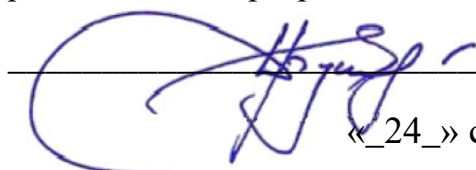


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы

 Буинцев Д.Н.
«_24_» сентября 2024 г

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.О.20 Безопасность операционных систем

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)*

Квалификация

бакалавр

Форма обучения

очная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Безопасность операционных систем составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(и):

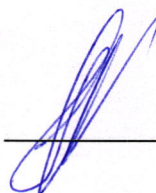
Г.В. Филиппова, старший преподаватель кафедры информатики



Рабочая программа дисциплины Безопасность операционных систем утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности
заведующего кафедрой

Г.С. Осипов



1. Цель и задачи дисциплины

Цель дисциплины

Целями освоения дисциплины *«Безопасность операционных систем»* являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по принципам администрирования подсистемы защиты информации операционных систем семейства Windows NT (Windows 7, Windows 10) и GNU/Linux достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- знакомство с основными администрирования подсистемы защиты информации;
- получение студентами знаний о методах несанкционированного доступа (НСД) к ресурсам ОС;
- получение студентами знаний о структуре подсистемы защиты в ОС;
- выработка практических навыков по использованию средств и методов защиты от НСД к ресурсам ОС
- выработка практических навыков по решению задач администрирования подсистемы защиты информации операционных систем, исходя из задач, стоящих перед вычислительной системой.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем» относится к обязательной части Блока 1 Дисциплины (модули) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знаниях, полученных в результате изучения таких дисциплин как «Основы информационной безопасности», «Операционные системы», «Администрирование операционных систем»,

Изучение данной дисциплины проходит параллельно с изучением такой дисциплины, как «Разработка и эксплуатация защищенных автоматизированных систем», «Безопасность систем баз данных» и базируется на знаниях, полученных в результате изучения этих дисциплин.

Постреквизиты дисциплины:

Изучение данной дисциплины предшествует изучению таких дисциплин, как «Безопасность компьютерных сетей», «Основы управления информационной безопасностью», «Администрирование информационных систем», «Комплексное обеспечение защиты информации объекта информатизации» и является для них одной из базовых.

Знания и умения, полученные студентами при изучении дисциплины Безопасность операционных систем, применяются ими во время учебной и преддипломной практик и в их профессиональной деятельности.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1 - Знает принципы поиска, обработки, обобщения и представления информации для решения задач профессиональной деятельности; ОПК-8.2 - Умеет работать с источниками информации, базами данных и нормативной документацией при решении профессиональных задач; ОПК-8.3 - Владеет практическими навыками поиска необходимой информации и обеспечения информационной безопасности при решении задач в области профессиональной деятельности
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц (72 академических часа).

Вид работы	Трудоемкость, акад. часов	
	6 семестр	всего
Общая трудоемкость	72	72
Контактная работа:	36	36
Лабораторные работы (Лаб)	32	32
Контактная работа в период теоретического обучения (КонТО) <i>(Проведение текущих консультаций и индивидуальная работа со студентами)</i>	4	4

Промежуточная аттестация (зачет)		
Самостоятельная работа: - самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий); - подготовка к лабораторным занятиям;	36	36
	12	12
	24	24

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
		контактная			Самостоятельная работа	
		Лекции	Практические занятия	Лабораторные занятия		
6 семестр						
1.	Тема 1. Основные механизмы обеспечения безопасности ОС			2	4	Выполнение практического задания
2.	Тема 2. Средства и методы аутентификации в ОС			10	10	Выполнение практического задания.
3.	Тема 3 Разграничение доступа к ресурсам ОС			10	10	Выполнение практического задания
4.	Тема 4. Контроль работы подсистемы защиты			10	12	Выполнение практического задания
	Итого:			32	36	

4.3.Содержание разделов дисциплины

Темы и планы лабораторных занятий

Лабораторное занятие №1 (2 ч.)

Тема. Основные механизмы обеспечения безопасности ОС

Вопросы для обсуждения:

1. Типовые угрозы безопасности ресурсов ОС.
2. Требования к безопасности ОС.
3. Основные группы механизмов защиты ресурсов ОС.

Лабораторное занятие №2-6 (10 ч.)

Тема. Средства и методы аутентификации в ОС

Вопросы для обсуждения:

1. Аутентификация на основе пароля.
2. Аутентификация с использованием физического объекта.
3. Биометрические методы аутентификации.
4. Двухфакторная аутентификация в операционных системах
5. Многофакторная аутентификация.
6. Технология SSO.

Лабораторное занятие №7-11 (10 ч)

Тема. Разграничение доступа к ресурсам ОС

Вопросы для обсуждения:

1. Классификация субъектов и объектов доступа.
2. Права доступа. Методы разграничения доступа.
3. Дискреционный механизм разграничения доступа к файловым объектам
4. Мандатный механизм разграничения доступа к файловым объектам
5. Разграничение доступа к файловым объектам. Наследование разрешений.
6. Разграничение доступа к устройствам.
7. Ограничения на запуск программного обеспечения.

Лабораторное занятие №12-16 (10 ч)

Тема. Контроль работы подсистемы защиты

Вопросы для обсуждения:

1. Организация и использование средств аудита.
2. Аудит событий безопасности операционной системы
3. Контроль и восстановление целостности подсистемы защиты и ее параметров.
4. Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты
5. Управление безопасностью ОС.
6. Контроль работы подсистемы защиты в ОС

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Тема 1. Основные механизмы обеспечения безопасности ОС	Лабораторное занятие 1	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
2.	Тема 2. Средства и методы аутентификации в ОС	Лабораторное занятие 1 Лабораторное занятие 2 Лабораторное занятие 3 Лабораторное занятие 4 Лабораторное занятие 5	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
3.	Тема 3 Разграничение доступа к ресурсам ОС	Лабораторное занятие 1 Лабораторное занятие 2 Лабораторное занятие 3 Лабораторное занятие 4 Лабораторное занятие 5	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
4.	Тема 4. Контроль работы подсистемы защиты	Лабораторное занятие 1 Лабораторное занятие 2 Лабораторное занятие 3 Лабораторное занятие 4 Лабораторное занятие 5	Лабораторное занятие в компьютерном классе.

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Форма контроля для очной формы обучения – 6 семестр – *зачет*,

Примеры заданий для текущего контроля и промежуточных заданий по различным темам:

Задание 1

1. Создайте пользователя.
2. Установите требования к качеству PIN-кода eToken в соответствии с Вашим вариантом (табл. 1).
3. Отформатируйте eToken, присвоив ему имя созданного пользователя и установив пароль, соответствующий требованиям п. 2.
4. Создайте профиль для входа в ОС созданного пользователя.

Задание 2

1. Создайте шаблон для окна приложения.
2. При создании шаблона задайте для него настройки.
3. На основе сформированного шаблона создайте и сохраните на eToken соответствующий профиль.

Задание 3

5. Создайте каталоги «Общедоступно» и «Конфиденциально».
6. В каждом из этих каталогов скопируйте исполняемый и текстовый файлы.
7. Разграничьте доступ к принтеру, а также созданным каталогам и файлам.

Задание 4

1. От имени администратора присвойте каталогам (находящимся в корне диска D:\) категории конфиденциальности.
2. В каждом каталоге создайте 2-4 документа от имени пользователя, допуск которого соответствует категории конфиденциальности каталога.
3. Проверьте возможность доступа к созданным документам.

Задание 5

Создайте следующую политику ограничения использования программ, которая будет удовлетворять следующим требованиям:

1. разрешает запуск ПО, подписанного сертификатом от «Microsoft»;
2. применяется ко всем пользователям, включая локальных администраторов;
3. не ограничивает использование программных библиотек, таких как «DLL»;
4. право выбора доверенных издателей разрешено только локальным администраторам;
5. запрещает запуск любых программ в качестве уровня безопасности по умолчанию;
6. разрешает запуск любых программ из папок: «C:\WINDOWS», «C:\Program Files», «C:\Documents and Settings\LocalService», «C:\Documents and Settings\All Users»;

Задание 6

Администратор безопасности Анатолий предоставил полный доступ к материалам по безопасности отдела только стажеру Дмитрий. Эти материалы были размещены на сетевом ресурсе «Ресурсы предприятия\Обмен\Дмитрию», к которому был заранее выставлен аудит чтения, записи, удаления, а также смены владельца. При утилизации документации Анатолий обнаружил распечатанные копии этих материалов. Стажер утверждает свою непричастность к распечатанным копиям важных документов. Докажите или опровергните причастность Дмитрия к распечатанным документам.

Задание 7

Создайте шаблон безопасности в соответствии и настройте операционную систему, используя созданный шаблон:

1. Локальные политики: Включите аудит доступа к объектам (успех и отказ)
2. Журнал событий: Сохранение событий в журнале безопасности – 30 дней
3. Файловая система : Аудит создания файлов и записи данных (успех и отказ) на каталог C:\Windows и дочерние для учётной записи «user»

Примерные вопросы к зачету

1. Основные группы механизмов защиты операционных систем; основные функции этих механизмов.
2. Процедуры идентификации, аутентификации, авторизации. Определение, принцип действия.
3. Функции аутентификации по контролю доступа при работе с ОС и при настройке ОС. Факторы аутентификации – определение, типы, примеры. Многофакторная аутентификация – определение, примеры.
4. Аутентификация с использованием паролей. Принцип действия, варианты реализации, недостатки.
5. Угрозы преодоления парольной защиты. Требования к паролям для увеличения их стойкости.
6. Аутентификация при помощи физического объекта. Принцип действия, варианты реализации, недостатки.
7. Технология однократного входа (SSO – Single Sign-on). Принцип действия, преимущества и недостатки. Применение физического объекта в технологии SSO.
8. Аутентификация при помощи биометрических систем. Принцип действия, варианты реализации, недостатки.
9. Методы биометрической аутентификации.
10. Принципы дискреционного управления доступом. Преимущества и недостатки дискреционной модели.
11. Реализация дискреционного механизма управления доступом в Windows и UNIX системах.
12. Принципы мандатного управления доступом. Преимущества и недостатки мандатной модели.
13. Основные права доступа к файловым объектам в ОС Windows.
14. Владелец файла и его возможности. Подходы к назначению владельца файла.
15. Классификация субъектов и объектов доступа.
16. Правила наследования прав доступа к иерархическим объектам в ОС Windows. Приоритеты правил наследования.
17. Способы обеспечения замкнутости программной среды. Достоинства и недостатки этих методов.
18. Уровни безопасности и правила политики ограниченного использования программ в ОС Windows. Приоритеты использования правил.
19. Способы разграничения доступа к устройствам. Типы прав доступа к устройствам.
20. Белый список устройств и способы его применения.
21. Аудит в операционных системах. Задачи аудита.
22. События, подвергаемые аудиту в ОС Windows. Данные, фиксируемые при аудите.
23. Задачи, решаемые с использованием оснастки «Анализ и настройка безопасности» в Windows

8. Система оценивания планируемых результатов обучения

Оценка «зачтено» выставляется,

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого

увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

- студенту, твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,5	1	8	16
Подготовка к занятию, выполнение домашнего задания	0,5	1	8	16
выполнение практических заданий по темам	3	5	27	45
Промежуточная аттестация (зачет)	10	23	10	23
Итого за семестр			53	100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

а) основная литература:

1. Киренберг, А. Г. Информационная безопасность современных операционных систем : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/128393.html>
2. Гриценко, Ю.Б. Операционные системы : в 2-х ч. / Ю.Б. Гриценко ; Федеральное агентство по образованию, Томский межвузовский центр дистанционного образования (ТУСУР). Кафедра автоматизации обработки информации (АОИ). — Томск: Томский государственный университет систем управления и радиоэлектроники, 2018. — Ч. 2. — 235 с. — Режим доступа: по подписке. — URL: <http://biblioclub.ru/index.php?page=book&id=208655>
3. Курячий, Г. В. Операционная система Linux. Курс лекций : учебное пособие / Г. В. Курячий, К. А. Маслинский. — Саратов : Профобразование, 2017. — 348 с. — ISBN 978-5-4488-0110-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/63944.html>

9.2.Дополнительная литература

1. В. Г. Олифер, Н. А. Олифер. Сетевые операционные системы. — учебник для вузов 2-е изд, СПб.: Питер, 2012. —672 с: ил.
2. Таненбаум Эндрю С. Современные операционные системы. 3-е изд. 2012 год, 1120с
3. Гостев, И. М. Операционные системы : учебник и практикум для академического бакалавриата / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 164 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-04520-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/book/operacionnye-sistemy-433850>

4. Хелен Кастер. Основы Windows NT и NTFS /пер.сангл. – М.:Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.». 2014. –440с
5. Ложников П.С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / Ложников П.С., Михайлов Е.М.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 263 с. — ISBN 978-5-4497-0666-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97553.html>

9.3. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Proffesional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. Дистрибутивы Ubuntu GNU/Linux, Debian GNU/Linux
13. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;
14. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
15. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

9.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)

8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).