


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.В.04 «Прикладная криптография»

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

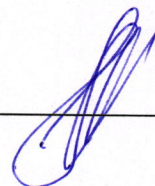
РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Б1.В.03 Методы оптимизации и теория принятия решений составлена в соответствии с с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность

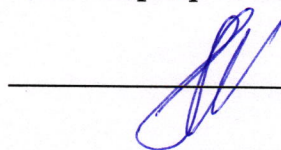
Программу составил:

профессор кафедры информатики Осипов Г.С.



Рабочая программа дисциплины Б1.В.03 Методы оптимизации и теория принятия решений утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности заведующего кафедрой информатики



Осипов Г.С.

1. Цель и задачи дисциплины

Цель дисциплины

Целями освоения дисциплины Прикладная криптография является формирование профессиональных компетенций будущих специалистов в области информационной безопасности, представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- формирование представления об основных проблемах, связанных с практическим использованием криптографических методов защиты информации.
- изучение основных криптографических протоколов.
- изучение инфраструктуры открытого ключа.
- изучение механизмов управления ключами.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Прикладная криптография» относится к обязательной части Блока 1 Дисциплины (модули) (Б1.В.04) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знании следующих дисциплин: Математический анализ; Линейная алгебра и аналитическая геометрия; Компьютерная алгебра, Операционные системы, Объектно-ориентированное программирование.

Постреквизиты дисциплины:

Основные положения данной дисциплины выступают опорой для дисциплин: Основы управления информационной безопасностью, Методы и средства криптографической защиты информации, Защита информации от утечки по техническим каналам, Программно-аппаратные средства защиты информации и др., призваны подготовить к прохождению учебной и производственной практик, к научно-исследовательской работе.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения системы защиты информации автоматизированной системы;

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **4** зачетные единицы (**144** академических часа).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	6	
Общая трудоемкость	144	468
Контактная работа:	54	54
Лекции (Лек)	16	16
Лабораторные работы (Лаб)	32	32
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	5	5
Контактная работа в период промежуточной аттестации (КонтПА)	1	1
Промежуточная аттестация – экзамен	26	26
Самостоятельная работа:	64	64
- самостоятельное изучение разделов (перечислить);	0	0
- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);	16	16
- подготовка к лабораторным занятиям;	36	36
- подготовка к коллоквиумам;	4	4
- подготовка к промежуточной аттестации и т.п.)	8	8

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы		Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
			контактная			Самостоятельная работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
1.	Тема 1. Введение в прикладные аспекты криптографической защиты информации	6	4	0	10	10	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Тема 2. Инфраструктура открытых ключей		4	0	10	10	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Тема 3. Механизмы управления ключами		4	0	8	16	Устный опрос по теме лекции. Проверка домашнего задания.
4.	Тема 4. Практические аспекты криптографической защиты информации		4	0	4	16	Устный опрос по теме лекции. Проверка домашнего задания.
	коллоквиумы					4	Собеседование
	экзамен					8	Устный экзамен (по билетам)
	итого:	103	16	0	32	64	

4.3. Содержание разделов дисциплины

Тема 1. Введение в прикладные аспекты криптографической защиты информации

Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы. Протоколы

идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ». Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.

Тема 2. Инфраструктура открытых ключей

Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.

Тема 3. Механизмы управления ключами

Изучение стандарта ISO/IEC 11770. Механизмы, использующие симметричные методы. Механизмы, использующие асимметричные методы. Механизмы, основанные на слабых секретах. Управление групповыми ключами. Формирование ключей.

Тема 4. Практические аспекты криптографической защиты информации

Проблемы реализации криптографических алгоритмов. Защита от утечки информации. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.

4.4 Темы и планы лабораторных занятий

Лабораторное занятие №1 (10 ч.)

Тема Введение в прикладные аспекты криптографической защиты информации

Вопросы для обсуждения:

1. Криптографические файловые системы.
2. Шифрованная файловая система Windows.
3. Криптографические файловые системы.
4. Шифрование диска BitLocker
5. Шифрование дисков VeraCrypt

Лабораторное занятие №2 (10 ч.)

Тема Инфраструктура открытых ключей

Вопросы для обсуждения:

1. Установка и настройка служб удостоверяющего центра.
2. Функции удостоверяющего центра.
3. Кросс-сертификация удостоверяющих центров.
4. Построение иерархической архитектуры инфраструктуры открытых ключей

Лабораторное занятие №3 (8 ч.)

Тема Механизмы управления ключами

Вопросы для обсуждения:

1. Изучение стандарта ISO/IEC 11770.
2. Механизмы, использующие симметричные методы.
3. Механизмы, использующие асимметричные методы.
4. Механизмы, основанные на слабых секретах.
5. Управление групповыми ключами. Формирование ключей.

Лабораторное занятие №4 (4 ч.)

Тема Практические аспекты криптографической защиты информации.

Вопросы для обсуждения:

1. Проблемы реализации криптографических алгоритмов.
2. Защита от утечки информации.
3. Построение безопасного коммуникационного канала на основе криптографических

алгоритмов.

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
	1 семестр		
1.	Тема 1. Введение в прикладные аспекты криптографической защиты информации	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Тема 2. Инфраструктура открытых ключей	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Тема 3. Механизмы управления ключами	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
4.	Тема 4. Практические аспекты криптографической защиты информации	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

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

Примерные перечень тестовых заданий

1. Независимый программный модуль, позволяющий осуществлять криптографические операции, называется...
 - a) Криптооператор
 - b) Криптопровайдер
 - c) Криптографический клиент
 - d) Криптошлюз
2. Какие протоколы входят в IPSec? Выбрать несколько вариантов
 - a) ISAKMP
 - b) TCP
 - c) ESP
 - d) Все перечисленные
3. Что такое PIM?
 - a) Система для централизованного управления большими массивами данных
 - b) Персональный множитель интеграций
 - c) Протокол шифрования данных транспортного уровня OSI, входящий в стек протоколов IPSec
 - d) Персональный идентификационный номер
4. Равенство значений хеш-функции на двух различных блоках данных называется?
 - a) Пересечение эллиптических кривых
 - b) Компрометация хэш-алгоритмов
 - c) Коллизия хэш-функций
 - d) Криптографическая соль
5. Какие средства шифрования из перечисленных являются стандартными в OS Windows?
 - a) Bitlocker
 - b) Шифрование дисков
 - c) VeraCrypt
 - d) eCryptfs
6. Что из перечисленного не является программным средством шифрования дисков?
 - a) Bitlocker
 - b) TPM
 - c) VeraCrypt
 - d) Ни один из вариантов
7. Что не относится к обязательным полям сертификата формата X.509?
 - a) Открытый ключ субъекта.
 - b) Идентификатор алгоритма подписи.
 - c) Имя объекта сертификата.
 - d) Имя субъекта сертификата.
8. Что означает аббревиатура KDF?
 - a) Функция формирования ключей.
 - b) Функция расширения ключей.
 - c) Функция извлечения ключей.
 - d) Код аутентификации сообщения.
9. Чем занимается сервис конфиденциальности PKI?
 - a) Агрегирует все сертификатов, необходимых для формирования полного пути.
 - b) Обеспечивает аутентификацию участников коммуникации и аутентификацию источника данных.
 - c) Предотвращает преднамеренное или случайное несанкционированное изменение данных.

d) Обеспечивает защиту от несанкционированного получения информации.

10. Что такое центр перевода ключей?

a) Доверенная сущность, генерирующая или получающая ключи, и передающая их общающимся группам, а также имеющая уникальный симметричный ключ с каждой такой группой.

b) Доверенная сущность, осуществляющая расшифрование ключа, сгенерированного и зашифрованного одной сущностью, и последующее зашифрование для другой сущности.

c) Сущность, ответственная за предоставление проверенных идентификаторов пользователей центру сертификации.

d) Доверенная сущность, создающая и назначающая сертификаты открытых ключей.

11. Какая из перечисленных ниже технологий Active Directory применяется для организации

инфраструктуры открытых ключей?

a) Доменные службы

b) Службы сертификации

c) Службы федерации

d) Службы управления правами

12. Что не относится к основным функциям, выполняемым центром сертификации?

a) Формирование собственного секретного ключа и сертификата ЦС.

b) Формирование сертификатов открытых ключей конечных пользователей.

c) Формирование списка отозванных сертификатов.

d) Регистрация новых пользователей центра сертификации.

13. Что из перечисленного ниже не является форматом сертификата?

a) X.509

b) PGP

c) SPKI

d) MD5

14. Какого этапа нет в жизненном цикле сертификата?

a) Запрос сертификата

b) Выдача сертификата

c) Копирование сертификата

d) Отзыв сертификата

Что 15. из перечисленного ниже является примером ситуации, при которой доверие к сертификату было подорвано до истечения срока его действия?

a) Смена фамилии владельца сертификата

b) Потеря ключевого носителя владельцем сертификата

c) Увольнение из организации владельца сертификата

d) Все вышеперечисленное

16. Какая из перечисленных ниже моделей доверия иначе называется «hub and spoke»?

a) Четырехсторонняя модель

b) Мостовая модель

c) Сетевая модель

d) Иерархическая модель

17. Выберите правильное определение пути сертификации.

a) Последовательность сертификатов, в которой издатель первого сертификата и субъект последнего сертификата являются конечными субъектами.

b) Последовательность сертификатов, в которой издатель первого сертификата является пунктом доверия, а субъект последнего сертификата - конечным субъектом.

c) Последовательность сертификатов, в которой издатель первого сертификата является конечным субъектом, а субъект последнего сертификата - пунктом доверия.

d) Последовательность сертификатов, в которой издатель первого сертификата и субъект последнего сертификата являются пунктами доверия.

18. Каким образом в приложениях проверяется валидность сертификата в процессе его использования?

a) По локальному списку отозванных сертификатов.

- b) По значению ключа субъекта сертификата.
 - c) По электронной подписи издателя сертификата.
 - d) По сроку действия сертификата.
19. В каком виде криптопровайдеры хранятся на компьютере?
- a) В формате исполняемых файлов.
 - b) В формате динамически подключаемых библиотек DLL.
 - c) В формате параметров реестра.
 - d) В виде ключевых контейнеров в корне диска.
20. Какую задачу не выполняет CryptoAPI?
- a) Надежность сокрытия данных.
 - b) Расшифровывание полученных конфиденциальных данных.
 - c) Дешифровывание полученных конфиденциальных данных.
 - d) Обеспечение работы с признанными криптографическими стандартами.

Примерные вопросы к экзамену

1. Понятие криптографического протокола.
2. Роль криптографических протоколов в системах защиты информации.
3. Основные атаки на криптографические протоколы.
4. Понятие электронной подписи.
5. Управление открытыми ключами.
6. Основные компоненты инфраструктуры открытых ключей.
7. Понятие сертификата открытого ключа.
8. Удостоверяющий центр.
9. Архитектура инфраструктуры открытого ключа.
10. Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ».
11. Понятие протоколов интерактивного доказательства и доказательства знания.
12. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.
13. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.
14. Проблемы реализации криптографических алгоритмов.
15. Защита от утечки информации.

8. Система оценивания планируемых результатов обучения

Критерии оценивания

Оценка «отлично» 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.

Оценка «хорошо» выставляется 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.

Оценка «удовлетворительно» выставляется 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 «неудовлетворительно» 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	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр /экзамен			60	100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. А. Яковлев. — Санкт-Петербург : Интермедия, 2017. — 312 с. — ISBN 978-5-89160-097-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/66798.html>
2. Информационный мир XXI века. Криптография – основа информационной безопасности / Б. П. Елисеев, Э. А. Болелов, О. Д. Гаранина [и др.] ; под редакцией Э. А. Болелова. — 3-е изд. — Москва : Дашков и К, Московский государственный технический университет гражданской авиации, 2019. — 126 с. — ISBN 978-5-394-03397-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/85368.html>
3. Теоретико-числовые методы в криптографии : учебное пособие / составители Ф. Б. Тебуева, В. О. Антонов. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 107 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/75601.html>

9.2. Дополнительная литература

1. Гулятьева, Т. А. Основы теории информации и криптографии : конспект лекций / Т. А. Гулятьева. — Новосибирск : Новосибирский государственный технический университет, 2010. — 88 с. — ISBN 978-5-7782-1425-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru>
2. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; перевод В. А. Хорев ; под редакцией С. М. Молявко. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 480 с. — ISBN 978-5-00101-700-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/20709.html> Микрюков В.Ю. Алгоритмизация и программирование: учебное пособие /В.Ю. Микрюков. - Ростов н/Д: Феникс, 2007. - 304 с.

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. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
 10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
 11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
 12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
 13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),
 14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
 15. Visual Studio Professional
 16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление);

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. Polpred.com Обзор СМИ (<http://polpred.com/>)
15. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
16. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
17. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
18. 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).