Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

**СОГЛАСОВАНО**

Декан ФИТ А.С. Авдеев

# Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.В.5 «Технологии защиты информации в вычислительных сетях»**

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

Направленность (профиль, специализация): **Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)**

Статус дисциплины: **часть, формируемая участниками образовательных отношений**

Форма обучения: **очная**

| Статус | Должность | И.О. Фамилия |
|---|---|---|
| Разработал | доцент | Е.В. Шарлаев |
| Согласовал | Зав. кафедрой «ИВТиИБ» | А.Г. Якунин |
| | руководитель направленности (профиля) программы | Е.В. Шарлаев |

г. Барнаул

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

| Компетенция | Содержание компетенции | Индикатор | Содержание индикатора |
|---|---|---|---|
| ПК-3 | Способен применять технологии защиты информации в сфере профессиональной деятельности | ПК-3.1 | Способен применять технологии защиты информации в вычислительных сетях |

## 2. Место дисциплины в структуре образовательной программы

| | |
|---|---|
| Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины. | Аппаратные средства вычислительной техники, Информатика, Информационные технологии, Программирование, Сети и системы передачи информации |
| Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения. | Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная практика, Технологии защиты веб-ресурсов, Технология проведения исследования защищенности объектов и средств защиты |

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 6 / 216

| Форма обучения | Виды занятий, их трудоемкость (час.) | | | | Объем контактной работы обучающегося с преподавателем (час) |
|---|---|---|---|---|---|
| | Лекции | Лабораторные работы | Практические занятия | Самостоятельная работа | |
| очная | 48 | 64 | 0 | 104 | 122 |

## 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

**Форма обучения: очная**

***Семестр: 6***

Объем дисциплины в семестре з.е. /час: 3 / 108

Форма промежуточной аттестации: Зачет

| Виды занятий, их трудоемкость (час.) | | | | Объем контактной работы обучающегося с преподавателем (час) |
|---|---|---|---|---|
| Лекции | Лабораторные работы | Практические занятия | Самостоятельная работа | |
| 32 | 32 | 0 | 44 | 71 |

**Лекционные занятия (32ч.)**

**1. Введение в технологии защиты информации в вычислительных сетях {беседа} (2ч.)[5,7]** Операционные возможности вычислительных сетей. Мультисервисная (конвергентная) сеть. Основные задачи администратора при проектировании, построении и сопровождении сети. Назначение основных сервисов вычислительных сетей, их особенности реализации и использования. Основы технологии защиты информации в вычислительных сетях

**2. Служба доменных имен. {беседа} (2ч.)[5,7]** Служба доменных имен. Терминология и принципы работы. Типы серверов доменных имен (Master, Slave, Cache, Stealth, Root). Понятие зон – прямая и обратная. Конфигурирование DNS в различных сетевых операционных системах. Протокол DNS.

**3. Маршрутизация. {беседа} (4ч.)[5,7,8]** Организация взаимодействия в глобальных вычислительных сетях. Пересылка пакетов. Маршрутизатор и принципы его работы. Интерфейсы маршрутизатора. Введение в таблицу маршрутизации. Directly-Connected сети. Next-hop и выходной интерфейс. Статическая маршрутизация. Протоколы ARP и RARP. Суммирование статических маршрутов. Маршрут по умолчанию.

**4. Динамическая маршрутизация. {беседа} (4ч.)[5,7,8]** Протоколы динамической маршрутизации. Классификация протоколов динамической маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протоколы маршрутизации состояния связей. Классовая и без классовая маршрутизация.

**5. Принципы динамической маршрутизации. {беседа} (4ч.)[5,7,8]** Понятие сходимости протокола маршрутизации. Принципы работы таблицы маршрутизации. Лучший маршрут и метрика. Распределение нагрузки. Административная дистанция. Дистанционно-векторные протоколы динамической маршрутизации RIP, EIGRP. Протоколы маршрутизации состояния связей OSPF.

**6. Почтовая служба {беседа} (4ч.)[5,7,8]** Организация почтовой службы. Основные способы организации (on-line, off-line). Средства реализации почтовой службы в различных сетевых операционных системах (sendmail, exim, postfix, Microsoft Exchange Server). Протоколы обмена почтовыми сообщениями (POP, SMTP, IMAP).

**7. Организация почтовой службы. {беседа} (4ч.)[5,7,8]** Организация служб электронного общения в режиме on-line. Мессенджеры и VoIP сервис. Телеконференции. Группы новостей.

**8. Инсталляция программного и аппаратного обеспечения. {беседа} (4ч.)[5,7,8]** Приложения и сервисы. Модель «клиент-сервер». Point-to-Point сети и приложения. Протоколы прикладного уровня: Web - HTTP (80) и HTTPS (443),

Протоколы файлового обмена – FTP (20, 21) и SMB (445), электронной почты – SMTP (25), POP (110) и IMAP (143), дистанционного управления – Telnet (23), RDP (3389) и SSH (22), система доменных имён – DNS (53), протокол динамической конфигурации узла DHCP (67, 68), протоколы управления – SNMP (161, 162). Формат данных HTTP, FTP, SMTP, POPv3, DNS, DHCP и принцип их работы.

**9. Уровень защищённых сокетов, протокол SSL и его применение. {беседа} (4ч.)[5,7,8]** Уровень защищённых сокетов, протокол SSL и его применение. Принцип работы протокола SSL. Аутентификация и обмен ключами. Почтовая система (MUA, MTA, MDA). Виды конференцсвязи (аудио, видео), примеры организации конференций.

**Лабораторные работы (32ч.)**

**1. Установка и администрирование сервера LDAP. {работа в малых группах} (4ч.)[1,2,3,8]** Настройка и администрирование сервера Ldap.

**2. Сервисы удаленного терминального доступа (Telnet, rlogin, RDP, SSH). Организация FTP-сервиса. {работа в малых группах} (4ч.)[1,2,3,8]** Практическое овладение методами администрирования компьютерных сетей, настройки FTP сервера. Работа с сервисами удаленного управления (Telnet, rlogin, RDP).

**3. Обеспечение Безопасности протокола IP с помощью средства IPsec. {работа в малых группах} (4ч.)[1,2,3,8]** Настройка защищенного соединения между двумя компьютерами в сети с помощью IPSec. Администрирование программно-аппаратных средств сети.

**4. Овладение навыками работы с прикладной криптосистемой PGP. {работа в малых группах} (4ч.)[1,2,3,8]** Методические указания для выполнения лабораторной работы с использованием PGP: 1)Осуществить защищённый обмен почтовыми сообщениями; 2) Сгенерировать ключевую пару; 3) Обменяться открытыми ключами с получателем; 4) Зашифровать текстовое сообщение (различными способами); 5) Зашифровать не текстовый файл; 6) Передать зашифрованные материалы получателю и получить от него другие зашифрованные материалы; 7) Расшифровать полученные материалы.

**5. Статическая маршрутизация. Протоколы ARP и RARP. Динамическая маршрутизация. Протоколы RIP, OSPF, BGP. {работа в малых группах} (4ч.)[1,2,3,8]** Указания для выполнения лабораторной работы: 1) С помощью протокола ARP собрать сведения по сегменту сети; 2) Используя три узла имеющейся сети, осуществить статическую маршрутизацию; 3) Результаты выполнения предыдущего пункта задокументировать; 4)Настроить маршрутизацию с помощью Quagga аналогично пункту 2.

**6. Администрирование сети средствами технологии Cisco. {работа в малых группах} (4ч.)[1,2,3,8]** Настройка сетевого оборудования Cisco с использованием консольного кабеля, маршрутизатора Cisco 1841, компьютера для настройки маршрутизатора, программы эмулятора iOS GNS3, PuTTY.

**7. Настройка точки доступа Cisco Aironet 1200 Series {работа в малых группах} (4ч.)[1,2,3,8]** Приобретение навыков настройки Wi-Fi точек доступа Cisco.
**8. Персональный межсетевой экран. {работа в малых группах} (4ч.)[1,2,3,8]** Приобретение практических навыков работы при настройке фаервола и биллинга Интернет трафика в корпоративной сети с помощью Kerio WinRoute Firewall

**Самостоятельная работа (44ч.)**
**1. Подготовка к лекционным занятиям. {с элементами электронного обучения и дистанционных образовательных технологий} (16ч.)[5,7,9]**
**2. Подготовка к текущему контролю (выполнение и защита лабораторных работ {использование общественных ресурсов} (24ч.)[1,2,3,8]**
**3. Подготовка к промежуточной аттестации (зачёт). {с элементами электронного обучения и дистанционных образовательных технологий} (4ч.)[1,2,3,4,5,7]**

***Семестр: 7***
Объем дисциплины в семестре з.е. /час: 3 / 108
Форма промежуточной аттестации: Экзамен

| Виды занятий, их трудоемкость (час.) | | | | Объем контактной работы обучающегося с преподавателем (час) |
|---|---|---|---|---|
| Лекции | Лабораторные работы | Практические занятия | Самостоятельная работа | |
| 16 | 32 | 0 | 60 | 52 |

**Лекционные занятия (16ч.)**
**10. Обеспечение безопасности межсетевого взаимодействия. {беседа} (6ч.)[5,7]** Тема 1. Межсетевое взаимодействие. Основы сетевого и межсетевого взаимодействия. Классификация сетевых атак. Информационная безопасность. Тема 2. Политика безопасности. Шаблоны политики безопасности. Сетевая политика безопасности. Эшелонированная оборона. Тема 3. Управление рисками. Основные понятия. Процесс оценки рисков. Уменьшение рисков. Аудит информационной безопасности. Механизмы и службы защиты. Тема 4. Определение информационных ресурсов, подлежащих защите, угроз безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
**11. Межсетевые экраны. {беседа} (4ч.)[5,7]** Тема 1. Классификация межсетевых экранов. Пакетные фильтры. Пример набора правил пакетного фильтра. Пакетный фильтр с учетом контекста (Stateful Packet Inspection). Межсетевые экраны host-based. Прокси-сервер прикладного уровня. Тема 2. Различные типы окружений межсетевых экранов. Основные принципы построения окружения межсетевого экрана. Конфигурация с одной DMZ-сетью. Конфигурация Service Leg. Конфигурация с двумя DMZ-сетями.

**12. Виртуальные частные сети. {беседа} (4ч.)[5,6,7]** Тема 1. Виртуализация. Гипервизоры (Microsoft Hyper-V, VMware ESX, VirtualBOX). Технологии распределённых вычислений. Облачные вычисления. Кластеры. Диагностика сетей (программные, аппаратные и программно-аппаратные комплексы для тестирования и сопровождения сетей). Тема 2. Виртуальные частные сети (VPN). Туннелирование. Протоколы VPN канального уровня. Протокол PPTP. Протокол L2TP. Протокол IPSec. Ассоциация обеспечения безопасности. Тема 3. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Совместное использование протоколов ESP и AH. Основные типы защищенных связей. Протоколы VPN транспортного уровня. Протокол SSL. Протокол SOCKS.

**13. Системы обнаружения вторжений (Intrusion Detection Systems). {беседа} (2ч.)[5,6,7]** Типы IDS. Архитектура IDS. Способы управления. Информационные источники. Анализ, выполняемый IDS. Возможные ответные действия IDS. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. Цели и задачи использования IDS. Существующая политика безопасности. Развертывание IDS. Сильные стороны и ограниченность IDS.

**Лабораторные работы (32ч.)**

**9. Защита сети и сокрытие ее топологии. FireWall & Proxy-сервис. {работа в малых группах} (4ч.)[1,2,3,4,12]** Обеспечить защиту локальной сети со стороны сети общего доступа путем установки и настройки межсетевого экрана Iptables и proxy-сервера squid. Задачи лабораторной работы: -закрепление, углубление и расширение знаний в процессе выполнения конкретных практических задач; -развитие профессиональных навыков, практическое овладение методами экспериментальных исследований в области администрирования компьютерных сетей; -обработки и представления результатов проведенных исследований и формирования выводов; -приобретение умений и навыков в настройке прокси сервера; -приобретение умений и навыков в настройке межсетевого экрана – фаэрвола Iptables.

**10. Настройка системы обнаружения сетевых атак Snort {работа в малых группах} (4ч.)[2,3,5,6]** Изучение и практическое применение системы обнаружения сетевых атак Snort. Задание к выполнению работы: Установить на сервер необходимую оснастку; В соответствие с вариантом настроить на сервере правила; Проверить работоспособность созданного сервера.

**11. Организация VPN средствами СЗИ Vipnet. {работа в малых группах} (4ч.)[2,3,5,6]** Изучение принципов построения виртуальных частных сетей средствами СЗИ Vipnet. Указания для выполнения работы: -установить на сервер необходимую оснастку; -в соответствии с вариантом работы настроить на сервере требуемые правила; проверить работоспособность созданного сервера.

**12. Защита сети средствами DLP {работа в малых группах} (4ч.)[2,3,5,6]** Указания для выполнения работы: -установить на сервер необходимую оснастку; -в соответствии с вариантом работы настроить на сервере требуемые правила; -

проверить работоспособность созданного сервера.

**13. Сканер уязвимостей OpenVas 8.0 {работа в малых группах} (4ч.)[2,3,4,6]** Приобретение навыков сканирования компьютера с целью поиска и устранения уязвимостей. Указания для выполнения лабораторной работы: 1) Установить OpenVas на компьютер; 2) Создать новую политику и задачу сканирования в соответствии с вариантом работы; 3) Провести сканирование одного или нескольких компьютеров; 4) Просмотреть результаты сканирования; 5) Проанализировать полученные результаты.

**14. Тестирование безопасности паролей системных служб и приложений путем эмуляции атак. {работа в малых группах} (4ч.)[2,3,4,6]** Приобретение навыков проверки безопасности паролей системных служб и приложений на предмет подверженности взлому. Указания для выполнения лабораторной работы: 1) На компьютере под управлением операционной системы Windows XP/7 создать 3 учетные записи, для администратора и одного пользователя установить пароли, вход для второго пользователя сделать без пароля, так же на этом компьютере нужно развернуть FTP-сервер и создать двух клиентов: root и обычного пользователя; 2) С помощью программы Hydra с компьютера под управлением Kali Linux произвести тесты по перехвату паролей по SMB и FTP протоколу с помощью созданного и скаченного словаря паролей; 3) Установить на учетные записи более сложные пароли и повторить пункт 2, затем установить ограничения на количество попыток ввода пароля при аутентификации ОС и повторить пункт 2.

**15. Тесты на проникновения СУБД MySQL {работа в малых группах} (4ч.)[3,4,6]** Приобретение навыков проверки безопасности СУБД MysSQL на предмет подверженности взлому. Указания к выполнению лабораторной работы: 1) Установить и настроить MySQL Server 5.1; 2) Создать базу данных с 2 двумя таблицами, наполнить их информацией, а так же создать дополнительного пользователя admin без пароля, чтобы он мог подключаться только из localhost; 3) С помощью утилит Metaslpoit Framework и HexorBase получить доступ к MySQL серверу; 4) Подключиться к серверу с нескольких пользователей; 5) Показать пример работы с базой данных (удаление записей, таблиц, добавление и удаление пользователей, сохранение базы на компьютер); 6) Усложнить пароль для администратора и повторить пункты 3-5.

**16. Обеспечение защиты от DoS-атак {работа в малых группах} (4ч.)[3,4,6]** Приобретение навыков обеспечения защиты от атак типа отказ – в – обслуживании на примере веб-сервера apache2. Указания для выполнения лабораторной работы: 1) На компьютере под управлением операционной системы Windows Server 2016 настроить терминальный доступ и проверить его работоспособность с компьютеров-клиентов под управлением Windows и Ubuntu; 2) С помощью программы Torshammer, установленной на компьютере под управлением Kali Linux 2.0 произвести эмуляцию DoS-атаки на Windows Server 2003 до отказа-в-обслуживании сервера терминального доступа; 3) На компьютере под управлением Ubuntu установить и настроить веб-сервер apache2; 4) Провести тесты DoS-атак типа SYN и HTTP флуд программами Torshammer,

PyLoris, Slowhttptest, установленные на компьютере под управлением Kali Linux 2.0; 5) Обнаружить данные атаки, реализовать меры по защиты от будущих подобных атак и проверить работоспособность реализованных мер.

**Самостоятельная работа (60ч.)**

**4. Подготовка к лекциям. {с элементами электронного обучения и дистанционных образовательных технологий} (8ч.)[5,6,7,9]**

**5. Подготовка к защите лабораторных работ {использование общественных ресурсов} (16ч.)[1,2,3,4,10,11,12,13,14,15,16]**

**6. Подготовка к промежуточной аттестации (экзамен). {использование общественных ресурсов} (36ч.)[5,6,7,8,9]**

## 5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Чугунов Г.А., Методические указания по выполнению лабораторных работ по дисциплине «Сети и телекоммуникации». – Барнаул: Изд-во АлтГТУ, 2012. – 17с.; Источник: электронная библиотека образовательных ресурсов АлтГТУ. Реж.доступа http://elib.altstu.ru/eum/download/vsib/tugunov-sit.pdf

2. Шарлаев Е.В. Вычислительные сети. Учебно-методическое пособие/ Е.В. Шарлаев; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2015. - 86 с.;Источник: электронная библиотека образовательных ресурсов АлтГТУ. Реж. доступа http://elib.altstu.ru/eum/download/ivtib/uploads/sharlaev-e-v-ivtiib-569e03fec1d87.pdf

3. Шарлаев Е.В. Администрирование глобальных вычислительных сетей: Учебно-методическое пособие.- Барнаул, АлтГТУ, 2010. -122с. Источник: электронная библиотека образовательных ресурсов АлтГТУ. Режим доступа http://new.elib.altstu.ru/eum/download/vsib/sharlaev_gvs.pdf

4. Рыбин В.В., Шарлаев Е.В. Безопасность вычислительных сетей. Лабораторный практикум: учебно-методическое пособие; Алт. гос. техн. ун–т им. И.И. Ползунова, - Барнаул: 2017. - 71 с.; Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/RybinSharlaev_BezopVSLP_ump.pdf

## 6. Перечень учебной литературы

6.1. Основная литература

5. Зензин, А.С. Информационные и телекоммуникационные сети: учебное пособие / А.С. Зензин; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. -

Новосибирск: НГТУ, 2011. - 80 с.: табл., схем. - ISBN 978-5-7782-1601-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=228912 (15.05.2019).

6. Мэйволд, Э. Безопасность сетей : учебное пособие : [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 09.03.2023).

7. Основы администрирования информационных систем : учебное пособие : [16+] / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 09.03.2023). – Библиогр. в кн. – ISBN 978-5-4499-1674-7. – DOI 10.23681/598955.

6.2. Дополнительная литература

8. Проскуряков, А.В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : [16+] / А.В. Проскуряков. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 202 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=561238 (дата обращения: 23.04.2021). – Библиогр.: с. 195-196. – ISBN 978-5-9275-2792-2. – Текст : электронный.

9. Гурчикова, А.С. Состав и функции сетевого оборудования ККС/ А.С. Гурчикова. -Москва: Лаборатория книги, 2012. -134 с.: табл., схем. - ISBN 978-5-504-00259-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=142472

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

10. Интернет-сайт открытого программного обеспечения OpenNET (http://opennet.ru/)

11. Интернет-сайт компании Cisco-Россия (http://www.cisco.ru/)

12. Операционная система Linux Ubuntu (http://www.ubuntu.com)

13. Программный продукт виртуализации для операционных систем http://www.virtualbox.org)

14. Сетевой сканер Nmap (http://nmap.org)

15. Анализатор сетевого трафика Wireshark (http://www.wireshark.org)

16. Графический симулятор сети GNS3 (http://www.gns3.net)

## 8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на

кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

## 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

| №пп | Используемое программное обеспечение |
|---|---|
| 1 | LibreOffice |
| 1 | Cisco Packet Tracer |
| 2 | Debian |
| 2 | Windows |
| 3 | Dia |
| 3 | Антивирус Kaspersky |
| 4 | FreeBSD |
| 6 | Linux |
| 7 | Mozilla Firefox |
| 8 | VirtualBox |
| 10 | Windows Server |
| 11 | Wine |
| 13 | 7-Zip |

| №пп | Используемые профессиональные базы данных и информационные справочные системы |
|---|---|
| 1 | Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru) |
| 2 | Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/) |

## 10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

| Наименование специальных помещений и помещений для самостоятельной работы |
|---|
| учебные аудитории для проведения учебных занятий |
| помещения для самостоятельной работы |

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями

здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».