МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
ИМЕНИ И. Т. ТРУБИЛИНА»**

ФАКУЛЬТЕТ ПРИКЛАДНОЙ ИНФОРМАТИКИ

УТВЕРЖДАЮ
Декан факультета
прикладной информатики
_____
профессор С. А. Курносов
«12» апреля 2022 г.

Рабочая программа дисциплины

Информационная безопасность

(Адаптированная рабочая программа для лиц с ограниченными возможностями здоровья и инвалидов, обучающихся по адаптированным основным профессиональным образовательным программам высшего образования)

Направление подготовки
09.03.02 Информационные системы и технологии

Направленность
Создание, модификация и сопровождение информационных систем, администрирование баз данных

Уровень высшего образования
бакалавриат

Форма обучения
очная

Краснодар
2022

Рабочая программа дисциплины «Информационная безопасность» разработана на основе ФГОС ВО 09.03.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки РФ 19 сентября 2017 г. № 926.

Автор:
канд. техн. наук, доцент  В.Н. Лаптев

Рабочая программа обсуждена и рекомендована к утверждению решением кафедры компьютерных технологий и систем от 18.04.2022 г., протокол №10.

Заведующий кафедрой
канд. техн. наук., доц.  Т.В. Лукьяненко

Рабочая программа одобрена на заседании методической комиссии факультета прикладной информатики, протокол № 8 от 25.04.2022 г.

Председатель
методической комиссии  Т.А. Крамаренко
канд. пед. наук, доцент

Руководитель
основной профессиональной
образовательной программы
канд. физ.-мат. наук, доцент  С.В. Лаптев

1 Цель и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является

— формирование у обучаемых потребности в постоянном развитии своих знаний и способностей их эффективного использования в области теоретических основ и технологий информационной безопасности (ИБ) и защиты информации (ЗИ);

— освоения умений и навыков практического обеспечения должной информационной безопасности (ИБ) при создании, модификации и сопровождении автоматизированных информационных систем (АИС), правильном администрировании их баз данных (БД) в строгом соответствии со стратегией развития искусственного интеллекта в Российской федерации (РФ) на период до 2030 года.

Такая целевая установка способствует быстрому развитию искусственного интеллекта (ИИ) - комплексу технологических решений, позволяющих имитировать когнитивные (познавательные) функции человека (включая самообучение и поиск управленческих решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс включает в себя информационно-коммуникационную инфраструктуру (ИКС), программное обеспечение (ПО), в котором используется методы машинного обучения, процессы и сервисы по обработке данных и быстрому поиску правильных управленческих решений. При этом ИИ обеспечивает эффективное использование программных средств и технологий систем ИБ и ЗИ в вычислительных системах и сетях (ВСС)

Задачи дисциплины

- Анализ возможностей по управлению вычислительными ресурсами, взаимодействующими с БД;
- Управления вычислительными ресурсами, взаимодействующими с БД.

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения АОПОП ВО

В результате освоения дисциплины формируются следующие компетенции:

ПКС-3. Способность выполнять работы по обеспечению функционирования баз данных и их информационной безопасности.

В результате изучения дисциплины «Информационная безопасность» обучающийся готовится к освоению трудовых функций и выполнению трудовых действий:

Профессиональный стандарт - 06.011 Администратор баз данных.

Трудовая функция - ТФ 3.2.2 Оптимизация распределения вычислительных ресурсов, взаимодействующих с БД.

Трудовые действия:

1. Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с БД;

2.Управления вычислительными ресурсами, взаимодействующими с БД;

3 Место дисциплины в структуре АОПОП ВО

«Информационная безопасность» является дисциплиной части, формируемой участниками образовательных отношений АОПОП ВО подготовки обучающихся 09.03.02 «Информационные системы и технологии», направленность «Создание, модификация и сопровождение информационных систем, администрирование баз данных».

4 Объем дисциплины (144 часа, 4 зачетные единицы)

Виды учебной работы	Объем, часов	
	Очная	Заочная
Контактная работа в том числе: — аудиторная по видам учебных занятий	**69** 66	 -
— лекции	22	-
— практические	22	-
— лабораторные	22	-
— внеаудиторная	3	-
— зачет	-	-
— экзамен	3	-
Самостоятельная работа в том числе:	**75**	-
— прочие виды самостоятельной работы	75	-
Итого по дисциплине	**144**	-

5 Содержание дисциплины

По итогам изучаемой дисциплины студенты (обучающиеся) сдают экзамен.

Дисциплина изучается на 4 курсе, в 8 семестре по учебному плану очной формы обучения.

Содержание и структура дисциплины по очной форме обучения

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			
				Лк	Пз	Лз	Ср
1	Национальная стратегия развития ИИ в РФ и ее связь с ИБ 1 Цели и задачи стратегии, ее основные понятия. 2 Принципы и технологии стратегии, их использование в совершенствовании ИБ в РФ. 3 Механизм совершенствования ИБ с учетом реализации стратегии развития ИИ.	ПК-3	8	2	2	2	6
2	Объект и предмет ИБ. 1 Угрозы и концепция ИБ. 2 Цели и задачи дисциплины. 3 Направления обеспечения ИБ		8	2	2	2	6
3	Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. 1. Классификация угроз. 2. Случайные и преднамеренные угрозы.		8	2	2	2	6
4	СЗИ от побочных электромагнитных излучений и наводок (ПЭМИН). 1.Методы защиты от ПЭМИН. 2. Средства выявления и защиты от ПЭМИН. 3. Активные методы защиты от ПЭМИН.		8	2	2	2	6
5	Защита информации (ЗИ) от несанкционированного доступа (НСД). 1. Общие требования к защищенности от НСД 2. Защита от программных и аппаратных закладок. 3. Защита от несанкционированных изменений структур		8	2	2	2	6
6	Компьютерные вирусы (КВ) и механизмы борьбы с ними. 1. Классификация КВ. 2. Принципы и методы защиты от КВ. 3. Профилактика заражений КВ в АИС.		8	2	2	2	6
7	Принципы применения криптографической защиты информации 1. Классификация методов криптографического преобразования информации. 2. Стандарты шифрования. 3. Перспективы использования шифрования в АИС.		8	2	2	2	6
8	Стенографическая защита информации. 1. Основные понятия стенографии. 2. Основные угрозы стенографии и типы нарушителей. 3. Компьютерная и цифровая стенография.		8	2	2	2	6

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			
				Лк	Пз	Лз	Ср
9	ЗИ в распределенных компьютерных системах (РКС). 1. Архитектура РКС. 2. Обеспечение ИБ в пользовательской подсистеме и специализированных РКС. 3. ЗИ на уровне подсистем управления РВС.		8	2	2	2	7
10	Особенности ЗИ в распределенных компьютерных систем (РКС). 1. Концепция создания защищенных РКС. 2. Методология проектирования защищенных РКС 3. Этапы создания РКС		8	2	2	2	10
11	Теория компьютерных систем защиты информации (КСЗИ). 1. Математическая постановка задачи разработки КСЗИ 2. Моделирование и реализация КСЗИ. 2. Эксплуатация КСЗМ.			2	2	2	10
				22	22	22	75

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Защита информации: практикум для бакалавров / В.Н. Лаптев, С.В. Лаптев, А.В. Параскевов. – Краснодар: КубГАУ, 2015. – 84 с. Режим доступа: https://edu.kubsau.ru/file.php/118/01_Zashchita_informacii_Praktikum_dlja_bakalavrov.pdf

7 Фонд оценочных средств для проведения промежуточной аттестации

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения АОПОП ВО

Номер семестра	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения АОПОП ВО
ПКС-3. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	

Номер семестра	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения АОПОП ВО
5	Операционные системы
6	Разработка приложений под мобильные устройства
7	Кроссплатформенные приложения
8	Преддипломная практика
8	Выполнение и защита выпускной квалификационной работы

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые результаты освоения компетенции. Индикаторы достижения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный не достигнут)	удовлетворительно (минимальный пороговый)	хорошо (средний)	отлично (высокий)	
ПКС-3. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности					
ИД 3.1 **Знать**: Архитектуру систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсные компоненты взаимодействия БД с системами хранения и обработки данных; **ИД 3.2** **Уметь**: Работать с системами хранения и обработки информации; Локализовать проблему работы с ресурсами, возникшую в системе хранения и обработки данных; **ИД 3.3** **Иметь навыки**: Анализа возможностей по	Фрагментарные знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки данных; Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с	Неполные знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки данных; Анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с	Сформированное, но содержащее отдельные пробелы знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки данных; Анализа возможностей по управлению вычислитель-	Сформированные полные знания архитектуры систем хранения и обработки информации и возможности их взаимодействия БД; Интерфейсных компонент взаимодействия БД с системами хранения и обработки данных; Работ с системами хранения и обработки информации; Локализации проблемы работы с ресурсами, возникшую в системе хранения и обработки данных; Анализа возможностей по управлению вычислительными ресурса-	Тест Реферат Экзамен

Планируемые результаты освоения компетенции. Индикаторы достижения компетенции	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный не достигнут)	удовлетворительно (минимальный пороговый)	хорошо (средний)	отлично (высокий)	
управлению вычислительными ресурсами, взаимодействующими с БД; Управления вычислительными ресурсами, взаимодействующими с БД;	БД; Управления вычислительными ресурсами, взаимодействующими с БД;	БД; Управления вычислительными ресурсами, взаимодействующими с БД;	ными ресурсами, взаимодействующими с БД Управления вычислительными ресурсами, взаимодействующими с БД;	ми, взаимодействующими с БД; Управления вычислительными ресурсами, взаимодействующими с БД;	

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения АОПОП ВО

Оценочное средство по компетенции ПКС-3. Способностью выполнять работы по обеспечению функционирование баз данных и их информационной безопасности.

Для текущего контроля

Практические занятия по дисциплине **«Информационная безопасность»**

Содержание тем практических (семинарских) занятий (Пз) по дисциплине представлено в следующих 4 файлах,

ИБ Раздел I Организация комплексной ЗИ.pdf

ИБ Раздел II Организационные меры защиты.pdf

ИБ Раздел III Защита от внутренних угроз.pdf

ИБ Раздел IV Защита персональных данных.pdf

имеющихся во всех учебных классах кафедры компьютерных технологий и систем (КТС).

В I разделе представлены материалы по выполнению практическим занятий Пз1–4:

Пз-1 Правовые и нормативно-методологические основы технической защите информации (ЗИ).

Пз-2 Основы технической защиты информации.

Пз-3 Методы и средства защиты информации.

Пз-4 Подготовка и аттестация объекта информатизации по требованиям информационной безопасности.

Во II разделе представлены материалы по темам Пз 5–6:

Пз-5 Практические правила управления ИБ организации.

Пз-6 Аудит ИБ.

В III разделе представлены материалы по темам Пз 7–9:

Пз-7 Внутренние угрозы.

Пз-8 Управление рисками ИБ.

Пз-9 Система управления ИБ организации.

В IV разделе представлены материалы по темам Пз10–11:

Пз-10 Организационно-правовые основы безопасности персональных данных (ПД).

Пз-11 Рекомендации и основные мероприятия по организации и техническому обеспечению безопасности ПД.

Пз 1. Организация комплексной технической ЗИ

Изучаемые вопросы:

1.Актуальность проблемы обеспечения информационной безопасности (ИБ) и защиты информации (ЗИ).

2. Специальные нормативные документы по технической ЗИ.

Задания:

1. Отечественные правовые и нормативно-методологические основы деятельности по ИБ.

2. Сравнительный анализ международных и национальных стандартов ИБ.

Пз 2 Основы технической ЗИ

Изучаемые вопросы:

Классификация информационного ресурса (ИР).

Разработка перечня сведений конфиденциального характера.

2. Угрозы несанкционированного доступа к информации.

Задания:

1. Общие положения и классификация угроз ИБ.

2. Отечественные правовые и нормативно-методологические основы деятельности по ИБ.

3. Технические каналы утечки информации, классификация и и способы реализации.

Пз 3 Методы и средства ЗИ

Изучаемые вопросы:

1. Требования и рекомендации по ЗИ от утечки и по техническим каналам.

2. Основные требования по ЗИ от несанкционированного доступа (НСД) к информации.

Задание:

1. Общие вопросы использования средств криптографической ЗИ.

Пз 4 Подготовка и аттестация объектов по требованиям ИБ

Изучаемые вопросы:

1. Лицензирование деятельности по технической защите конфиденциальной информации (КИ).

2. Категорирование объекта информатизации.

3. Подготовка автоматизированной системы к аттестации по требованиям ИБ.

4. Аттестация объекта информатизации по требованиям ИБ.

Задания:

1. Подготовка защищаемого помещения к аттестации по требованиям ИБ

1. Сертификация средств ЗИ по требованиям ИБ.

3. Методика оценки защищенности КИ от утечки по техническим каналам.

4. Методика аттестационных испытаний системы защиты от НСД.

Пз 5 Практические правила управления ИБ организации

Изучаемые вопросы:

1. Организационная структура обеспечения ИБ.

2. Защита информационных активов (ИА) от физического воздействия.

3. Проблемы разработки, приобретения и обслуживания информационной системы (ИС).

4. Разработка концепции, политик и стандартов ИБ организации.

Задания:

1. Классификация и управление активами.

2. Защита конфиденциальной информации при управлении передачей данных и операционной деятельности.

3. Управление инцидентами ИБ.

4. Основные вопросы управления непрерывностью бизнеса.

Пз 6 Аудит информационной безопасности

Изучаемые вопросы:

1.Актуальность аудита ИБ организации.

2. Проведение аудита ИБ.

Задания:

1. Основные принципы, виды, способы и критерии аудита ИБ.

3. Подготовка к аудиту ИБ предприятия, состав и роли участников.

Пз 7 Внутренние угрозы

Изучаемый вопрос:

1. Персонал компании и безопасность ее информационных активов.

Задание:

1. Процессный подход как основа защиты ИА от внутренних угроз.

Пз-8. Управление рисками ИБ

Изучаемые вопросы:

1. Общие понятия управления информационными ресурсами (ИР).

2. Отработка рисков и факторов, влияющих на выбор средств их минимизации в ИБ.

Задания:

1. Основные внутренние уязвимости информационных активов

2. Анализ рисков ИБ.

Пз-9. Система управления ИБ организации

Изучаемые вопросы:

1. Определение области и границ действия систем управления (СУ) ИБ.

2. Внедрение и функционирование систем управления ИБ организации.

Задание:

1. Роли, обязанности и полномочия по внедрению, мониторингу, анализу и совершенствованию системы управления (СУ) ИБ.

Пз-10. Организационно-правовые основы обеспечения безопасности персональных данных

Изучаемые вопросы:

1. Особенности правового и нормативно-методического регулирования деятельности по обеспечению безопасности ПД.

2. Корпоративные и частные модели угроз по безопасности ПД.

Задание:

1. Использование нормативных документов ФСБ для обеспечения безопасности ПД.

Пз-11 Рекомендации и мероприятия по организации и техническому обеспечению безопасности персональных данных

Изучаемые вопросы:

1. Общий порядок организации обеспечения безопасности персональных данных (ПД) в информационных системах ПД.

2. Классификация ИС ПД.

3. Требования к материальным носителям биометрических ПД и технологиям их хранения вне ИС ПД.

Задания:

1. Классификация ИС ПД.

2. Методы и способы ЗИ от утечки по техническим каналам

Лабораторные занятия по дисциплине

Лз-1. Решения проблем и задач на базе искусственного интеллекта.

Лз-2. Создание цифрового сигнала, обеспечивающего требуемый для выживания ОС «эффект системы».

Лз-3. Разграничение доступа к информации в ОС Windows.

Лз-4. Контроль обеспечения безопасности информации.

Лз-5. Применение программных антивирусных комплексов.

Лз- 6. Программирование симметричных и алгебраических алгоритмов шифрования.

Лз7-8. Построение систем защиты информации на основе криптографических преобразований.

Лз-9. Защита программ от изучения.

Лз-10. Система защиты информации Secret Net.

Лз-11. Система защиты информации Net Ware.

Тестирование

Тестирование обучаемых по отдельным темам, разделам и по всей дисциплине «Информационная безопасность» осуществляется с помощью компьютерной программы в INDIGO.

Ниже представлены два правильных ответа при тестировании знаний обучающихся по ИБ с помощью компьютерной программы в INDIGO.

№1 (Балл 1)

Организационные средства обеспечения информационной безопасности (ИБ):

1 ○ специальные пакеты программ или отдельные программы, предназначенные для решения задач ИБ;

2 ○ сложившиеся в обществе нормы или правила, нарушение которых приравнивается к несоблюдению правил поведения;

3 ◉ мероприятия, специально предусматриваемые в технологии функционирования;

4 ○ автоматизированных систем с целью решения задач ИБ;

5 ○ различные механические, электронные и т.п. устройства, встраиваемые в аппаратуру с целью решения задач ИБ;

№37 (1)

Внешняя защита, осуществляемая техническими средствами:

1 ☑ охрана территории и помещений;

2 ☐ подавление электромагнитного излучения;

3 ☑ наблюдение;

4 ☐ идентификация;

5 ☑ разграничение доступа;

6 ☐ блокировка;

Темы докладов:

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Таксономия нарушений ИБ вычислительной системы

6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы ИБ.
8. Модели ИБ и их применение.
9. Классификация средств и методов ИБ от несанкционированного доступа (НСД).
10. Механизмы ИБ от НСД.
11. Государственные требования к системам ИБ.
12. Концепция ИБ от НСД.
13. Особые требования к криптографическим средствам СЗИ.
14. Показатели защищенности средств вычислительной техники (СВТ)
15. Исследование результатов работы антивирусных программ.
16. Алгоритмы электронной цифровой подписи (ЭЦП).
17. Защита файлов и каталогов.
18. Шифрованные логические диски.
19. Криптосистема архиватора WinZip.
20. Уязвимости криптосистемы архиватора Arj.
21. Основные положения национальной стратегии развития искусственного интеллекта на период до 2030 года.
22. Взламывание защиты КС и программ.
23. Средства простановки ключевых меток и защиты программ от копирования.
24. Защита программ при их отладке.
25. Работа пользователей ПК в защищенной среде.

Темы рефератов

1. Классификация компьютерных систем (КС) и требования к защите информации в них.
2. Использование защищенных компьютерных систем.
3. Методы контроля доступа к ресурсам КС.
4. Способы фиксации факта доступа.
5. Структура и функции подсистемы контроля доступа программ и пользователей.
6. Средства активного аудита компьютерных систем.
7. Идентификация и аутентификация субъектов и объектов КС.
8. Идентифицирующая информация и протоколы идентификации.
9. Основные подходы к защите данных от НСД.
10. Иерархический доступ к файлу.
11. Доступ к данным со стороны процесса.
12. Понятие скрытого доступа.
13. Модели управления доступом.
14. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
15. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
16. Активный контроль состояния безопасности КС.

17. Централизованное управление пользователями и контроль их действий.

18. Средства контроля вычислительных процессов.

19. Свойства вычислительных процессов и управление ими.

20. Восстановление удаленных файлов.

21. Средства гарантированного удаления информации.

22. Средства анализа программ.

23. Антивирусные программные комплексы.

24. Настройка и применение антивирусных программ.

25. Устранение проникновения КВ в компьютерную систему

26. Методы криптографии и задачи, решаемые криптографическими средствами в КС.

27. Алгоритмы криптографических преобразований и их характеристики.

28. ЗИ в персонального компьютера (ПК).

29. Перечень и характеристики сертифицированных программно-аппаратных средств (ПАС) СЗИ для ПК.

Вопросы к экзамену

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Таксономия нарушений ИБ вычислительной системы
6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы информационной безопасности.
8. Модели безопасности и их применение.
9. Классификация методов ИБ от несанкционированного доступа (НСД).
10. Классификация средств ИБ от НСД.
11. Механизмы ИБ от НСД.
12. Государственные требования к системам ИБ.
13. Концепция ИБ от НСД.
14. Требования к криптографическим средствам систем ЗИ (СЗИ).
15. Показатели защищенности средств вычислительной техники (СВТ) от НСД.
16. Классификация компьютерных систем и требования ИБ к них.
17. Использование защищенных компьютерных систем.
18. Методы контроля доступа к ресурсам КС.
19. Способы фиксации факта доступа.
20. Структура и функции подсистемы контроля доступа программ и пользователей.
21. Средства активного аудита компьютерных систем.

22. Идентификация и аутентификация субъектов и объектов КС.

23. Идентифицирующая информация и протоколы идентификации.

24. Основные подходы к защите данных от НСД.

25. Иерархический доступ к файлу.

26. Доступ к данным со стороны процесса.

27. Понятие скрытого доступа.

28. Модели управления доступом.

29. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.

30. Защита алгоритма шифрования и программно-аппаратные средства шифрования.

31. Построение аппаратных компонент криптозащиты данных.

32. Сущность разрушающих программных средств.

33. Взаимодействие прикладных программ и программы злоумышленника.

34. Классификация разрушающих программных средств и их воздействий.

35. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.

36. Сущность, проявление, классификация КВ.

37. Необходимые и достаточные условия недопущения разрушающих программных воздействий.

38. Понятие изолированной программной среды.

39. Организационные средства защиты от КВ.

40. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.

41. Проблема обеспечение целостности информации.

42. Защита файлов от изменений.

43. Способы обеспечения целостности информации.

44. Электронная цифровая подпись.

45. Криптографические хэш-функции. Схемы вычисления хэш-функции.

46. Методы криптографии и задачи, решаемые криптографическими средствами в КС.

47. Алгоритмы криптографических преобразований, их характеристики.

48. Методы и средства ограничения доступа к компонентам компьютеров.

49. Построение средств ЗИ для персонального компьютера (ПК).

50. Перечень и характеристики сертифицированных программно-аппаратных средств систем ЗИ от НСД для ПК.

51. Особенности ЗИ в вычислительных сетях.

52. Механизмы реализации атак на вычислительные сети.

53. Защита сетевого файлового ресурса.

54. Определение перечня защищаемых ресурсов и их критичности.

55. Определение категорий персонала и ПАС, на которые распространяется политика безопасности.

56. Определение угроз ИБ.

57. Формирование требований к построению системы ЗИ.

58. Определение уязвимости КС и выбор средств ЗИ.

59. Создание учетных записей пользователей.

60. Создание учетных записей групп.

61. Организация общего доступа к папкам.

62. Активный контроль состояния безопасности КС.

63. Средства ведения и анализа системных журналов ОС Windows NT.

64. Централизованное управление пользователями и контроль их действий.

65. Средства контроля вычислительных процессов.

66. Свойства вычислительных процессов и управление ими.

67. Восстановление удаленных файлов.

68. Восстановление отформатированных (дискет) флешек.

69. Средства гарантированного удаления информации.

70. Средства анализа программ.

71. Дизассемблирование программ и исследование кода.

72. Антивирусные программные комплексы.

73. Настройка и применение антивирусных программ.

74. Устранение проникновения КВ в КС.

75. Исследование результатов воздействия КВ на программы в ОС.

76. Исследование результатов работы антивирусных программ.

77. Алгоритмы электронной цифровой подписи.

78. Защита файлов и каталогов. Шифрованные логические диски.

79. Криптосистема архиватора WinZip.

80. Уязвимости криптосистемы архиватора Arj.

81. Основные положения национальной стратегии развития искусственного интеллекта на период до 2030 года.

82. Средства анализа и копирования защищенных флешек (дискет).

83. Взламывание защиты компьютерных программ.

84. Средства простановки ключевых меток и защиты программ от копирования.

85. Исследование дискет, защищенных от копирования

86. Исследование программ с защитой от копирования.

87. Защита программ при их отладке.

88. Защита информации от НСД с помощью СЗИ "Secret Net".

89. Защита информации от НСД в ЛВС с помощью СЗИ "Net Ware".

90. Работа пользователей в защищенной компьютерной среде.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков характеризующих этапы формирования компетенций

Контроль освоения дисциплины проводится в соответствии с Пл КубГАУ 2.5.1 «Текущий контроль успеваемости и промежуточная аттестация обучающихся».

Текущий контроль по дисциплине позволяет оценить степень восприятия учебного материала и проводится для оценки результатов изучения разделов/тем дисциплины.

Текущий контроль проводится как контроль тематический (по итогам изучения определенных тем дисциплины) и рубежный (контроль определенного раздела или нескольких разделов, перед тем, как приступить к изучению очередной части учебного материала).

Критерии оценки теста:

Оценка «**отлично**» выставляется при условии правильного ответа студента не менее чем 85 % тестовых заданий;

Оценка «**хорошо**» выставляется при условии правильного ответа студента не менее чем 70 % тестовых заданий;

Оценка «**удовлетворительно**» выставляется при условии правильного ответа студента не менее 51 %; .

Оценка «**неудовлетворительно**» выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Реферат

Реферат — это краткое изложение в письменном виде содержания и результатов индивидуальной учебно-исследовательской деятельности, имеет регламентированную структуру, содержание и оформление. Его задачами являются:

1. Формирование умений самостоятельной работы студентов с источниками литературы, их систематизация;

2. Развитие навыков логического мышления;

3. Углубление теоретических знаний по проблеме исследования.

Текст реферата должен содержать аргументированное изложение определенной темы. Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список используемых источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д.

Критериями оценки реферата являются: новизна текста, обоснованность выбора источников литературы, степень раскрытия сущности вопроса, соблюдения требований к оформлению.

Оценка «**отлично**» — выполнены все требования к написанию реферата: обозначена проблема и обоснована её актуальность; сделан анализ различных

точек зрения на рассматриваемую проблему и логично изложена собственная позиция; сформулированы выводы, тема раскрыта полностью, выдержан объём; соблюдены требования к внешнему оформлению.

Оценка «**хорошо**» — основные требования к реферату выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении.

Оценка «**удовлетворительно**» — имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата; отсутствуют выводы.

Оценка «**неудовлетворительно**» — тема реферата не раскрыта, обнаруживается существенное непонимание проблемы или реферат не представлен вовсе.

Критерии оценки на экзамене

Оценка «отлично» выставляется обучающемуся, который обладает всесторонними, систематизированными и глубокими знаниями материала учебной программы, умеет свободно выполнять задания, предусмотренные учебной программой, усвоил основную и ознакомился с дополнительной литературой, рекомендованной учебной программой. Как правило, оценка «отлично» выставляется обучающемуся усвоившему взаимосвязь основных положений и понятий дисциплины в их значении для приобретаемой специальности, проявившему творческие способности в понимании, изложении и использовании учебного материала, правильно обосновывающему принятые решения, владеющему разносторонними навыками и приемами выполнения практических работ.

Оценка «хорошо» выставляется обучающемуся, обнаружившему полное знание материала учебной программы, успешно выполняющему предусмотренные учебной программой задания, усвоившему материал основной литературы, рекомендованной учебной программой. Как правило, оценка «хорошо» выставляется обучающемуся, показавшему систематизированный характер знаний по дисциплине, способному к самостоятельному пополнению знаний в ходе дальнейшей учебной и профессиональной деятельности, правильно применяющему теоретические положения при решении практических вопросов и задач, владеющему необходимыми навыками и приемами выполнения практических работ.

Оценка «удовлетворительно» выставляется обучающемуся, который показал знание основного материала учебной программы в объеме, достаточном и необходимым для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных учеб-ной программой, знаком с основной литературой, рекомендованной учебной программой. Как правило, оценка «удовлетворительно» выставляется обучающемуся, допустившему погрешности в ответах на экзамене или выполнении

экзаменационных заданий, но обладающему необходимыми знаниями под руководством преподавателя для устранения этих погрешностей, нарушающему последовательность в изложении учебного материала и испытывающему затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, не знающему основной части материала учебной программы, допускающему принципиальные ошибки в выполнении предусмотренных учебной программой заданий, неуверенно с большими затруднениями выполняющему практические работы. Как правило, оценка «неудовлетворительно» выставляется обучающемуся, который не может продолжить обучение или приступить к деятельности по специальности по окончании университета без дополнительных занятий по соответствующей дисциплине.

8 Перечень основной и дополнительной учебной литературы

Основная учебная литература

1. Буйневич М.В. Защита информации в компьютерных системах /М.В. Буйневич, И.Н. Васильева и др. – СПб.: СПбГЭУ. 2017. - 95 с. https://elibrary.ru/download/elibrary_32254007_85522439.pdf

2. Графов А.А. Информационная безопасность в системе экономической безопасности: уч. пособие / А.А. Графов , В.А. Моровец - СПб.: СПбГЭУ, 2018. – 75 с. https://elibrary.ru/download/elibrary_35582235_98659341.pdf.

3. Информационная безопасность : учеб. пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. В. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с. https://edu.kubsau.ru/file.php/118/IB_Uch_posobie_21.05.2020_AAA_570178_v1_.PDF

4. Прохорова О.В. Информационная безопасность и защита информации. Учебник. / О.В. Прохорова - Самара: СГАСУ, 2014. – 114 с. https://elibrary.ru/download/elibrary_24801295_31142861.pdf.

5. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/33857.html

Дополнительная учебная литература

1. Панфилова О.А. Информационная безопасность и защита информации: уч.пособие / О.А. Панфилова, Д.Ю. Крюкова, В.В. Наимов - Вологда: ВИПЭ ФСИН, 2018. — Режим доступа: https://elibrary.ru/download/elibrary_35364068_98259713.pdf.

2. Рагозин Ю.Н. Инженерно-техническая защита информации / Ю.Н. Рагозин - СПб.: ООО "Издательский центр "Интермедия", 2018. – 168 с. — Режим доступа: https:/ /elibrary.ru/download/elibrary_38238251_90615975.pdf.

3. Тельный А.В. Техническая защита информации. Аппаратура поиска каналов и устройств несанкционированного съема информации. Методики и рекомендации по применению технических средств защиты информации / А.В. Тельный, Ю.М. Монахов - Владимир: ВГУ, 2018. - 86 с. — Режим доступа: https://elibrary.ru/download/elibrary_36953583_33059976.pdf.

4. Тельный А.В. Техническая защита информации. Защита информации от утечки по техническим каналам. Основные понятия, термины, определения и характеристики / А.В. Тельный, Ю.М. Монахов - Владимир: ВГУ, 2018. – 168 с. — Режим доступа: https://elibrary.ru/download/elibrary_36953575_71006753.pdf.

5. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/33430.html

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень ЭБС

№	Наименование	Тематика	Ссылка
1.	IPRbook	Универсальная	http://www.iprbookshop.ru/
2.	Образовательный портал КубГАУ	Универсальная	https://edu.kubsau.ru/

10 Методические указания для обучающихся по освоению дисциплины

1. Защита информации: практикум для бакалавров / В.Н. Лаптев, С.В. Лаптев, А.В. Параскевов. – Краснодар: КубГАУ, 2015. – 84 с. — Режим доступа: https://edu.kubsau.ru/file.php/118/01_Zashchita_informacii_Praktikum_dlja_bakalavrov.pdf

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

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют: обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети "Интернет"; фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы; организовать процесс образования путем визуализации изучаемой информации посредством использования презентационных технологий; контролировать результаты обучения на основе компьютерного тестирования.

11.1 Перечень лицензионного программного обеспечения

№	Наименование	Краткое описание
1.	Microsoft Windows	Операционная система
2.	Microsoft Office (включает Word, Excel, PowerPoint)	Пакет офисных приложений
3.	Система тестирования INDIGO	Тестирование

11.2 Перечень профессиональных баз данных и информационных справочных систем

№	Наименование	Тематика	Электронный адрес
1.	Гарант	Правовая	https://www.garant.ru/
2.	Консультант	Правовая	https://www.consultant.ru/
3.	Научная электронная библиотека «eLIBRARY.RU»	Универсальная	https://elibrary.ru

11.3 Доступ к сети Интернет и ЭИОС университета

12 Материально-техническое обеспечение обучения по дисциплине для лиц с ОВЗ и инвалидов

Входная группа в главный учебный корпус и корпус зооинженерного факультета оборудован пандусом, кнопкой вызова, тактильными табличками, опорными поручнями, предупреждающими знаками, доступным расширенным входом, в корпусе есть специально оборудованная санитарная комната. Для перемещения инвалидов и ЛОВЗ в помещении имеется передвижной гусеничный ступенькоход. Корпуса оснащены противопожарной звуковой и визуальной сигнализацией.

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1	Информационная безопасность	Помещение №221 ГУК, площадь — 101 м²; посадочных мест 95, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе для обучающихся с инвалидностью и ОВЗ специализированная мебель (учебная доска, учебная мебель) , в том числе для обучающихся с инвалидностью и ОВЗ; технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий (ноутбук, проектор, экран), в том числе для обучающихся с инвалидностью и ОВЗ	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13
2	Информационная безопасность	114 ЗОО учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе для обучающихся с инвалидностью и ОВЗПомещение №114 ЗОО, посадочных мест — 25; площадь — 43м²; учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе для обучающихся с инвалидностью и ОВЗ специализированная мебель(учебная доска, учебная мебель), в том числе для обучающихся с инвалидностью и ОВЗ	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

13 Особенности организации обучения лиц с ОВЗ и инвалидов

Для инвалидов и лиц с ОВЗ может изменяться объём дисциплины (модуля) в часах, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося (при этом не увеличивается количество зачётных единиц, выделенных на освоение дисциплины).

Фонды оценочных средств адаптируются к ограничениям здоровья и восприятия информации обучающимися.

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа.

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ

Категории студентов с ОВЗ и инвалидностью	Форма контроля и оценки результатов обучения
С нарушением зрения	– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.; – при возможности письменная проверка с использованием рельефно- точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние задания, эссе, отчеты и др.
С нарушением слуха	– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – с использованием компьютера: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.; – при возможности устная проверка с использованием специальных технических средств (аудиосредств, средств коммуникации, звукоусиливающей аппаратуры и др.): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.
С нарушением опорно-двигательного аппарата	– письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и

	др.; с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.

Адаптация процедуры проведения промежуточной аттестации для инвалидов и лиц с ОВЗ

В ходе проведения промежуточной аттестации предусмотрено:

– предъявление обучающимся печатных и (или) электронных материалов в формах, адаптированных к ограничениям их здоровья;

– возможность пользоваться индивидуальными устройствами и средствами, позволяющими адаптировать материалы, осуществлять приём и передачу информации с учетом их индивидуальных особенностей;

– увеличение продолжительности проведения аттестации;

– возможность присутствия ассистента и оказания им необходимой помощи (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем).

Формы промежуточной аттестации для инвалидов и лиц с ОВЗ должны учитывать индивидуальные и психофизические особенности обучающегося/обучающихся по АОПОП ВО (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Специальные условия, обеспечиваемые в процессе преподавания дисциплины

Студенты с нарушениями зрения

– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить плоскопечатную информацию в аудиальную или тактильную форму;

– возможность использовать индивидуальные устройства и средства, позволяющие адаптировать материалы, осуществлять приём и передачу информации с учетом индивидуальных особенностей и состояния здоровья студента;

– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;

– использование чёткого и увеличенного по размеру шрифта и графических объектов в мультимедийных презентациях;

– использование инструментов «лупа», «прожектор» при работе с интерактивной доской;

– озвучивание визуальной информации, представленной обучающимся в ходе занятий;

– обеспечение раздаточным материалом, дублирующим информацию, выводимую на экран;

– наличие подписей и описания у всех используемых в процессе обучения рисунков и иных графических объектов, что даёт возможность перевести письменный текст в аудиальный,

– обеспечение особого речевого режима преподавания: лекции читаются громко, разборчиво, отчётливо, с паузами между смысловыми блоками информации, обеспечивается интонирование, повторение, акцентирование, профилактика рассеивания внимания;

– минимизация внешнего шума и обеспечение спокойной аудиальной обстановки;

– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, на ноутбуке, в виде пометок в заранее подготовленном тексте);

– увеличение доли методов социальной стимуляции (обращение внимания, апелляция к ограничениям по времени, контактные виды работ, групповые задания и др.) на практических и лабораторных занятиях;

– минимизирование заданий, требующих активного использования зрительной памяти и зрительного внимания;

– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы.

Студенты с нарушениями опорно-двигательного аппарата (маломобильные студенты, студенты, имеющие трудности передвижения и патологию верхних конечностей)

– возможность использовать специальное программное обеспечение и специальное оборудование и позволяющее компенсировать двигательное нарушение (коляски, ходунки, трости и др.);

– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;

– применение дополнительных средств активизации процессов запоминания и повторения;

– опора на определенные и точные понятия;

– использование для иллюстрации конкретных примеров;

– применение вопросов для мониторинга понимания;

– разделение изучаемого материала на небольшие логические блоки;

– увеличение доли конкретного материала и соблюдение принципа от простого к сложному при объяснении материала;

– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;

– увеличение доли методов социальной стимуляции (обращение внимания, аппеляция к ограничениям по времени, контактные виды работ, групповые задания др.);

– обеспечение беспрепятственного доступа в помещения, а также пребывания них;

– наличие возможности использовать индивидуальные устройства и средства, позволяющие обеспечить реализацию эргономических принципов и комфортное пребывание на месте в течение всего периода учёбы (подставки, специальные подушки и др.).

Студенты с нарушениями слуха
(глухие, слабослышащие, позднооглохшие)

– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить аудиальную форму лекции в плоскопечатную информацию;

– наличие возможности использовать индивидуальные звукоусиливающие устройства и сурдотехнические средства, позволяющие осуществлять приём и передачу информации; осуществлять взаимообратный перевод текстовых и аудиофайлов (блокнот для речевого ввода), а также запись и воспроизведение зрительной информации.

– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;

– наличие наглядного сопровождения изучаемого материала (структурно-логические схемы, таблицы, графики, концентрирующие и обобщающие информацию, опорные конспекты, раздаточный материал);

– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;

– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;

– особый речевой режим работы (отказ от длинных фраз и сложных предложений, хорошая артикуляция; четкость изложения, отсутствие лишних слов; повторение фраз без изменения слов и порядка их следования; обеспечение зрительного контакта во время говорения и чуть более медленного темпа речи, использование естественных жестов и мимики);

– чёткое соблюдение алгоритма занятия и заданий для самостоятельной работы (называние темы, постановка цели, сообщение и запись плана, выделение основных понятий и методов их изучения, указание видов деятельности студентов и способов проверки усвоения материала, словарная работа);

– соблюдение требований к предъявляемым учебным текстам (разбивка текста на части; выделение опорных смысловых пунктов; использование

наглядных средств);

– минимизация внешних шумов;

– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;

– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего).

Студенты с прочими видами нарушений

(ДЦП с нарушениями речи, заболевания эндокринной, центральной нервной и сердечно-сосудистой систем, онкологические заболевания)

– наличие возможности использовать индивидуальные устройства и средства, позволяющие осуществлять приём и передачу информации;

– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;

– наличие наглядного сопровождения изучаемого материала;

– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;

– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;

– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;

– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего);

– предоставление образовательного контента в текстовом электронном формате;

– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;

– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, в виде пометок в заранее подготовленном тексте).

– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы,

– стимулирование выработки у студентов навыков самоорганизации и самоконтроля;

– наличие пауз для отдыха и смены видов деятельности по ходу занятия.