МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора института перспективной инженерии канд. техн. наук, доцент Порохня А.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность жизненного цикла

Направление подготовки	09.04.04 Программная инженерия
Направленность (профиль)	Разработка, мониторинг и управление жизненным циклом инженерных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	3

Разработано
К.ф.-м.н., доцент, заведующая межинститутской базовой кафедрой
Новикова Елена Николаевна

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Цель дисциплины: формирование у обучающихся системных знаний и практических навыков по интеграции практик безопасности на всех этапах жизненного цикла разработки программных и программно-аппаратных инженерных систем (включая наземные и автономные), обеспечению непрерывного соответствия (continuous compliance) требованиям безопасности, а также выявлению, анализу и устранению киберугроз для автономных систем (БПЛА, робототехнических комплексов) на уровнях канала связи, бортового ПО, наземной инфраструктуры управления и цепочек поставок.

Задачи освоения дисциплины:

1. Задачи в области DevSecOps и анализа безопасности кода (ПК-8)

1.1. Изучить методологию «Shift Left» (сдвиг безопасности влево) и освоить интеграцию инструментов статического (SAST), динамического (DAST) анализа безопасности и анализа зависимостей (SCA) в CI/CD-пайплайны с настройкой автоматических шлюзов качества (Quality Gates).

1.2. Освоить практики управления цепочкой поставок (Supply Chain Security): формирование спецификации программных компонентов (SBOM) в форматах SPDX/CycloneDX, проверку целостности и подлинности артефактов с использованием инструментов подписи (Cosign).

1.3. Научиться применять политики безопасности контейнеров (Pod Security Standards, Admission Controllers) и инструменты сканирования образов (Trivy, Grype) для обеспечения безопасности контейнеризованных приложений.

1.4. Сформировать навыки непрерывного соответствия (Continuous Compliance) с использованием методологии «Compliance as Code» и инструментов политик как кода (Open Policy Agent/Regal, Cloud Custodian).

2. Задачи в области безопасности автономных систем (ПК-11)

2.1. Изучить методологии анализа угроз кибербезопасности (STRIDE, DREAD) и освоить их применение для автономных систем (БПЛА, наземные робототехнические комплексы) с построением моделей угроз и оценкой рисков.

2.2. Освоить методы защиты каналов связи автономных систем на основе анализа уязвимостей протоколов (MAVLink, ROS 2 DDS) и настройки механизмов шифрования, аутентификации и защиты от атак типа replay.

2.3. Научиться внедрять механизмы безопасных массовых OTA-обновлений (по воздуху) бортового программного обеспечения, обеспечивающие надежность доставки, целостность, подлинность прошивок и защиту от отката версий.

2.4. Изучить правовые и регуляторные аспекты обеспечения безопасности в Российской Федерации (152-ФЗ, приказы ФСТЭК России) применительно к наземным станциям управления и критической информационной инфраструктуре.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Безопасность жизненного цикла» относится к части, формируемой участниками образовательных отношений (вариативная часть) и является дисциплиной по выбору (Б1.В.09).

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций,

		индикаторов
ПК-8. Способен интегрировать практики безопасности на всех этапах жизненного цикла, включая статический и динамический анализ кода, анализ уязвимостей зависимостей, безопасность контейнеров и облачной инфраструктуры, обеспечивая непрерывное соответствие требованиям безопасности.	**ИД-1$_{ПК-8}$** Внедряет инструменты статического анализа безопасности (SAST) в процесс разработки для автоматического выявления уязвимостей в исходном коде на этапе pull request'ов.	Способен настраивать и интегрировать продвинутые SAST-инструменты (Semgrep/CodeQL) в CI/CD-пайплайн с автоматической блокировкой слияния при обнаружении HIGH/CRITICAL уязвимостей.
	ИД-5$_{ПК-8}$. Сканирует конфигурации инфраструктуры как кода (IaC) на соответствие политикам безопасности и лучшим практикам до их применения.	Способен интегрировать Checkov/tfsec в CI/CD-пайплайн для проверки Terraform/Pulumi кода на соответствие стандартам CIS, а также разрабатывать кастомные политики безопасности для IaC.
	ИД-6$_{ПК-8}$. Интегрирует инструменты безопасности в CI/CD-пайплайны, настраивая автоматические шлюзы качества (quality gates), блокирующие поставку при обнаружении критических уязвимостей.	Способен настраивать многоступенчатые quality gates в CI/CD на основе CVSS-оценок и эксплуатируемости уязвимостей (SAST/SCA), обеспечивая автоматическую остановку пайплайна при критических угрозах.
	ИД-7$_{ПК-8}$. Мониторит состояние безопасности контейнеров и инфраструктуры в рантайме, выявляя инциденты и аномальное поведение.	Способен настраивать политики runtime-безопасности (Falco/Tetragon) для обнаружения аномальной активности в контейнерах, анализировать инциденты и интегрировать их с SIEM-системами.
	ИД-8$_{ПК-8}$. Обеспечивает непрерывное соответствие (continuous compliance) систем требованиям стандартов безопасности и регуляторным нормам через автоматизированный сбор доказательств и генерацию отчетов.	Способен разрабатывать политики Rego для OPA/Cloud Custodian для проверки соответствия облачных ресурсов, анализировать нарушения и генерировать автоматизированные отчеты для аудита (включая требования 152-ФЗ, ФСТЭК)
ПК-11 Способен проводить анализ угроз кибербезопасности для автономных систем, проектировать и внедрять меры защиты на уровнях канала связи, бортового ПО, наземной	ИД-1$_{ПК-11}$. Проводит анализ угроз кибербезопасности для автономных систем с использованием методологии STRIDE, моделируя атаки на каналы связи, бортовые компоненты и наземные станции управления.	Способен применять методологию STRIDE для анализа угроз автономных систем (БПЛА/роботов), строить DFD-диаграммы и составлять документ «Модель угроз и нарушителя».
	ИД-2$_{ПК-11}$. Проектирует меры защиты для каналов связи автономных систем на основе анализа уязвимостей протоколов (MAVLink, DDS,	Способен анализировать защищенность протоколов MAVLink и ROS 2 DDS, выявлять уязвимости (подмена пакетов, replay-атаки) и настраивать шифрование/аутентифи

инфраструктуры управления и цепочек поставок, обеспечивая целостность, конфиденциальность и доступность системы.	XBee) и требований к целостности/конфиденциальности.	кацию каналов связи
	ИД-3$_{ПК-11}$. Внедряет механизмы защиты бортового ПО автономных систем, включая безопасную загрузку (Secure Boot), изоляцию процессов и контроль целостности.	Способен настраивать политики безопасности для ROS 2 узлов (SROS 2) и исследовать механизмы изоляции процессов (AppArmor/SELinux) для обеспечения целостности бортового ПО.
	ИД-4$_{ПК-11}$. Обеспечивает безопасность цепочки поставок (supply chain) для автономных систем, анализируя уязвимости компонентов и зависимостей прошивок.	Способен формировать SBOM для прошивок автопилотов (PX4/ArduPilot), анализировать CVE-уязвимости зависимостей и разрабатывать политику управления уязвимостями для парка устройств.
	ИД-5$_{ПК-11}$. Внедряет механизмы безопасных массовых OTA-обновлений (по воздуху) бортового ПО, обеспечивающие надежность доставки, целостность, подлинность прошивок и защиту от отката версий.	Способен проектировать пайплайн безопасных OTA-обновлений с использованием Cosign/GPG, настраивать подпись и верификацию прошивок, а также обеспечивать защиту от отката версий (rollback protection).

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 3 з.е. 144 ак.ч.	ОФО, в ак. часах
Контактная работа:	54
Лекции/из них практическая подготовка	18
Лабораторных работ/из них практическая подготовка	36
Практических занятий/из них практическая подготовка	
Самостоятельная работа	
Формы контроля	
Экзамен	54
Зачет	
Зачет с оценкой	
Расчетно-графические работы	
Курсовые работа	
Контрольные работы	

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма			
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	
1	**Тема 1. Введение в безопасность жизненного цикла и DevSecOps.** Понятие безопасности жизненного цикла ПО. Место безопасности в DevOps-культуре (DevSecOps). Концепция «Shift Left» (сдвиг безопасности влево). Обзор инструментов безопасности: SAST, DAST, IAST, SCA, RASP. Обзор российских регуляторных требований (152-ФЗ, 187-ФЗ, приказы ФСТЭК).	ПК-8 ИД-1 ПК-8 ИД-6	2		4	4
2	**Тема 2. Управление цепочкой поставок (Supply Chain Security).** Атаки на цепочку поставок (SolarWinds, log4shell, 3CX). SBOM (Software Bill of Materials): форматы SPDX и CycloneDX. Инструменты генерации SBOM (Syft, CycloneDX). Подпись артефактов (Cosign). Безопасное управление зависимостями.	ПК-8 ИД-6 ПК-8 ИД-8	2		4	4
3	**Тема 3. Статический и динамический анализ безопасности.** Углубленный SAST: принципы работы, ложные срабатывания, кастомизация правил (Semgrep, CodeQL). DAST: сканирование веб-приложений и API (OWASP ZAP). IAST: интерактивный анализ. Интеграция в CI/CD.	ПК-8 ИД-1 ПК-8 ИД-6	2		4	4

4	**Тема 4. Безопасность контейнеров и оркестрации.** Уязвимости Docker-образов. Сканирование образов (Trivy, Grype). Политики безопасности в Kubernetes: Pod Security Standards (PSA), Pod Security Policies (PSP), Security Context. Admission Controllers. Runtime-безопасность (Falco).	ПК-8 ИД-1 ПК-8 ИД-6	2		4	4
5	**ема 5. Compliance as Code (непрерывное соответствие).** Концепция Compliance as Code. Язык Rego и Open Policy Agent (OPA). Инструменты: Gatekeeper (Kubernetes), Conftest, Cloud Custodian. Автоматизированный сбор доказательств. Генерация отчетов для аудита (CIS, PCI DSS, российские стандарты)	ПК-8 ИД-5 ПК-8 ИД-8	2		4	4
6	**Тема 6. Анализ угроз для автономных систем (БПЛА/роботы).** Специфика угроз для автономных систем. Методология STRIDE. Построение DFD-диаграмм. Моделирование атак: каналы связи (MAVLink/DDS), бортовое ПО, GCS, телеметрия, саботаж. Оценка рисков (DREAD, CVSS)	ПК-11 ИД-1 ПК-11 ИД-2	2		4	5
7	**Тема 7. Безопасность каналов связи автономных систем.** Протоколы MAVLink (v1/v2) и ROS 2 DDS: архитектура, уязвимости (отсутствие шифрования, подмена пакетов, replay-атаки). Шифрование и аутентификация в MAVLink 2.0 (Signing). DDS Security: аутентификация, шифрование, access control. Анализ трафика (Wireshark).	ПК-11 ИД-2 ПК-11 ИД-3	2		4	5
8	**Тема 8. Безопасность бортового ПО и OTA-обновления.** Безопасная загрузка (Secure Boot, Trusted Execution Environment). Изоляция процессов (SROS 2, AppArmor). Архитектура безопасных OTA-обновлений: клиент-сервер, подпись прошивки (Cosign/GPG), целостность, защита от отката (rollback protection), A/B-разделы, канареечные обновления.	ПК-11 ИД-3 ПК-11 ИД-5	2		4	3

9	**Тема 9. Регуляторные требования и аудит безопасности в РФ.** 152-ФЗ (персональные данные), 187-ФЗ (безопасность КИИ), приказы ФСТЭК России. Требования к наземным станциям управления БПЛА. Сертификация средств защиты информации. Подготовка к аудиту: сбор доказательств, документирование, автоматизация отчетности.	ПК-8 ИД-8 ПК-11 ИД-4	2		4	3
	Экзамен					
	ИТОГО за 3 семестр		18		36	36
	ИТОГО		18		36	36

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств (ФОС) по дисциплине (модулю) базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины.

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

8.1.1. Перечень основной литературы:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-14565-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. —

URL: https://urait.ru/bcode/541253 (дата обращения: 15.04.2026). — Режим доступа: по подписке.
2. Лаврищева, Е. М. Программная инженерия и технологии программирования сложных систем : учебник для вузов / Е. М. Лаврищева. — 2-е изд. — Москва : Юрайт, 2023. — 432 с. — (Высшее образование). — ISBN 978-5-534-12866-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511473 (дата обращения: 15.04.2026). — Режим доступа: по подписке.
3. Корягин, В. В. Система управления версиями Git. Базовый уровень : учебное пособие / В. В. Корягин, А. В. Корягин. — 2-е изд., испр. — Санкт-Петербург : Лань, 2021. — 224 с. — (Высшее образование). — ISBN 978-5-8114-6789-7. — Текст : непосредственный.
4. Ким, Д. The DevOps Handbook. Как создать мир, в котором разработка и эксплуатация станут лучшими друзьями / Д. Ким, П. Дебуа, Д. Уиллис ; перевод с английского. — Санкт-Петербург : Питер, 2021. — 512 с. — (Бестселлеры O'Reilly). — ISBN 978-5-4461-1235-2. — Текст : непосредственный.
5. Ньюмен, С. Создание микросервисов / С. Ньюмен ; перевод с английского. — 2-е изд. — Санкт-Петербург : Питер, 2024. — 622 с. — (Бестселлеры O'Reilly). — ISBN 978-5-4461-1145-9. — Текст : непосредственный.

8.1.2. Перечень дополнительной литературы:

1. Ехлаков, Ю. П. Управление жизненным циклом программных продуктов: модели и алгоритмы : монография / Ю. П. Ехлаков, Д. Н. Бараксанов, Е. А. Янченко. — Томск : ТУСУР, 2013. — 196 с. — ISBN 978-5-86889-661-3. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/72135.html (дата обращения: 15.04.2026). — Режим доступа: по подписке.
2. Буканин, В. А. Вопросы безопасности программного обеспечения приборов и систем : учебное пособие / В. А. Буканин, А. Н. Иванов, В. Н. Павлов, А. О. Трусов. — Санкт-Петербург : СПбГЭТУ «ЛЭТИ», 2020. — 111 с. — ISBN 978-5-7629-2641-6. — Текст : непосредственный.
3. Лукс, С. Kubernetes в действии / С. Лукс ; перевод с английского. — Москва : ДМК-Пресс, 2021. — 672 с. — ISBN 978-5-97060-567-8. — Текст : непосредственный.
4. Резчиков, Е. А. Управление безопасностью жизнедеятельности : учебник для вузов / Е. А. Резчиков. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2024. — 65 с. — (Высшее образование). — ISBN 978-5-534-20035-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557485 (дата обращения: 15.04.2026). — Режим доступа: по подписке.
5. Каменская, Е. Н. Безопасность жизнедеятельности и управление рисками : учебное пособие / Е. Н. Каменская. — Москва : РИОР : ИНФРА-М, 2024. — 251 с. — (Высшее образование). — ISBN 978-5-369-01541-4. — Текст : электронный // Znanium : [сайт]. — URL: https://znanium.com/catalog/document/?pid=2122055 (дата обращения: 15.04.2026). — Режим доступа: по подписке.

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Безопасность жизненного цикла» для студентов направления подготовки 09.04.04 Программная инженерия.
2. Методические указания по организации и проведению самостоятельной работы по дисциплине «Безопасность жизненного цикла» для студентов направления подготовки 09.04.04 Программная инженерия.
3. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине «Безопасность жизненного цикла» для студентов направления подготовки 09.04.04 Программная инженерия

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

www.biblioclub.ru - Электронная библиотечная система «Университетская библиотека онлайн»

www.eLibrary.ru - Научная электронная библиотека

www.iprbookshop.ru - Электронно-библиотечная система IPRbooks

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

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На семинарских и практических занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1. КонсультантПлюс - справочно-правовая система (актуальная версия).
2. Гарант - информационно-правовое обеспечение (актуальная версия).
3. Техэксперт - электронные фонды нормативно-технической документации (ГОСТы, СНиПы, СанПиНы) (актуальная версия).
4. Научная электронная библиотека eLIBRARY.RU - база научных публикаций.
5. ЭБС «Университетская библиотека онлайн» - доступ к электронным учебным изданиям.
6. ЭБС IPR SMART - доступ к электронным учебным изданиям.
7. Официальная документация DevSecOps-инструментов (Semgrep, Trivy, Checkov, OPA, Cosign, Falco) -— открытая онлайн-документация (доступна на территории РФ без ограничений).

Программное обеспечение:

1. Git - Open Source (GNU GPL v2), свободно распространяемое. Система контроля версий.
2. GitLab Community Edition - Open Source (MIT), свободно распространяемое (возможна установка на собственные серверы). CI/CD-платформа для организации пайплайнов.

3. Docker CE - Freemium (базовый функционал - Apache 2.0), свободно распространяемое. Контейнеризация приложений и тестовых окружений.
4. Minikube / Kind - Open Source (Apache 2.0), свободно распространяемое. Локальный Kubernetes-кластер для развертывания.
5. Semgrep CE - Open Source (LGPL 2.1), свободно распространяемое. Статический анализ безопасности кода (SAST).
6. Trivy - Open Source (Apache 2.0), свободно распространяемое. Сканирование уязвимостей (SCA, контейнеры, IaC).
7. Checkov - Open Source (Apache 2.0), свободно распространяемое. Статический анализ конфигураций IaC (Terraform, Kubernetes, CloudFormation).
8. OWASP ZAP - Open Source (Apache 2.0), свободно распространяемое. Динамический анализ безопасности веб-приложений и API (DAST).
9. Gitleaks / TruffleHog - Open Source (MIT / AGPL 3.0), свободно распространяемое. Поиск секретов и ключей в Git-репозиториях.
10. Cosign (Sigstore) - Open Source (Apache 2.0), свободно распространяемое. Подпись и верификация артефактов (контейнеров, бинарных файлов).
11. Open Policy Agent (OPA) / Conftest - Open Source (Apache 2.0), свободно распространяемое. Политики как код (Compliance as Code) для проверки конфигураций.
12. Falco - Open Source (Apache 2.0), свободно распространяемое. Runtime-безопасность контейнеров и обнаружение аномалий.
13. Syft / Grype - Open Source (Apache 2.0), свободно распространяемое. Генерация SBOM и анализ уязвимостей в контейнерах.
14. PX4 SITL / Gazebo - Open Source (BSD), свободно распространяемое. Симуляция автономных систем (БПЛА) для SITL-тестирования.
15. Python 3.x - Open Source (OSI-approved), свободно распространяемое. Язык программирования для разработки тестов и скриптов.
16. Visual Studio Code - Free (Microsoft), свободно распространяемое. Среда разработки с поддержкой расширений для SAST/DevOps.
17. Dependency-Track - Open Source (Apache 2.0), свободно распространяемое. Платформа управления цепочкой поставок (SBOM management, анализ уязвимостей).
18. Wireshark - Open Source (GPL v2), свободно распространяемое. Анализ сетевого трафика (для ЛР по безопасности каналов связи БПЛА).
19. VirtualBox - Open Source (GPL v2), свободно распространяемое. Средство виртуализации для локального развертывания тестовых стендов.
20. Astra Linux Common Edition / Ред ОС - Бесплатные для образовательных учреждений (по запросу) / коммерческие. Альтернативная операционная система для выполнения лабораторных работ (изучение совместимости инструментов безопасности в российской ОС).

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Лабораторные работы	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.

Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается

организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются: способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование); ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»; для синхронного обучения - время проведения онлайн-занятий и преподаватели; для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнаки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.