлы не старше 7 дней остаются в каталоге.
Результаты: Изучены механизмы регистрации различных событий в ОС. Студенты ознакомлены с методами анализа событий по различным критериям
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/8739

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Основные понятия и положения защиты информации в информационно вычислительных системах
2. Трехэтапная разработка мер по обеспечению безопасности информационных систем. Стадия выработки требований
3. Трехэтапная разработка мер по обеспечению безопасности информационных систем. Стадия определения способов защиты
4. Трехэтапная разработка мер по обеспечению безопасности информационных систем. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты
5. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС)
6. Угрозы безопасности информации в информационно-вычислительных системах и их классификацию
7. Доступность информации. Угроза доступности
8. Конфиденциальность информации. Угроза нарушения конфиденциальности
9. Основные направления и методы реализации угроз информационной безопасности
10. Основные понятия программно-технического уровня обеспечения информационной безопасности
11. Основные сервисы безопасности и их особенности
12. Требования к защите компьютерной информации с учетом различных нормативных документов
13. Принципиальные недостатки защитных механизмов ОС семейства Windows
14. Механизм идентификации пользователей в ОС семейства Windows
15. Механизм аутентификации пользователей в ОС семейства Windows
16. Механизмы разграничения доступа к файлам в ОС семейства Windows
17. Подсистема аудита в ОС семейства Windows. Категории аудита
18. Журналы аудита. Типы регистрируемых событий в журналах аудита
19. Файловая система EFS в ОС семейства Windows
20. Возможности шифрующей файловой системы EF

21. Работа с поставщиками службы шифрования CSP
22. Возможности CryptoAPI в ОС семейства Windows
23. Служба UAC в ОС семейства Windows
24. Шаблоны безопасности в ОС семейства Windows
25. Шифрования дисков BitLocker в ОС семейства Windows
26. Противодействие вирусным атакам в системе. Выбор антивируса
27. Организация антивирусной защиты
28. Подсистема защиты в ОС семейства Windows
29. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства Windows
30. Возможности усиления подсистемы безопасности в ОС семейства Windows
31. Основные механизмы защиты в ОС семейства UNIX
32. Особенности подсистемы безопасности в ОС семейства UNIX
33. Механизм идентификации пользователей в ОС семейства UNIX
34. Механизм аутентификации пользователей в ОС семейства UNIX
35. Подключаемые модули аутентификации PAM и работе с ними в ОС семейства UNIX
36. Механизм разграничения доступа к файлам в ОС семейства UNIX
37. Система шифрования файлов PGP в ОС семейства UNIX
38. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства UNIX
39. Bash-скрипты и работа с ними в ОС семейства UNIX
40. Возможности усиления подсистемы безопасности в ОС семейства UNIX
41. Централизованная система регистрации системных сообщений Syslog
42. Шифрование файлов при помощи PGP. Особенности PGP
43. Подсистема аудита в UNIX
44. Ведение и анализ журналов безопасности в ОС

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Защита информации в современных информационных системах			
Тема 1.1. Основные понятия и положения защиты инормации в информационных системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Вопросы к экзамену, Тестирование
Тема 1.2. Угрозы безопасности информации в информационно-вычислительных системах	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 1.3. Программно-технический уровень обеспечения информационной безопасности и его организация	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Раздел 2. Подсистема безопасности в ОС семейства Windows			
Тема 2.1. Анализ подсистемы безопасности в ОС семейства Windows	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 2.2. Идентификация, аутентификация и авторизация в ОС семейства Windows	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Вопросы к экзамену, Тестирование
Тема 2.3. Аудит в ОС семейства Windows	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 2.4. Возможности шифрования файлов в ОС семейства Windows	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Вопросы к экзамену, Тестирование
Тема 2.5. Прочие возможности подсистемы безопасности в ОС семейства Windows	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Вопросы к экзамену, Тестирование
Тема 2.6. Усиление подсистемы безопасности в ОС семейства	Проработка учебного материала с использованием ресурсов учебно-	4	Вопросы к экзамену, Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Windows	методического и информационного обеспечения дисциплины.		
Раздел 3. Подсистема безопасности в ОС семейства UNIX			
Тема 3.1. Анализ подсистемы безопасности в ОС семейства UNIX	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Вопросы к экзамену, Тестирование
Тема 3.2. Идентификация, аутентификация и авторизация в ОС семейства UNIX	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Вопросы к экзамену, Тестирование
Тема 3.3. Аудит в ОС семейства UNIX	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	6	Вопросы к экзамену, Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы
основная

1. Проскурин В.Г. Защита в операционных системах : учебное пособие / В.Г. Проскурин ; Проскурин В.Г. - Москва : Горячая линия - Телеком, 2014. - 192 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991203791.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0379-1. / .— ISBN 0_242653

2. Мартемьянов Ю.Ф. Операционные системы. Концепции построения и обеспечения безопасности : учебное пособие / Ю.Ф. Мартемьянов, А.В. Яковлев, А.В. Яковлев ; Мартемьянов Ю.Ф.; Яковлев Ал.В.; Яковлев Ан.В. - Москва : Горячая линия - Телеком, 2010. - 332 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991201285.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0128-5. / .— ISBN 0_242489

3. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов ; Душкин А.В.; Барсуков О.М.; Кравцов Е.В.; Славнов К.В. - Москва : Горячая линия - Телеком, 2016. - 248 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991204705.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0470-5. / .— ISBN 0_250838

дополнительная

1. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации : практическое пособие / Г.А. Бузов ; Бузов Г.А. - Москва : Горячая линия - Телеком, 2010. - 240 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991201216.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0121-6. / .— ISBN 0_242453

2. Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня ; Е. А. Басыня. - Новосибирск : Новосибирский государственный технический университет, 2018. - 79 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Гарантированный срок размещения в ЭБС до 05.02.2025 (автопролонгация). - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/91423.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-7782-3484-0. / .— ISBN 0_151757

3. Гостев Иван Михайлович. Операционные системы : Учебник и практикум для вузов / И.М. Гостев. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2021. - 164 с. - (Высшее образование). - https://urait.ru/bcode/470010. - https://urait.ru/book/cover/EF64B22F-9C6D-4F58-9CC5-E667300ACA28. - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-04520-8 : 539.00. / .— ISBN 0_301601

учебно-методическая

1. Клочков А. Е. Методические указания для самостоятельной работы студентов по дисциплине «Безопасность операционных систем» для студентов специалитета по специальности 10.05.03 очной формы обучения / А. Е. Клочков ; УлГУ, ФМИиАТ. - 2019. - Загл. с экрана. - Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 345 КБ). - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_42213.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Академическая лицензия на УМК ViPNet "Защита сетей"
- Альт рабочая станция
- Комплект «Максимальная защита» Средства защиты информации Secret Net Studio 8

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим

доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Кандидат технических наук, Доцент	Иванцов Андрей Михайлович
	Должность, ученая степень, звание	ФИО