УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от « 18 » 05 2021 г., протокол № 4/21
Председатель М.А. Волков
(подпись, расшифровка подписи)
« 18 » 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Безопасность операционных систем
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	2-3

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Безопасность открытых информационных систем"
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: « 01 » 09 2021 г.

Программа актуализирована на заседании кафедры: протокол № 13 от 11.05.2022 г.
Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г.
Программа актуализирована на заседании кафедры: протокол № __ от _____ 20____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент
Клочков Андрей Евгеньевич	ИБ и ТУ	Старший преподаватель

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/ _____ / Андреев А.С. / *(подпись) (Ф.И.О.)* « 12 » 05 2021 г.

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:

- 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 ВО

Дисциплина ««Безопасность операционных систем»» изучается в 4 и 5 семестрах и относится к обязательной части дисциплин блока Б1.О специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами «Информатика», «Языки программирования», «Основы информационной безопасности» и «Введение в специальность.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информатики, вычислительной техники, электроники и схемотехники;

способность анализировать проблемы и процессы;

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Безопасность сетей ЭВМ»; «Разработка и эксплуатация защищённых автоматизированных систем»; «Безопасность открытых информационных систем»; «Инструментальные средства контроля защищенности информации»; «Сертификация средств защиты информации».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
1	2
ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	**Знать:** основные принципы обеспечения безопасности вычислительных сетей, операционных систем и баз данных 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-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
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

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 10.

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

Вид учебной работы	**Количество часов (форма обучения ___*очная*_____)**			
	Всего по плану	**В т.ч. по семестрам**		
		4 семестр	**5 семестр**	
1	2	3	**4**	5
Контактная работа обучающихся с преподавателем	170	80/80*	90/90*	
Аудиторные занятия:	170	80/80*	90/90*	
Лекции	68	32/32*	36/36*	
Практические и семинарские занятия	34	16/16*	18/18*	
Лабораторные работы (лабораторный практикум)	68	32/32*	36/36 *	
Самостоятельная работа	118	64	54	
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на семинарах; - вопросы при защите лабораторных работ - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	зачёт экзамен	зачёт	Экзамен 36	
Всего часов по дисциплине:	360	180	180	

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины (модуля.) Распределение часов по темам и видам учебной работы:

Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		Лекции	Практ. занятия, семинар	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Защита информации в современных информационных системах							
1. Основные понятия и положения защиты информации в информационно вычислительных системах	8	4				4	Тесты Т1,
2. Угрозы безопасности информации в информационно-вычислительных системах	12	4	4			4	Тесты Т2,
3. Программно-технический уровень обеспечения информационной безопасности и его организация	12	4	4			4	Тесты Т3,
Раздел 2. Подсистема безопасности в ОС семейства Windows							
4. Анализ подсистемы безопасности в ОС семейства Windows	26	4		8		12	Тесты Т4, Лаб. раб 1
5. Идентификация, аутентификация и авторизация в ОС семейства Windows	30	4	4	8	4	24	Тесты Т5, Лаб. раб 2
6. Аудит в ОС семейства Windows	26	4	4	8	4	24	Тесты Т6, Лаб. раб 3
7. Возможности шифрования файлов в ОС семейства Windows	22	4		8	4	24	Тесты Т7, Лаб. раб 5
8. Прочие возможности подсистемы безопасности в ОС семейства Windows	8	4				4	Тесты Т8
9. Усиление подсистемы безопасности в ОС семейства Windows	40	10	4	12	6	14	Тесты Т9, Лаб. раб. 4, 6
Раздел 3. Подсистема безопасности в ОС семейства UNIX							
10. Анализ подсистемы безопасности в ОС семейства UNIX	36	10	4	6	6	16	Тесты Т10, Лаб. раб. 7
11. Идентификация, аутен-	34	10	6	6	6	12	Тесты Т11,

тификация и авторизация в ОС семейства UNIX							Лаб. раб. 8
12. Аудит в ОС семейства UNIX	34	6	4	12	4	12	Тесты Т12, Лаб. раб. 9, 10
Итого:	360	68	34	68	34	118	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Защита информации в современных информационных системах

Тема 1. Основные понятия и положения защиты информации в информационно вычислительных 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 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 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 4. Анализ подсистемы безопасности в ОС семейства Windows

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

Тема 5. 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 6. 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 7. 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 8. 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 9. 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 10. 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 11. 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 12. 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

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Защита информации в современных информационных системах

Тема 2. Угрозы безопасности информации в информационно-вычислительных системах (семинар).

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 3. Программно-технический уровень обеспечения информационной безопасности и его организация (семинар).

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 5. Идентификация, аутентификация и авторизация в ОС семейства Windows (семинар).

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 6. Аудит в ОС семейства Windows (семинар).

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 9. Усиление подсистемы безопасности в ОС семейства Windows (семинар).

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 10. Анализ подсистемы безопасности в ОС семейства UNIX (семинар).

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 11. Идентификация, аутентификация и авторизация в ОС семейства UNIX (семинар).

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 12. Аудит в ОС семейства UNIX (семинар).

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 (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Цель. Лабораторный практикум по дисциплине направлен на изучение студентами всех современных подходов для обеспечения информационной безопасности современных операционных систем. Охватывает клиентские операционные системе (на базе Microsoft Windows 10 и Alt Linux), а также серверные операционное системы (на базе Microsoft Server 2026R2 и Alt Linux Server). В соответствии с руководящими документами обучение происходит на сертифицированные версиях операционных систем.

Методология основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Все работы обладают дифференцированной линейно растущей сложностью выполнению и созданы на основе стандартных практических задач современного предприятия. Поиск технической информации, а также подбор необходимого решения производиться самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и процессе демонстрации полученного решения.

Результат. Полученные решения демонстрируются студентом для каждого из типа операционных систем. При необходимости демонстрируется ход выполнения работы.

Требования к оборудованию. Для выполнения работ студенты используют несколько виртуальных машин с различными версиями операционных систем. Возможно самостоятельное выполнение лабораторных работ вне лаборатории. Компьютер с жестким

диском – 100 Gb, ОЗУ: 8 Gb, Windows 10 Pro, BaseAlt (Альт Рабочая станция, Альт сервер), Kali Linux, Oracle Virtual Box, Putty, PGP, Apache, nginx, Statistica, Origin. По желанию студента все виртуальные машины могут быть развернуты на выделенном сервере виртуальных машин в лаборатории.

Раздел 2. Подсистема безопасности в ОС семейства Windows.

Тема 4. Анализ подсистемы безопасности в ОС семейства Windows

Лабораторная работа № 1 (8 часов). Пользователи и группы.

Цель. 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).

- 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.

Тема 5. Идентификация, аутентификация и авторизация в ОС семейства Windows

Лабораторная работа № 2 (8 часов). Массовая регистрация пользователей

Цель. 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).
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.

Тема 6. Аудит в ОС семейства Windows

Лабораторная работа № 3 (8 часов). Политика безопасности

Цель. Изучение возможности управления групповой политики операционных систем семейства Microsoft Windows.
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.

Тема 9. Усиление подсистемы безопасности в ОС семейства Windows

Лабораторная работа № 4 (6 часов). Ограниченное использование программ

Цель. Изучение возможности изменения уровней безопасности операционной системы путем блокирования определённых приложений.

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.

Тема 7. Возможности шифрования файлов в ОС семейства Windows

Лабораторная работа № 5 (8 часов). Взлом паролей пользователей

Взлом паролей Microsoft Windows 10.

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.

Тема 9. Усиление подсистемы безопасности в ОС семейства Windows

Лабораторная работа № 6 (6 часов). Прозрачное шифрование файловой системы

Цель. Изучение возможностей применения «прозрачного» шифрования данных в файловых системах.

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.

Раздел 3. Подсистема безопасности в ОС семейства UNIX

Тема 10. Анализ подсистемы безопасности в ОС семейства UNIX

Лабораторная работа № 7 (6 часов). Шифрование и хеширование

Цель. Изучение методов контроля целостности и шифрования данных.

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.

Тема 11. Идентификация, аутентификация и авторизация в ОС семейства UNIX

Лабораторная работа № 8 (6 часов). Отказоустойчивость. RAID массивы

Цель. Изучение возможностей программный средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации.

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.

Тема 12. Аудит в ОС семейства UNIX

Лабораторная работа № 9 (6 часов). Домены

Цель. Изучение возможностей создания контура безопасности предприятия на основе доменной структуры. Применение групповых политик безопасности к пользователям и компьютерам предприятия.

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.

Тема 12. Аудит в ОС семейства UNIX

Лабораторная работа №10 (6 часов). Аудит событий

Цель. Изучение механизмов регистрации различных событий в ОС. Ознакомление с методами анализа событий по различным критериям.

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.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Контрольные работы, рефераты и курсовые работы не предусмотрены учебным планом дисциплины.

9.1 ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

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. Целостность информации. Угроза нарушения целостности
9. Конфиденциальность информации. Угроза нарушения конфиденциальности
10. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников.
11. Основные понятия программно-технического уровня обеспечения информационной безопасности.
12. Основные сервисы безопасности и их особенности.
13. Требования к защите компьютерной информации с учетом различных нормативных документов.

14. Принципиальные недостатки защитных механизмов ОС семейства Windows.
15. Механизм идентификации пользователей в ОС семейства Windows.
16. Механизм аутентификации пользователей в ОС семейства Windows.
17. Механизмы разграничения доступа к файлам в ОС семейства Windows
18. Подсистема аудита в ОС семейства Windows. Категории аудита
19. Журналы аудита. Типы регистрируемых событий в журналах аудита
20. Файловая система EFS в ОС семейства Windows
21. Возможности шифрующей файловой системы EFS
22. Шифрования дисков BitLocker в ОС семейства Windows
23. Работа с поставщиками службы шифрования CSP
24. Возможности CryptoAPI в ОС семейства Windows
25. Служба UAC в ОС семейства Windows

9.2 ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Шаблоны безопасности в ОС семейства Windows.
2. Подсистема защиты в ОС семейства Windows.
3. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства Windows.
4. Возможности усиления подсистемы безопасности в ОС семейства Windows.
5. Противодействие вирусным атакам в системе. Выбор антивируса.
6. Организация антивирусной защиты.
7. Основные механизмы защиты в ОС семейства UNIX
8. Принципиальные недостатки защитных механизмов ОС семейства UNIX
9. Особенности подсистемы безопасности в ОС семейства UNIX.
10. Механизм идентификации пользователей в ОС семейства UNIX.
11. Механизм аутентификации пользователей в ОС семейства UNIX.
12. Подключаемые модули аутентификации PAM и работе с ними в ОС семейства UNIX.
13. Механизм разграничения доступа к файлам в ОС семейства UNIX.
14. Система шифрования файлов PGP в ОС семейства UNIX.
15. Конфигурация подсистемы защиты в ОС семейства UNIX.
16. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства UNIX.
17. Bash-скрипты и работа с ними в ОС семейства UNIX.
18. Возможности усиления подсистемы безопасности в ОС семейства UNIX
19. Централизованная система регистрации системных сообщений Syslog. Возможности системы Syslog.
20. Шифование файлов при помощи PGP. Особенности PGP
21. Подсистема аудита в UNIX
22. Ведение и анализ журналов безопасности в ОС

8. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Защита информации в современных информационных системах			
1. Основные понятия и положения защиты информации в информацион-но	Подготовка к лекции, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен

вычислительных системах			
2. Угрозы безопасности информации в информационно-вычислительных системах	Подготовка к лекции, подготовка к семинару, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен
3. Программно-технический уровень обеспечения информационной безопасности и его организация	Подготовка к лекции, подготовка к семинару, подготовка к сдаче экзамена	4	Тесты перед лекцией, экзамен
Раздел 2. Подсистема безопасности в ОС семейства Windows			
4. Анализ подсистемы безопасности в ОС семейства Windows	Подготовка к лекции, подготовка к сдаче лаб. работ, экзамена	12	Тесты перед лекцией, защита лаб. работ, экзамен
5. Идентификация, аутентификация и авторизация в ОС семейства Windows	Подготовка к лекции, подготовка к семинару, подготовка к сдаче лаб. работ, экзамену	24	Тесты перед лекцией, защита лаб. работ, экзамен
6. Аудит в ОС семейства Windows	Подготовка к лекции, подготовка к семинару, подготовка к сдаче лаб. работ, экзамену	24	Тесты перед лекцией, защита лаб. работ, экзамен
7. Возможности шифрования файлов в ОС семейства Windows	Подготовка к лекции, подготовка к сдаче лаб. работ, экзамена	24	Тесты перед лекцией, защита лаб. работ, экзамен
8. Прочие возможности подсистемы безопасности в ОС семейства Windows	Подготовка к лекции, подготовка к сдаче лаб. работ, экзамена	4	Тесты перед лекцией, защита лаб. работ, экзамен
9. Усиление подсистемы безопасности в ОС семейства Windows	Подготовка к лекции, подготовка к семинару, подготовка к сдаче лаб. работ, экзамену	14	Тесты перед лекцией, защита лаб. работ, экзамен
Раздел 3. Подсистема безопасности в ОС семейства UNIX			
10. Анализ подсистемы безопасности в ОС семейства UNIX	Подготовка к лекции, подготовка к семинару, подготовка к сдаче лаб. работ, экзамену	16	Тесты перед лекцией, защита лаб. работ, экзамен
11. Идентификация, аутентификация и авторизация в ОС семейства UNIX	Подготовка к лекции, подготовка к семинару, подготовка к сдаче лаб. работ, экзамену	12	Тесты перед лекцией, защита лаб. работ, экзамен
12. Аудит в ОС семейства UNIX	Подготовка к лекции, подготовка к семинару, подготовка к сдаче лаб. работ, экзамену	12	Тесты перед лекцией, защита лаб. работ, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1.Проскурин, В. Г. Защита в операционных системах : учебное пособие для вузов / Проскурин В. Г. - Москва : Горячая линия - Телеком, 2014. - 192 с. - ISBN 978-5-9912-0379-1. - Текст: электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991203791.html

2. Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности : учебное пособие для вузов / Мартемьянов Ю. Ф. , Яковлев Ал. В. , Яковлев Ан. В. - Москва : Горячая линия - Телеком, 2010. - 332 с. - ISBN 978-5-9912-0128-5. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785991201285.html

3. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html

дополнительная

1. Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. - М.: Горячая линия - Телеком, 2010. - 240 с. - ISBN 978-5-9912-0121-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201216.html

2. Некоммерческая интернет-версия СПС "КонсультантПлюс":

2.1 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

2.2 Федеральный закон от 27 июля 2006 г. № 149 - ФЗ «Об информации, информационных технологиях и о защите информации»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

2.3 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

2.4 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»
Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/

3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" [Электронный ресурс] : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий, Каф. информ. безопасности и теории управления. - Электрон. текстовые дан. (1 файл : 352 КБ). - Ульяновск : УлГУ, 2017 URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915/Andreev_2017.pdf

2. Андреев А. С.Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" [Электронный ресурс] / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. - Электрон. текстовые дан. (1 файл : 14, 7 Мб). - Ульяновск : УлГУ, 2015. Режим доступа http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf

3. 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. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 345 КБ). - Текст: электронный.
http://lib.ulsu.ru/MegaPro/Download/MObject/8739

Согласовано:

Гл.библ-рь НБ УлГУ	Попина И.Ю		04.05.2021
должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир.

пользователей. – Текст : электронный.

1.7. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL : http://www.edu.ru . – Текст : электронный

Согласовано:

Экспре Зам.нач. УИТиТ / Клочкова А.В. / 04.05.2021
научно должность сотрудника УИТиТ ФИО подпись дата

Согласовано:

Зам.нач. УИТиТ / Клочкова А.В. / 04.05.2021
должность сотрудника УИТиТ ФИО подпись дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций – 3/316, 2/26, 3/420, семинарских, лабораторных занятий: 3/317, 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

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: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО

Разработчик: _____ ст. преподаватель кафедры Клочков Андрей Евгеньевич
подпись должность ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 1	Андреев А.С.		11.05.2022 Протокол заседания кафедры № 13
2.	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения № 2	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12

Приложение 1

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, [2022]. – 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, [2022]. - 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, [2022]. – 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, [2022]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2022]. – 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, [2022]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. База данных «Русский как иностранный» : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2022]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase : научно-информационная база данных EBSCO // EBSCOhost

: [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал . – URL: http://window.edu.ru/ . – Текст : электронный.

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

7. Образовательные ресурсы УлГУ:

7.1. 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.

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/
должность сотрудника УИТиТ	ФИО	подпись	дата

Приложение 2

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, [2023]. – 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, [2023]. - 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, [2023]. – 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, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – 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, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com :** электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - 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, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – 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.