Аннотация к рабочей программе дисциплины «Безопасность распределённых систем»

Цель преподавания дисциплины

Формирование у студентов знаний в области в области информационной безопасности распределенных вычислительных систем для последующего практического использования.

Задачи изучения дисциплины

– изучение методов проектирования распределенных вычислительных систем;

– изучения принципов работы с СУБД;

–определение критериев защищенности распределенных вычислительных систем;

–освоения механизмов контроля целостности в распределенных вычислительных системах;

– формирования правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Компетенции, формируемые в результате освоения дисциплины

Способен формировать проектные решения по созданию и модернизации защищённых информационных систем.(ПК-1)

Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах (ПК-2)

Разделы дисциплины

Понятия и определения безопасности распределенных систем. Структура связи распределенных системах. Современные ОС. Распределенные файловые системы. История безопасности распределенных систем.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета фундаментальной и прикладной информатики
(наименование факультета полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
«31» 08 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность распределенных систем
(наименование дисциплины)

ОПОП ВО 10.04.01 Информационная безопасность
(шифр согласно ФГОС и наименование направления подготовки (специальности))

Защищенные информационные системы
наименование направленности (профиля, специализации)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы)», одобренного Ученым советом университета (протокол № 6 «26» 02 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы)» на заседании кафедры информационной безопасности № 1 «30» 08 2021 г.

Зав. кафедрой _____ Таныгин М.О.

Разработчик программы
к.т.н., доцент _____ Спеваков А.Г.
(ученая степень и ученое звание, Ф.И.О.)

Директор научной библиотеки _____ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ №11 от 30.06.22г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О. _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 2022 г., на заседании кафедры ИБ протокол №1 от 30.08.2023.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1. Цель и задачи дисциплины, планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Формирование у студентов знаний в области в области информационной безопасности распределенных вычислительных систем для последующего практического использования.

1.2. Задачи дисциплины

- изучение методов проектирования распределенных вычислительных систем;
- изучения принципов работы с СУБД;
- определение критериев защищенности распределенных вычислительных систем;
- освоения механизмов контроля целостности в распределенных вычислительных системах;
- формирования правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательный программы

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК 1	Способен формировать проектные решения по созданию и модернизации защищённых информационных систем	ПК-1. Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	***Знать:*** - нормативную базу, регламентирующую создание средств защиты информации распределенных систем; - назначение и классификацию средств защиты информации; - источники и классификацию угроз; - методы проектирования защищенных распределенных систем. ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты

			информации; - разрабатывать проекты нормативно-распорядительной документации; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий; - навыками разработки проектов нормативно- распорядительных документов; - навыками оценки угроз ИБ.
		ПК-1.2 Готовит техническую и проектную документацию по вопросам создания защищённых информационных систем	***Знать:*** - основные методы организационного обеспечения процесса подготовки документов, регламентирующих создание защищённых распределённых систем; - организационные меры по защите информации; - нормативные правовые акты в области защиты информации. ***Уметь:*** - готовить проектную и техническую документацию по вопросам создания защищённых распределённых систем; - готовить проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
		ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации	***Знать:*** - характеристики проектируемых решений; - нормативную базу, регламентирующую создание защищенных распределённых систем; ***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик проектируемых решений с требованиями защиты информации.
		ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем	***Знать:*** - состав типовых конфигураций защищенных распределенных систем; - архитектуру средств контроля конфигурации; ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем;

			- навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.
ПК-2	Способен организовать работы по выполнению требований защиты информации ограниченного доступа в защищённых информационных системах	ПК-2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах -	***Знать:*** - методы и подходы управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах. ***Уметь:*** -организовать выполнение работ; -управлять коллективом исполнителей и принимать управленческие решения; ***Владеть (****или* ***Иметь опыт деятельности):*** -способностью организовать выполнение работ, управлять коллективом исполнителей
		ПК-2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах	***Знать:*** - комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, - перечень принципов, правил, процедур, практических приемов, методов, средств для защиты в защищённых информационных системах провести выбор ***Уметь:*** - разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности инфокоммуникационного объекта, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение готовить проектную и техническую документацию по вопросам создания защищённых распределённых систем; - готовить проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
		ПК-2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем	***Знать:*** - характеристики проектируемых решений; - нормативную базу, регламентирующую создание защищенных распределённых систем; ***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик

			проектируемых решений с требованиями защиты информации.
		ПК-2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах	***Знать:*** - состав типовых конфигураций защищенных распределенных систем; - архитектуру средств контроля конфигурации; ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем; - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.

2. Указание места дисциплины в структуре образовательной программы

Дисциплина «Безопасность распределенных систем» входит в часть, формируемая участниками образовательных отношений, блока 1 «Дисциплины (модули») основной профессиональной образовательной программы – программы магистратуры 10.04.01. Информационная безопасность, профиль «Защищенные информационные системы». Дисциплина изучается на 1 курсе во 2 семестре.

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

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы (з.е.), 108 академических часов.

Таблица 3.1 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	46,1
в том числе:	
лекции	16
лабораторные занятия	30
практические занятия	не предусмотрены

Виды учебной работы	Всего, часов
Самостоятельная работа обучающихся (всего)	61,9
Контроль (подготовка к экзамену)	
Контактная работа по промежуточной аттестации (всего АттКР)	
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен
экзамен (включая консультацию перед экзаменом)	не предусмотрен

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

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Понятия и определения безопасности распределенных систем	Понятие распределенной системы. Преимущества и недостатки распределенных систем. Масштабируемость. Прозрачность. Аппаратные и программные средства построения распределенных систем.
2	Структура связи в распределенных системах	Связь в распределенных системах. Удаленный вызов процедур. Сохранность. Типы связей.
3	Современные ОС	Средства современных ОС. Многозадачность. Многопоточность. Планировщик ОС. Изоляция приложений. Механизмы синхронизации процессов.
4	Распределенные файловые системы	Распределенные файловые системы. Файловая система NFS. Семантика совместного использования файлов. Проблема отказов.
5	История безопасности распределенных систем	Тенденции в области безопасности распределенных систем

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		Лек., час	№ лб.	№пр			
1	2	3	4	5	6	7	8

1	2	3	4	5	6	7	8
1	Понятия и определения безопасности распределенных систем	2	1		О-1,2 Д-1,2 МУ-1	С	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4.
2	Структура связи в распределенных системах	4	2		О-1,2 Д-2,4 МУ-2	С	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4.
3	Современные ОС	4			О-1,2 Д-5,6	С	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4.
4	Распределенные файловые системы	4	3		О-1,2 Д-4,5,6 МУ-3	С	ПК-2.1, ПК-2.2, ПК-2.3, ПК-2.4.
5	История безопасности распределенных систем	2	4		О-1,2 Д-3,4,6,7 МУ-4	Т	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4.

С – собеседование, Т-тест.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	Выполнение работы №1 «Аппаратные и программные средства построения распределенных систем»	8
2	Выполнение работы №2 «Средства защиты распределенных систем»	10
3	Выполнение работы №3 «Файловая система NFS»	6
4	Выполнение работы №4 «Определение параметров видеокарты с поддержкой технологии CUDA в среде Microsoft Visual Studio»	6
Итого		30

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ Раздела (Темы)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение

			СРС, час.
1	Истоки создания распределенных вычислительных систем.	1-2 неделя	8
2	Архитектура распределенных вычислительных систем.	3-4 неделя	8
3	Программное обеспечение распределенных вычислительных систем.	5-6 неделя	8
4	Комплексы защищенных вычислительных сетей. Защищенные распределенные структуры.	7-8 неделя	8
5	Межсетевое взаимодействие в сетях ViPNet.	9-10 неделя	8
6	Администрирование ОС Linux. Особенности архитектуры, сетевые сервисы. WEB-технологии.	11-12 неделя	8
7	Облачные технологии	13-14 неделя	8
8	Распределенные системы мультимедиа	15-16 неделя	5,9
Итого			61.9

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

− библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

− имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

− путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

− путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

− путем разработки вопросов к экзамену, методических указаний к выполнению лабораторных и практических работ.

типографией университета:

− путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

− путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных работ практико-ориентированных заданий.

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплины

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модуле), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-1. Разрабатывает проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	Безопасность распределённых систем Методы и средства защиты информации в системах электронного документооборота Управление разработкой систем безопасности		Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах -	Безопасность распределённых систем Методы и средства защиты информации в системах электронного документооборота Организация работ по обеспечению безопасности в информационных системах		Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2.2 Формирует комплекс мер (принципов, правил, процедур,	Безопасность распределённых систем Методы и средства защиты		Производственная проектно-технологическая

практических приемов, методов, средств) для защиты в защищённых информационных системах	информации в системах электронного документооборота Организация работ по обеспечению безопасности в информационных системах	практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем	Безопасность распределённых систем Методы и средства защиты информации в системах электронного документооборота Организация работ по обеспечению безопасности в информационных системах	Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы
ПК-2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах	Безопасность распределённых систем Методы и средства защиты информации в системах электронного документооборота Организация работ по обеспечению безопасности в информационных системах	Производственная проектно-технологическая практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ПК-1 / начальны	ПК-1.1 Разрабатывает	***Знать:*** - нормативную базу,	***Знать:*** - назначение и классификацию	***Знать:*** - нормативную базу, регламентирующую

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
й	проектные документы на средства защиты информации создаваемых телекоммуникационных систем и сетей	регламентирующую создание средств защиты информации, создаваемых телекоммуникационными системами и сетями; - источники и классификацию угроз; ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий;	средств защиты информации; - источники и классификацию угроз; - методы проектирования средств защиты информации, создаваемых телекоммуникационных систем и сетей. ***Уметь:*** - разрабатывать проекты нормативно-распорядительных документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов;	создание средств защиты информации, создаваемых телекоммуникационных систем и сетей; - назначение и классификацию средств защиты информации; - источники и классификацию угроз; - методы проектирования средств защиты информации, создаваемых телекоммуникационных систем и сетей. ***Уметь:*** - разрабатывать проекты технических заданий на проектирование средств защиты информации; - разрабатывать проекты нормативно-распорядительных документов; - классифицировать и оценивать угрозы ИБ для объекта информатизации; - составлять проектную документацию на систему защиты информации. ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками разработки технических заданий; - навыками разработки проектов нормативно-распорядительных документов; - навыками оценки угроз ИБ.
	ПК-1.2 Готовит техническую и проектную	***Знать:*** - основные методы организационног	***Знать:*** - организационные меры по защите информации;	***Знать:*** - организационные меры по защите информации; - нормативные правовые

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	документацию по вопросам создания защищённых информационных систем	о обеспечения процесса подготовки документов, регламентирующих создание защищённых информационных систем; ***Уметь:*** - разрабатывать проектную и техническую документацию по вопросам создания защищённых информационных систем; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта;	- нормативные правовые акты в области защиты информации. ***Уметь:*** - разрабатывать проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;	акты в области защиты информации. ***Уметь:*** - разрабатывать проектную и техническую документацию по вопросам создания защищённых информационных систем; - разрабатывать проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
	ПК-1.3 Сопоставляет характеристики проектируемых решений с требованиями защиты информации	***Знать:*** - характеристики проектируемых решений; ***Уметь:*** - анализировать характеристики проектируемых решений; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений;	***Знать:*** - нормативную базу, регламентирующую создание средств защиты информации; ***Уметь:*** - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик	***Знать:*** - характеристики проектируемых решений; - нормативную базу, регламентирующую создание средств защиты информации; ***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками составления

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
			проектируемых решений с требованиями защиты информации.	проектируемых решений; - навыками анализа характеристик проектируемых решений с требованиями защиты информации.
	ПК-1.4 Формирует конфигурацию и состав защищённых информационных систем	***Знать:*** - определение конфигурации; - архитектуру средств контроля конфигурации; ***Уметь:*** - формировать эталон конфигурации ИС; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем;	***Знать:*** - состав защищённых информационных систем; - архитектуру средств контроля конфигурации; ***Уметь:*** - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.	***Знать:*** - определение конфигурации; - состав защищённых информационных систем; - архитектуру средств контроля конфигурации; ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть (****или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем; - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.
ПК -2 / начальный	ПК-2.1 Управляет работой специалистов по созданию и эксплуатации средств защиты информации в защищённых	***Знать***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 50% до 69% пунктов из столбца 5 данной	***Знать***: от 70% до 84% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 70% до 84% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 70% до 84% пунктов из	***Знать:*** - методы и подходы управления работой специалистов по созданию и эксплуатации средств защиты информации в защищённых информационных системах. ***Уметь:*** -организовать выполнение работ;

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	информационных системах -	Таблицы ***Владеть***: - от 50% до 69% пунктов из столбца 5 данной Таблицы	столбца 5 данной Таблицы	-управлять коллективом исполнителей и принимать управленческие решения; ***Владеть*** *(или* ***Иметь опыт деятельности):*** -способностью организовать выполнение работ, управлять коллективом исполнителей
	ПК-2.2 Формирует комплекс мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в защищённых информационных системах	***Знать***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 50% до 69% пунктов из столбца 5 данной Таблицы	***Знать***: от 70% до 84% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 70% до 84% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 70% до 84% пунктов из столбца 5 данной Таблицы	***Знать:*** - комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, - перечень принципов, правил, процедур, практических приемов, методов, средств для защиты в защищённых информационных системах провести выбор ***Уметь:*** - разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности инфокоммуникационного объекта, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение готовить проектную и техническую

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
				документацию по вопросам создания защищённых распределённых систем; - готовить проекты методических документов; - применять необходимые нормативные правовые акты; ***Владеть** (или **Иметь опыт деятельности):*** - навыками организации проекта; - навыками подготовки необходимой технической и проектной документации;
	ПК-2.3 Управляет процессом разработки моделей угроз и моделей нарушителя безопасности информационных систем	***Знать***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 50% до 69% пунктов из столбца 5 данной Таблицы	***Знать***: от 70% до 84% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 70% до 84% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 70% до 84% пунктов из столбца 5 данной Таблицы	***Знать:*** - характеристики проектируемых решений; - нормативную базу, регламентирующую создание защищенных распределённых систем; ***Уметь:*** - анализировать характеристики проектируемых решений; - сопоставлять характеристики проектируемых решений с требованиями защиты информации; ***Владеть** (или **Иметь опыт деятельности):*** - навыками составления проектируемых решений; - навыками анализа характеристик проектируемых решений с требованиями защиты информации.

Код компетенции/ этап *(указывается название этапа из п.7.1)*	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
	ПК-2.4 Разрабатывает организационно-распорядительные документы, регламентирующие порядок эксплуатации защищённых информационных системах	***Знать***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 50% до 69% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 50% до 69% пунктов из столбца 5 данной Таблицы	***Знать***: от 70% до 84% пунктов из столбца 5 данной Таблицы ***Уметь***: - от 70% до 84% пунктов из столбца 5 данной Таблицы ***Владеть***: - от 70% до 84% пунктов из столбца 5 данной Таблицы	***Знать:*** - состав типовых конфигураций защищенных распределенных систем; - архитектуру средств контроля конфигурации; ***Уметь:*** - формировать эталон конфигурации ИС; - считывать текущую конфигурацию и сравнивать её с эталонной; ***Владеть*** *(или* ***Иметь опыт деятельности):*** - навыками анализа состава защищённых информационных систем; - навыками работы с конфигурационными файлами; - навыками работы с несколькими модулями проверки.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология форматирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Понятия и определения безопасности	ПК-1.1,ПК-1.2, ПК-1.3,ПК-1.4, ПК-2.1,ПК-2.2,	Лекция, СРС, Практическая работа №1	Собеседование, контрольные вопросы к пр.		Согласно табл. 7.2

	распределенных систем	ПК-2.3,ПК-2.4.		№1		
2	Структура связи в распределенных системах	ПК-1.1,ПК-1.2, ПК-1.3,ПК-1.4.	Лекция, СРС, Практическая работа №2	Собеседование, контрольные вопросы к пр. №2		Согласно табл. 7.2
3	Современные ОС	ПК-2.1,ПК-2.2, ПК-2.3,ПК-2.4.	Лекция, СРС	Собеседование		Согласно табл. 7.2
4	Распределенные файловые системы	ПК-2.1,ПК-2.2, ПК-2.3,ПК-2.4.	Лекция, СРС, Практическая работа №3	Собеседование, контрольные вопросы к пр. №3		Согласно табл. 7.2
5	История безопасности распределенных систем	ПК-1.1,ПК-1.2, ПК-1.3,ПК-1.4.	Лекция, СРС, Практическая работа №4	Тест, контрольные вопросы к пр. №4		Согласно табл. 7.2

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Тестирование лекция №1: Понятия и определения безопасности распределенных систем

Информация - это

Вариант 1: любые сведения, принимаемые и передаваемые, сохраняемые различными источниками

Вариант 2: изменение физической величины, несущее информацию, кодированную определённым способом, либо синхронизированное (заранее оговоренное с получателем) отсутствие изменения физической величины

Вариант 3: зарегистрированная информация; представление фактов, понятий или инструкций в форме, приемлемой для общения, интерпретации, или обработки человеком или с помощью автоматических средств

1. Информационная безопасность — это:

Вариант 1: прикладная наука

Вариант 2: гуманитарная наука

Вариант 3: общественная наука

2. Сигнал - это

Вариант 1: изменение физической величины, несущее информацию, кодированную определённым способом, либо синхронизированное (заранее оговоренное с получателем) отсутствие изменения физической величины

Вариант 2: любые сведения, принимаемые и передаваемые, сохраняемые различными источниками

Вариант 3: зарегистрированная информация; представление фактов, понятий или инструкций в форме, приемлемой для общения, интерпретации, или обработки человеком или с помощью автоматических средств

Рефераты

1. История развития систем баз данных.
2. Программные закладки. Программы – шпионы
3. Парольная защита.
4. Сетевые атаки. Системы обнаружения атак

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена. Экзамен проводится в форме тестирования (бланкового).

Для тестирования используются контрольно-измерительные материалы (КИМ) – задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%).

Для проверки *знаний* используются вопросы и задания в закрытой форме (с выбором одного или нескольких правильных ответов).

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество

освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулирующих следующими нормативными актами университета:

- Положение П 02.016 – 2018 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете бально-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Выполнение работы №1 «Аппаратные и программные средства построения распределенных систем»	4	Выполнил, но «не защитил»	10	Выполнил, и «защитил»
Выполнение работы №2 «Средства защиты распределенных систем»	5	Выполнил, но «не защитил»	10	Выполнил, и «защитил»
Выполнение работы №3 «Файловая система NFS»	5	Выполнил, но «не защитил»	10	Выполнил, и «защитил»
Выполнение работы №4 «Определение параметров видеокарты с поддержкой технологии CUDA в среде Microsoft Visual Studio»	5	Выполнил, но «не защитил»	10	Выполнил, и «защитил»
СРС	5		8	
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

При итоговом контроле в форме бланкового тестирования студенту предлагается 15 вопросов по различным темам курса. Каждый вопрос оценивается в 4 условных балла. Полученную итоговую сумму условных баллов (максимум 60) переводят в баллы на зачете (максимум 36) путём умножения на 0.6 и округления до целого значения. Пример билета в тестовой форме приведён в приложении Д.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1Основная учебная литература

1. Основы построения защищенных баз данных: практикум : [16+] / авт.-сост. Л. Л. Гусева. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 110 с. : ил. – Режим доступа:– URL: https://biblioclub.ru/index.php?page=book&id=563266. – Библиогр. в кн. – Текст : электронный.
2. Митин, А. И. Работа с базами данных Microsoft SQL Server: сценарии практических занятий : [16+] / А. И. Митин. – Москва ; Берлин : Директ-Медиа, 2020. – 143 с. : табл., ил. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=571169 . – Библиогр.: с. 132-134. – ISBN 978-5-4499-0420-1. – DOI 10.23681/571169. – Текст : электронный.
3. Сидорова, Н. П. Базы данных: практикум по проектированию реляционных баз данных : [16+] / Н. П. Сидорова ; Технологический университет, Институт техники и цифровых технологий, Факультет инфокоммуникационных систем и технологий. – Москва ; Берлин : Директ-Медиа, 2020. – 93 с. : ил. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=575080. – Библиогр.: с. 85. – ISBN 978-5-4499-0799-8. – Текст : электронный.
4. Шилин, А. С. Перспективные методы проектирования реляционных баз данных : учебное пособие : [12+] / А. С. Шилин. – Москва ; Берлин : Директ-Медиа, 2021. – 137 с. : ил., схем., табл. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=602240. – Библиогр. в кн. – ISBN 978-5-4499-1890-1. – Текст : электронный.
5. Беспалов, Д. А. Администрирование баз данных и компьютерных сетей : учебное пособие : [16+] / Д. А. Беспалов, А. И. Костюк ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 127 с. : ил., табл. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=612220. – Библиогр. в кн. – ISBN 978-5-9275-3577-4. – Текст : электронный.

8.2 Дополнительная учебная литература

1. Основы построения защищенных баз данных: лабораторный практикум : [16+] / авт.-сост. Л. Л. Гусева ; Министерство науки и высшего образования Российской Федерации, Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 120 с. : ил. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=563264. – Библиогр. в кн. – Текст : электронный.
2. Базы данных в высокопроизводительных информационных системах : учебное пособие / авт.-сост. Е. И. Николаев ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 163 с. : ил. – Режим доступа: – URL: https://biblioclub.ru/index.php?page=book&id=466799. – Библиогр.: с. 161. – Текст : электронный.
3. Фисун А.П., Спеваков А.Г. Основы правового обеспечения информационной безопасности [Электронный ресурс] : учебное пособие - Курск : ЮЗГУ, 2013 - .Ч. 1 / Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - 149 с. : ил., табл. - Имеется печ. аналог. - Библиогр.: с. 137-149.

8.3 Перечень методических указаний

1. Проектирование базы данных, работа с таблицами, создание диаграммы [Текст]: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 46 с.
2. Заполнение БД в среде MS SQL Server 2008 r2, выборка данных с помощью запросов [Текст]: методические указания по выполнению лабораторной работы №2/ Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 31 с.
3. Администрирование базы данных [Текст]: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 37 с.
4. Разработка клиентского интерфейса для БД и создание отчетов в клиентском приложении [Текст]: методические указания по выполнению лабораторной работы №4/ Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 35 с.

5. Шифрование SQL Server [Текст]: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 48 с.
6. Безопасность систем баз данных [Текст]: методические указания по выполнению практических работ / Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 34 с.
7. Безопасность систем баз данных [Текст]: методические указания по выполнению самостоятельной работы/ Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 27 с.
8. Безопасность систем баз данных [Текст]: методические указания по выполнению курсового проекта / Юго-Зап. гос. ун-т; сост.: Спеваков. – Курск, 2017. - 164 с.

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

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/

2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3. Корпорация «Microsoft» [официальный сайт]. Режим доступа: https://www.microsoft.com/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Безопасность распределенных систем» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных

выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовить рефераты по отдельным темам дисциплины, выступать на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Безопасность распределенных систем»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность распределенных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Безопасность распределенных систем» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осущест-влении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,
Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,
Windows 7, договор IT000012385
Oracle Virtualbox (Бесплатная, GNU General Public License),
Microsoft Visual Studio 2010 Professional Договор IT000012385
MS SQL Server Developer Edition (Бесплатная, GNU General Public License)

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноутбукASUSX50VLPMD-T2330/14"/1024Mb/ 160Gb/сумка/проектор inFocusIN24+.

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

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие

ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. **Лист дополнений и изменений, внесенных в рабочую программу дисциплины**

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			

ПРИЛОЖЕНИЕ А Список рефератов

История развития систем баз данных.

Программные закладки. Программы – шпионы

Парольная защита.

Сетевые атаки. Системы обнаружения атак

Современные СУБД.

Межсетевые экраны

Компьютерные вирусы

Защита в базах данных

Программно–аппаратные комплексы разграничения доступа отечественного и зарубежного производства

Реляционная модель данных.

Технологии аутентификации

Оптимистическая и пессимистическая стратегии разграничения доступа.

Устройства ввода идентификационных признаков (смарт–карты, ТМ – идентификаторы)

Защита программ от несанкционированного копирования

Технологии шифрования данных. Шифрование файлов, каталогов, дисков. Шифрованные файловые системы

Программные продукты для криптографической защиты данных