МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель образовательной программы
_____А.С. Ксенофонтов

«30» мая 2023 г.

УТВЕРЖДАЮ

Директор ИИИиЦТ
_____А.Х. Шапсигов

«30» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Нормативная база стандартизации информационной безопасности

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Нальчик 2023

Рабочая программа дисциплины «Теория информационной безопасности и методология защиты информации» / сост. С.М. Арванова – Нальчик: ФГБОУ КБГУ, 2023. – 19 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части студентам очной формы обучения по направлению подготовки 10.03.01 Информационная безопасность, в 5 семестре, 3 курса.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлениям подготовки 10.03.01 Информационная безопасность, утвержденному приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427, зарегистрированного в Минюсте России 18 февраля 2021 г. N 62548.

Содержание

1. Цели и задачи освоения дисциплины

Дисциплина «Нормативная база. Российские и международные стандарты по информационной безопасности» как дисциплина профессионального цикла направлена на достижение следующих целей – является изложением основополагающих принципов защиты информации с использованием нормативной документации по информационной безопасности, протоколов и профилей защиты информации.

Задачи: обучение студентов систематизированного представления системного подхода к организации защиты информации, передаваемой и обрабатываемой программными средствами на основе использование нормативной документации по информационной безопасности.

2. Место дисциплины в структуре ООП ВПО

Изучение дисциплины «Нормативная база. Российские и международные стандарты по информационной безопасности» базируется на следующих дисциплинах: «Сети и системы передачи информации», «Сети и системы передачи информации», «Управление информационной безопасностью», «Организационное и правовое обеспечение информационной безопасности», «Вычислительные сети. Контроль безопасности в компьютерных сетях».

Знания и практические навыки, полученные из дисциплины «Нормативная база. Российские и международные стандарты по информационной безопасности», используются обучаемыми студентами при разработке курсовых и дипломных работ.

3. Требования к результатам освоения содержания дисциплины

Изучение дисциплины «Нормативная база. Российские и международные стандарты» обеспечивает овладение следующими компетенциями:

- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
- ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;
- ПКС-1.1 Способен применить национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информацииспособностью принимать

участие в проведении экспериментальных исследований системы защиты информации.

В результате изучения дисциплины «Нормативная база. Российские и международные стандарты по информационной безопасности» студенты должны:

знать:

- нормативную документацию по информационной безопасности;
- российские стандарты по информационной безопасности;
- международные стандарты по информационной безопасности;

уметь:

- ориентироваться в стандартах и спецификациях, выделив наиболее важные из них, проанализировав их сильные и слабые стороны, а также способы применения;
- применять отечественные и зарубежные стандарты в области информационной безопасности компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- уметь пользоваться научно-технической литературой в области информационной безопасности;

владеть:

- терминологией нормативной документации по информационной безопасности.

4. Содержание и структура дисциплины

4.1 Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	**2**	**3**	**4**
1	Обзор наиболее важных стандартов и спецификаций в области информационной безопасности	Выделяются наиболее важные стандарты и спецификации. Приводятся краткие сведения о стандартах, не являющихся предметом данного курса. Аннотируются спецификации, детально рассматриваемые в последующей части курса.	1. Устный опрос; 2. Тестирование.
2	"Общие критерии", часть 1. Основные идеи	Рассматривается история создания "Общих критериев", описывается их текущий статус, анализируются основные идеи.	1. Устный опрос; 2. Тестирование.

3	"Общие критерии", часть 2. Функциональные требования безопасности	Детально рассматриваются семейства функциональных требований безопасности, представленные в "Общих критериях". Анализируются достоинства и недостатки принятого в них подхода.	1. Устный опрос; 2. Тестирование.
4	"Общие критерии", часть 3. Требования доверия безопасности	Детально рассматриваются семейства требований и оценочные уровни доверия безопасности, представленные в "Общих критериях". Анализируются достоинства и недостатки принятого в них подхода.	1. Устный опрос; 2. Тестирование.
5	Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности	Определяется роль профилей защиты, описывается их структура. Выделяются общие требования к сервисам безопасности.	1. Устный опрос; 2. Тестирование.
6	Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности	Описываются предположения и цели безопасности, функциональные требования и требования доверия, специфичные для конкретных сервисов безопасности. Основное внимание уделено функциональным требованиям, как наиболее важным для обеспечения безопасности.	1. Устный опрос; 2. Тестирование.
7	Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности	Описываются предположения и цели безопасности, функциональные требования и требования доверия, специфичные для конкретных комбинаций и приложений сервисов безопасности. Наиболее подробно рассматриваются частные функциональные требования.	1. Устный опрос; 2. Тестирование.

8	Рекомендации семейства X.500	Данные рекомендации очень важны в концептуальном плане. Служба директорий, формат сертификатов открытых ключей и атрибутов - это базовые элементы инфраструктуры программно-технического уровня информационной безопасности.	1. Устный опрос; 2. Тестирование.
9	Спецификации Internet-сообщества IPsec	Данные спецификации имеют фундаментальное значение, описывая полный набор средств обеспечения конфиденциальности и целостности на сетевом уровне.	1. Устный опрос; 2. Тестирование.
10	Спецификация Internet-сообщества TLS	Спецификация TLS развивает и уточняет популярный протокол Secure Socket Layer (SSL), используемый в большом числе программных продуктов. Она может служить основой обеспечения безопасности протоколов прикладного уровня.	1. Устный опрос; 2. Тестирование.
11	Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности"	Рассматривается прикладной программный интерфейс к средствам защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Данная спецификация логически дополняет защитные протоколы сетевого и транспортного уровней.	1. Устный опрос; 2. Тестирование.
12	Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия"	Анализируются рекомендации по формированию политики безопасности организации, имеющей современную информационную систему и активно использующей сетевые сервисы.	1. Устный опрос; 2. Тестирование.

13	Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности"	Рассматривается взаимодействие групп реагирования на нарушения информационной безопасности и опекаемого сообщества во время ликвидации нарушений; анализируются используемые при этом документы, правила и процедуры.	1. Устный опрос; 2. Тестирование.
14	Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"	Данная спецификация важна с точки зрения формирования организационной и архитектурной безопасности, на которой базируются прочие меры процедурного и программно-технического уровней.	1. Устный опрос; 2. Тестирование.
15	Британский стандарт BS 7799	Подробно рассматривается британский стандарт BS 7799, ставший основой международного стандарта ISO/IEC 17799. Он помогает решить проблемы административного и процедурного уровней информационной безопасности.	1. Устный опрос; 2. Тестирование.
16	Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	Рассматриваемый стандарт играет организующую роль, описывая внешний интерфейс криптографического модуля и общие требования к подобным модулям. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них.	1. Устный опрос; 2. Тестирование.
17	Обзор и закрепление знаний по дисциплине	Подводится итог курса, кратко суммируются полученные знания.	1. Устный опрос; 2. Тестирование.

4.2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 часа):

Вид работы	Трудоемкость часов	
	№ семестра	Всего
	5	
Общая трудоемкость	**144**	**144**
Аудиторная работа:	**53**	**53**
Лекции (Л)	30	30
Практические занятия (ПЗ)	30	30
Лабораторные работы (ЛР)	15	15
Аудиторные занятия в интерактивной форме	0	0
Самостоятельная работа:	**42**	**42**
Курсовой проект (КП)		
Реферат (Р)		
Самостоятельно изучение разделов	42	42
Подготовка и сдача экзамена	27	27
Вид итогового контроля (экзамен)	**экзамен**	**экзамен**

Разделы дисциплины, изучаемые в 5 семестре:

№ раздела	**Наименование разделов**	**Количество часов**		
		Всего	**Аудиторная работа**	
			СЗ	**ПЗ**
1	Обзор наиболее важных стандартов и спецификаций в области информационной безопасности	6	2	4
2	"Общие критерии", часть 1. Основные идеи	4	2	2
3	"Общие критерии", часть 2. Функциональные требования безопасности	4	2	2
4	"Общие критерии", часть 3. Требования доверия безопасности	4	2	2
5	Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности	4	2	2
6.	Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности	4	2	2

7	Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности	4	2	2
8	Рекомендации семейства X.500	3	1	2
9	Спецификации Internet-сообщества IPsec	3	1	2
10	Спецификация Internet-сообщества TLS	3	1	2
11	Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности"	4	2	2
12	Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия"	4	2	2
13	Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности"	4	2	2
14	Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"	4	2	2
15	Британский стандарт BS 7799	3	1	2
16	Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	3	1	2
17	Обзор и закрепление знаний по дисциплине	3	1	2

4.3. Лабораторные работы не предусмотрены

4.4. Самостоятельное изучения разделов дисциплины на 5 семестр

№ раздела	Вопросы, выносимые на самостоятельное изучение	Кол-во часов
1	Безопасность сетей.	8
2	Безопасность сети Internet.	8
3	Категории сетевых атак.	6
4	Юридические вопросы информационной безопасности.	8
5	Архитектура интернета.	8
6	Вопросы безопасности Windows Server.	8

7	Организация семейства протоколов TCP/IP.	8

5. Образовательные технологии

Лекционные занятия по «Нормативная база. Российские и международные стандарты по информационной безопасности» проводятся в аудиториях оснащенных мультимедийным проектором. Наряду с традиционными типами лекций (вводная, мотивационная, подготовительная, интегрирующая, установочная и др.) при изложении отдельных разделов дисциплины следует использовать лекции с применением дидактического метода «мозговой атаки».

5.1. Самостоятельная работа

Цели самостоятельной работы: формирование способностей к самостоятельному познанию и обучению, поиску литературы, обобщению, оформлению и представлению полученных результатов, их критическому анализу, поиску новых и неординарных решений, аргументированному отстаиванию своих предложений, умений подготовки выступлений и ведения дискуссий.

Организация самостоятельной работы. Самостоятельная работа заключается в проработке лекционного материала, изучении отдельных тем курса по заданию преподавателя по рекомендуемой литературе, в выполнении индивидуальных заданий, в подготовке к практическим занятиям, к рубежным контролям, экзамену.

6. Фонд оценочных средств для текущего и рубежного контроля успеваемости и промежуточной аттестации.

Освоение тем раздела завершается формированием у студента следующих компетенций(контролируемая компетенция ОПК-6, ОПК-8, ПКС-1.1)

Результаты обучения (компетенции)	Основные показатели оценки результатов обучения	Вид оценочного материала
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	*Знать:* систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
	Уметь: разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)

	Владеть: определить политику контроля доступа работников к информации ограниченного доступа.	Коллоквиум Выполнение и защита лабораторных работ Тестирование (раздел 5)
способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности *(ОПК-8)*	***Знать:*** - основные понятия и направления в защите компьютерной информации, - принципы классификации и примеры угроз безопасности базам данных и компьютерным системам, - современные подходы к защите баз данных и систем информационных технологий, - основные инструменты обеспечения многоуровневой безопасности в базах данных и информационных системах. ***Уметь:*** - конфигурировать встроенные средства безопасности в базах данных, - устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; - устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; - настроить инструменты резервного копирования и восстановления информации ***Владеть:*** - методами аудита безопасности баз данных информационных систем, - методами анализа защищенности баз данных информационных систем	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов и эссе *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)* Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); примерные темы докладов (раздел); типовые тестовые задания (раздел 5.2.2.) примерные темы рефераты (раздел 5.1.3).; примерные темы эссе (раздел 5.1.5);
Способен применить национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации (ПКС-1.1)	***Знать:*** нормативно-методическое обеспечение защиты информации, требования к формированию политики информационной безопасности на предприятии, способы управления процессом их реализации, особенности формирования, организации и поддержания работоспособности комплекса мер по обеспечению информационной безопасности предприятия в рамках службы защиты информации. ***Уметь:*** - организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности;	Типовые оценочные материалы для устного опроса *(раздел 5.1.1);* типовые тестовые задания *(раздел 5.2.2.);* примерные темы рефератов и эссе *(раздел 5.1.5);* типовые оценочные материалы к экзамену *(раздел 5.2.)* Оценочные материалы для самостоятельной работы (типовые задачи раздел 5.1.2.); примерные темы рефератов (раздел 5.1.3.); примерные темы докладов (раздел); типовые тестовые задания (раз-

	- составлять «модель» нарушителя, возможные пути и способы его проникновения на охраняемый объект. ***Владеть:*** методикой обеспечения комплексной защиты информации, навыками применения национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации	дел 5.2.2.) примерные темы рефераты (раздел 5.1.3).; примерные темы эссе (раздел 5.1.5);

6.1. Примерная тематика курсовых проектов (работ).

Курсовой проект (работа) не предусмотрен.

6.2. Вопросы к экзамену (контролируемая компетенция ОПК-6, ОПК-8, ПКС-1.1)

1. Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности.
2. Перечислите международные стандарты и кратко их опишите.
3. Перечислите российские стандарты и кратко их опишите.
4. История создания и текущий статус "Общих критериев".
5. Основные понятия и идеи "Общих критериев".
6. Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий".
7. Перечислите и опишите оценочные уровни доверия безопасности.
8. Биометрическая идентификация и аутентификация.
9. Требования к произвольному (дискреционному) управлению доступом.
10. Требования к принудительному (мандатному) управлению доступом.
11. Ролевое управление доступом.
12. Межсетевое экранирование.
13. Системы активного аудита.
14. Анонимизаторы.
15. Выпуск и управление сертификатами.
16. Частные требования безопасности в Операционных системах.
17. Частные требования безопасности в Системах управления базами данных (СУБД).
18. Частные требования безопасности в Виртуальных частных сетях.
19. Частные требования безопасности в Виртуальных локальных сетях.
20. Профиль защиты для смарт-карт.
21. Основные понятия и идеи рекомендаций семейства X.500.
22. Каркас сертификатов открытых ключей рекомендаций семейства X.500.
23. Каркас сертификатов атрибутов рекомендаций семейства X.500.
24. Простая и сильная аутентификация рекомендаций семейства X.500.

25.Архитектура средств безопасности IP-уровня.
26.Обеспечение аутентичности IP-пакетов.
27.Основные понятия Спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности".
28.Взаимодействие между группой реагирования, опекаемым сообществом и другими группами.
29.Порядок публикации правил и процедур деятельности групп реагирования.
30.Описание правил группы реагирования.
31.Описание услуг группы реагирования.
32.Общие положения Спецификации Internet-сообщества "Как выбирать поставщика Интернет-услуг".
33.Роль поставщика Internet-услуг в реагировании на нарушения безопасности.
34.Меры по защите Internet-сообщества.
35.Маршрутизация, фильтрация и ограничение вещания.
36.Размещение Web-серверов.
37.Возможные вопросы к поставщику Internet-услуг.
38.Обзор стандарта BS 7799.
39.Регуляторы безопасности и реализуемые ими цели. Регуляторы общего характера.
40.Регуляторы безопасности и реализуемые ими цели. Регуляторы технического характера.
41.Регуляторы безопасности и реализуемые ими цели. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия.
42.Четырехфазная модель процесса управления информационной безопасностью.
43.Основные понятия и идеи стандарта FIPS 140-2.
44.Требования безопасности. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация.
45.Требования безопасности. Модель в виде конечного автомата, физическая безопасность.
46.Требования безопасности. Эксплуатационное окружение, управление криптографическими ключами.
47.Требования безопасности. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.
48.Основные идеи спецификации Internet-сообщества для программно-технического уровня ИБ.
49.Спецификации Internet-сообщества для административного и процедурного уровней ИБ.

7. Учебно-методическое обеспечение дисциплины (модуля)

7.1. Основная литература

1. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 432 с.

2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.

3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2030. - 324 с.

4. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: Учебник для бакалавриата и магистратуры. – М.: Юрайт, 2017

7.2 Дополнительная литература

1. Основы информационной безопасности: учеб. пособ. для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М.: Горячая линия - Телеком, 2006. - 544 с.: ил.

2. Основы информационной безопасности/В.А. Галатенко. - М.: ИНТУИТ, 2003. - 280 с.

3. Методы и технологии информационных войн / С.Н. Бухарин, В.В. Цыганов. - М.: Академический Проект, 2007. - 382 с.

4. Основы информационной безопасности. Курс лекций: учебное пособие. Третье издание/ В.А. Галатенко/М.: Интернет - Унивеститет Информационных Технологий, www.intuit.ru, 2006. -200 с.

5. Аудит информационной безопасности/ А.П. Курило, С.Л. Зефиров, В.Б. Голованов/ М: Издательская группа "БДЦ - пресс", 2006. - 305 с.

6. Техническая защита информации/ А.П. Зайцев, А.А. Шелупанов/ М: Горячая линия Телеком, 2007. - 616 с.

7. Расторгуев С.П. Основы информационной безопасности: учеб. по-соб. / С.П. Расторгуев. - М.: Академия, 2007. - 192 с.

8. Доктрина информационной безопасности Российской Федерации.

7.3. Периодические издания

"Открытые системы / СУБД": Журнал. – АО "Открытые системы"

7.4. Интернет-ресурсы

Интернет-ресурс «Интернет университет информационных технологий» www.intuit.ru

Документация по Oracle Database 10*g* XE http://st-curriculum.oracle.com/tutorial/ DBXETutorial/index.htm

www.ihtika.lib.ru/ Библиотека учебной и методической литературы

www.osp.ru/ Журнал «Открытые системы»

www.window.edu.ru/ Библиотека учебной и методической литературы

www.intuit.ru/ Образовательный сайт

www.tests.specialist.ru/ Центр компьютерного обучения МГТУ им. Н.Э.Баумана.

www.microinform.ru/ Учебный центр компьютерных технологий «Микроинформ».

www.rsl.ru/ Российская государственная библиотека.

www.nns.ru/ Национальная электронная библиотека.

www.nlr.ru/ Российская национальная библиотека.

www.gpntb.ru/ Государственная публичная научно-техническая библиотека.

8. Материально-техническое обеспечение дисциплины

Минимально необходимый для реализации ОПОП перечень материально-технического обеспечения включает в себя: лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций, средствами звуковоспроизведения, экраном и имеющие выход в сеть Интернет), помещения для проведения семинарских и практических занятий (оборудованные учебной мебелью), компьютерные классы и др.

При проведении занятий лекционного типа, семинарских занятий используются:

лицензионное программное обеспечение:

- Продукты MICROCOFT (WINEDUperDVC ALNG UpgrdSAPk MVL A Faculty EES (Корпоративная подписка на продукты Windows операционная система и офис)) ДОГОВОР №10/ЭА-223.
- Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License, ДОГОВОР № 15/ЭА-223.
- Mathlab/Simulink ДОГОВОР №80/ЕЛ-223.
- Adobe Creative Cloud for Teams – All Apps. Лицензии Education Device license для образовательных организаций ДОГОВОР № 15/ЭА-223.
- ABBYY FineReader ДОГОВОР № 15/ЭА-223.
- Антиплагиат ВУЗ ДОГОВОР № 15/ЭА-223.
- файловый менеджер Far Manager.
- 7zip-архиватор.
- Adobe Reader (свободное распространение)

8.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;
2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):
   - присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;
   - задания для выполнения на экзамене зачитываются ассистентом;
   - письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

   - на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
   - зачет/экзамен проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по желанию студента экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

.

9. ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа:

одобрена на 2023/2024 учебный год. Протокол № _____ заседания кафедры от «___»_____20__ г.

В рабочую программу внесены следующие изменения:

_____
_____
_____
_____
_____

Разработчик программы _____
Зав. кафедрой _____

ПРИЛОЖЕНИЕ

Распределение баллов текущего и рубежного контроля

№п/п	Вид контроля	Сумма баллов			
		Общая сумма	**1-я точка**	**2-я точка**	**3-я точка**
1	Посещение занятий	до 10 баллов	до 3 б.	до 3б.	до 4б.
2	Текущий контроль:	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
3	Рубежный контроль (тестирование и коллоквиум)	до 30 баллов	до 10 б.	до 10 б.	до 10 б.
4	Итого сумма текущего и рубежного контроля	до 70 баллов	до 23б	до 23 б	до 24 б