МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф.,д.т.н.,доц.
(должность, уч. степень, звание)
С.В. Бегзатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации в распределенных информационных системах»
(Название дисциплины)

Код направления	10.05.03
Наименование направления/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Обеспечение информационной безопасности распределенных информационных систем
Форма обучения	очная

Санкт-Петербург– 2020 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

проф.,к.т.н.,проф.	24.06.21	С.Г. Фомичева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34
«24» июня 2021 г, протокол № 11

Заведующий кафедрой № 34

проф.,д.т.н.,доц.	«24» июня 2021 г	С.В. Бегзатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.03(07)

доц.,к.т.н.,доц.	24.06.21	В.А. Мыльников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц.,к.э.н.,доц.	24.06.21	Г.С. Армашова-Тельник
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Защита информации в распределенных информационных системах» входит в базовую часть образовательной программы подготовки обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленность «Обеспечение информационной безопасности распределенных информационных систем». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-6 «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»;

общепрофессиональных компетенций:

ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»;

профессиональных компетенций:

ПК-12 «способность участвовать впроектировании системы управления информационной без

ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»,

ПК-28 «способность управлять информационной безопасностью автоматизированной системы»;

профессионально-специализированных компетенций:

ПСК-7.1 «способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах».

Содержание дисциплины охватывает круг вопросов, связанных с изучением архитектуры распределенных информационных систем (РИС), особенностей защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, защитой информации на уровне подсистемы управления, защитой информации в каналах связи и особенностями защиты информации в базах данных.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель преподавания дисциплины «Защита информации в распределенных информационных системах» для студентов специальности «10.05.03 «Информационная безопасность автоматизированных систем» заключается в приобретении теоретических знаний и формировании практических навыков , связанных с проектированием архитектуры распределенных ИС, разработкой системы защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, организации защиты информации на уровне подсистемы управления, в каналах связи и в распределенных базах данных.

Под распределенными понимаются ИС, которые не располагаются на одной контролируемой территории, на одном объекте.

В общем случае, распределенная информационная система (РИС) представляет собой множество сосредоточенных ИС, связанных в единую систему с помощью коммуникационной подсистемы.

Сосредоточенными ИС могут быть отдельные ЭВМ, в т.ч. и ПЭВМ, вычислительные системы и комплексы, а также локальные вычислительные сети (ЛВС).

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-6 «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»:

знать – основные принципы технологии «клиент-сервер», надежность и безопасность технологии;
уметь – рассчитывать и анализировать показатели надежности и безопасности РИС;
владеть навыками – проведения комплексного анализа системы защиты РИС от несанкционированного доступа;
иметь опыт деятельности – в расчете показателей и определения уровня защиты информации в РИС;

ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»:

знать – типы серверов приложений, функции прикладных протоколов и системы их защиты;
уметь – проектировать систему защиты информации в распределенных информационных системах, проводить синтез и анализ проектных решений по обеспечению безопасности РИС;
владеть навыками – выбора и обоснования проектных решений для обеспечения безопасности РИС;
иметь опыт деятельности – по анализу спроектированных систем защиты информации в РИС;

ПК-12 «способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»:

знать – способы представления и защиты данных в распределенных информационных системах;

уметь - применять криптографические протоколы для передачи и хранения данных в распределенных информационных системах;
владеть навыками – реализации криптографических протоколов в каком-либо языке программирования;
иметь опыт деятельности – внедрения криптографических протоколов в процессы передачи данных в РИС.

ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»:

знать – методы, способы и средства получения, хранения и переработки информации;
уметь – использовать источники экономической, социальной и управленческой информации;
владеть навыками – применения современных методов сбора, обработки и анализа данных;
иметь опыт деятельности – по построению информационных моделей;

ПК-28 «способность управлять информационной безопасностью автоматизированной системы»:

знать – современные инструментальные средства разработки схемы базы данных;
уметь – создавать объекты баз данных в современных системах управления базами данных и управлять доступом к этим объектам;
владеть навыками – использования технологий разработки баз данных в различных предметных областях;
иметь опыт деятельности – работы с объектами базы данных в конкретной системе управления базами данных

ПСК-7.1 «способность разрабатывать и исследовать
модели информационно-технологических
ресурсов, разрабатывать модели угроз и
модели нарушителя информационной
безопасности в распределенных
информационных системах»:
знать – методы проектирования системы управления информационной безопасностью;
уметь - проектировать системы управления информационной безопасностью;
владеть навыками – разрабатывать системы управления информационной безопасностью автоматизированной системы;
иметь опыт деятельности – в методах проектировании системы управления информационной безопасностью автоматизированной системы;

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Учебная практика
- Производственная (эксплуатационная) практика
- Учебная (ознакомительная) практика
- Информатика
- Информационные технологии
- Основы программирования
- Основы информационной безопасности
- Технологии и методы программирования
- Теория информации

- Теория информационной безопасности
- Производственная (эксплуатационная) практика
- Моделирование систем
- Техническая защита информации
- Распределенные сети хранения данных
- Распределенные информационные системы

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Проектирование безопасных информационных систем
- Научно-технический семинар
- Управление информационной безопасностью
- Научно-исследовательская работа
- Производственная преддипломная практика
- Информационная безопасность распределенных информационных систем
- Технология построения защищенных распределенных приложений
- Защита информации в сенсорных сетях
- Технологии защиты электронных платежей
- Защита банковской информации
- Разработка мобильных приложений

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	8	8
Аудиторные занятия, всего час., ***В том числе***	51	51
лекции (Л), (час)	34	34
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	36	36

Самостоятельная работа, всего	21	21
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 8					
Раздел 1. Архитектура распределенных ИС	2		2		2
Раздел 2. Особенности защиты информации в РИС	4		2		2
Раздел 3. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС	6		2		3
Раздел 4. Защита информации на уровне подсистемы управления	6		3		4
Раздел 5. Защита информации в каналах связи	8		4		4
Раздел 6. Особенности защиты информации в распределенных базах данных	8		4		4
Итого в семестре:	34		17		21
Итого:	34	0	17	0	21

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Архитектура распределенных ИС Коммутационная подсистема РИС: - коммутационные модули (КМ); - каналы связи; - концентраторы; - межсетевые шлюзы. Подсистемы РИС: - пользовательская; - подсистема управления; - коммуникационная подсистема
2	Раздел 2. Особенности защиты информации в РИС Корпоративные и общедоступные РИС.

	Построение системы защиты информации в РИС. Особенности защиты информации от непреднамеренных угроз в РИС. Помехоустойчивое кодирование. Потери информации в РИС. Пассивные и активные угрозы безопасности информации в РИС. Меры, предпринимаемые для обеспечения безопасности информации в сосредоточенных ИС, механизмы для защиты информации при передаче ее по каналам связи, а также для защиты от несанкционированного воздействия на информацию ИС с использованием ИС. Методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети
3	Раздел 3. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС Необходимость поддержки механизмов аутентификации и разграничения доступа удаленных процессов к ресурсам объекта, а также наличие в сети специальных коммуникационных компьютерных систем. Специализированные коммуникационные компьютерные системы. Концентраторы, коммуникационные модули (серверы), шлюзы и мосты Виды шифрования в ИС: линейное и абонентское шифрование. Центр управления сетью. Средства защиты информации специализированной ИС администратора сети как от непреднамеренных, так и от преднамеренных угроз. Защита процедур со средств, связанных с хранением и работой с ключами. Механизмы, блокирующие возможность работы с информационной частью сообщений, которые не предназначаются администратору
4	Раздел 4. Защита информации на уровне подсистемы управления Управление передачей сообщений по определенным протоколами. Международные стандарты взаимодействия удаленных элементов сети: протокол TCP/IP и протокол X.25. Модель OSI. Задачи обеспечения безопасности информации в сети на различных уровнях. Проблемы защиты информации в РИС
5	Раздел 5. Защита информации в каналах связи Комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. Шифрование на абонентском уровне. Линейное шифрование. Процедуры взаимного подтверждения подлинности абонентов или процессов.
6	Раздел 6. Особенности защиты информации в распределенных базах данных Базы данных как надежное хранилище структурированных данных, снабженное специальным механизмом для их эффективного использования в интересах пользователей (процессов). СУБД – система управления базой данных, под которой понимаются программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т.п. Проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Особенности защиты информации в базах данных. Встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент. Решение задач разграничения доступа, поддержания физической

	целостности и логической сохранности данных. Разграничение доступа к файлам баз данных и к частям баз данных путем установления полномочий пользователей и контроля этих полномочий при допуске к объектам доступа. Использование отказоустойчивых устройств, построенных по технологии RAID. Шифрование с помощью единого ключа, или индивидуальных ключей пользователей. Режимы работы с зашифрованными базами данных. Методы противодействия угрозам информации в базах данных

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисципли-ны
Учебным планом не предусмотрено				
Всего:				

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 8				
1	Архитектура распределенных ИС	2		1
2	Особенности защиты информации в РИС	2		2
3	Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС	2	2	3
4	Защита информации на уровне подсистемы управления	3	2	4
5	Защита информации в каналах связи	4	2	5
6	Особенности защиты информации в распределенных базах данных	4	2	6
Всего:		17	8	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 8, час
1	2	3
Самостоятельная работа, всего	21	21
изучение теоретического материала дисциплины (ТО)	10	10
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	11	11
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

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

Учебно-методические материалы для самостоятельной работы студентов указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 И 74	Информационный менеджмент [Текст] : учебник / Н. М. Абдикеев [и др.] ; ред. Н. М. Абдикеев. - М. : ИНФРА-М, 2012. - 400 с.	50
681.3 М 48	Мельников, В. П. Информационная безопасность [Текст] : учебное пособие для СПО / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 7-е изд., стер. - М. : Академия, 2012. - 332 с.	40
004 Ф 34	Федотова, Е. Л. Информационные технологии и системы [Текст] : учебное пособие / Е. Л. Федотова. - М. : ФОРУМ : ИНФРА-М, 2012. - 352 с.	50
355/359 О-93	Оценка устойчивости функционирования объектов экономики [Текст] : методические указания к практическим занятиям / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; Сост. А. В. Матвеев, Ю. В. Симагин. - СПб. : Изд-во ГУАП, 2013. - 44 с.	200
Х Т 69	Трифонова, Юлия Викторовна. Организация обработки персональных данных в соответствии с законодательством РФ [Текст] : учебное пособие / Ю. В. Трифонова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2013. - 99 с.	60
004 М 87	Мошак, Николай Николаевич (проф.). Защищенные инфотелекоммуникации. Анализ и синтез [Текст] : монография / Н. Н. Мошак ; С.-Петерб. гос. ун-т	40

	аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 197 с.	
004 М 87	Мошак, Николай Николаевич (проф.). Организация безопасного доступа к информационным ресурсам [Текст] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 121 с.	40

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 И 74	Информационные системы и технологии в экономике и управлении [Электронный ресурс] : учебник / С.-Петерб. гос. ун-т экономики и финансов ; ред. В. В. Трофимов. - 3-е изд. перераб. и доп. - Электрон. текстовые дан. - М. : Юрайт, 2012.	1
Х С 50	Смирнов, А. А. Обеспечение информационной безопасности в условиях виртуализации общества : Опыт Европейского Союза [Текст] / А. А. Смирнов. - М. : ЮНИТИ-ДАНА : Закон и право, 2012. - 159 с.	2
004(075) А 91	Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД [Текст] : учебное пособие / А. В. Астахова. - СПб. : Троицкий мост, 2014. - 216 с. : рис., табл. - Библиогр.: с. 210 - 214	5
004 М 48	Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с.	10
004 О-54	Олифер, В. Г. Безопасность компьютерных сетей [Текст] : [учебное пособие] / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия - Телеком, 2014. - 644 с.	10

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
www.intuit.ru	Национальный Открытый Университет "ИНТУИТ"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование

	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-6 «способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»	
1	История
2	Философия
2	Учебная (ознакомительная) практика

3	Социальная психология
3	Психология и педагогика
4	Учебная практика
6	Производственная (эксплуатационная) практика
8	Производственная (конструкторская) практика
8	Защита информации в распределенных информационных системах
9	Проектирование безопасных информационных систем
9	Основы управленческой деятельности
9	Управление информационной безопасностью
9	Научно-технический семинар
9	Научно-исследовательская работа
9	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-технический семинар
10	Научно-исследовательская работа
10	Производственная преддипломная практика
ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»	
1	Промышленная экология
1	Информатика
1	Экология
2	Основы программирования
2	Учебная (ознакомительная) практика
3	Основы программирования
3	Информационные технологии
4	Основы информационной безопасности
4	Учебная практика
4	Технологии и методы программирования
4	Безопасность жизнедеятельности
5	Теория информации
6	Теория информационной безопасности
6	Производственная (эксплуатационная) практика
6	Моделирование систем
7	Техническая защита информации
8	Производственная (конструкторская) практика
8	Языки программирования
8	Защита информации в распределенных информационных системах
9	Научно-исследовательская работа
9	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Информационная безопасность распределенных

	информационных систем
10	Технология построения защищенных распределенных приложений
10	Производственная преддипломная практика
ПК-12 «способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»	
5	Мультимедиа технологии
5	Технологии обработки аудио- и видеоданных
8	Защита информации в распределенных информационных системах
8	Производственная (конструкторская) практика
10	Производственная преддипломная практика
ПК-13 «способность участвовать в проектировании средств защиты информации автоматизированной системы»	
2	Учебная (ознакомительная) практика
4	Учебная практика
7	Распределенные сети хранения данных
7	Распределенные информационные системы
8	Защита от вредоносных программ
8	Производственная (конструкторская) практика
8	Защита информации в распределенных информационных системах
9	Защита информации в сенсорных сетях
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Разработка мобильных приложений
10	Производственная преддипломная практика
ПК-28 «способность управлять информационной безопасностью автоматизированной системы»	
6	Производственная (эксплуатационная) практика
7	Распределенные сети хранения данных
7	Распределенные информационные системы
8	Защита информации в распределенных информационных системах
10	Технология построения защищенных распределенных приложений
10	Производственная преддипломная практика
ПСК-7.1 «способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах»	
8	Защита информации в распределенных информационных системах

10	Методы проектирования защищенных распределенных информационных систем

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \le К \le 84$	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \le К \le 69$	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$К \le 54$	«неудовлетво рительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	2. Коммутационная подсистема РИС 3. Подсистемы РИС 4. Особенности защиты информации в РИС

	5. Корпоративные и общедоступные РИС. 6. Построение системы защиты информации в РИС. 7. Особенности защиты информации от непреднамеренных угроз в РИС. 8. Помехоустойчивое кодирование. 9. Потери информации в РИС. 10. Пассивные и активные угрозы безопасности информации в РИС. 11. Меры, предпринимаемые для обеспечения безопасности информации в сосредоточенных ИС 12. Механизмы для защиты информации при передаче ее по каналам связи 13. Механизмы для защиты информации для защиты от несанкционированного воздействия 14. Методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети 15. Обеспечение безопасности информации в специализированных коммуникационных ИС 16. Необходимость поддержки механизмов аутентификации и разграничения доступа удаленных процессов к ресурсам объекта, 17. Специализированные коммуникационные компьютерные системы. Концентраторы, коммуникационные модули (серверы), шлюзы и мосты Виды шифрования в ИС: линейное и абонентское шифрование. 18. Центр управления сетью. 19. Средства защиты информации специализированной ИС администратора сети как от непреднамеренных, так и от преднамеренных угроз. 20. Защита процедур со средств, связанных с хранением и работой с ключами. 21. Механизмы, блокирующие возможность работы с информационной частью сообщений, которые не предназначаются администратору 22. Управление передачей сообщений по определенным протоколам Международные стандарты взаимодействия удаленных элементов сети: протокол TCP/IP и протокол X.25. 23. Модель OSI. 24. Задачи обеспечения безопасности информации в сети на различных уровнях. 25. Проблемы защиты информации в РИС 26. Защита информации в каналах связи 27. Комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. 28. Шифрование на абонентском уровне. 29. Линейное шифрование. 30. Процедуры взаимного подтверждения подлинности абонентов или процессов 31. Особенности защиты информации в распределенных базах данных 32. Базы данных как надежное хранилище структурированных данных 33. Проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. 34. Встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент. 35. Решение задач разграничения доступа, поддержания физической целостности и логической сохранности данных. 36. Использование отказоустойчивых устройств, построенных по технологии RAID. 37. Шифрование с помощью единого ключа, или индивидуальных ключей пользователей. 38. Режимы работы с зашифрованными базами данных.

	39. Методы противодействия угрозам информации в базах данных

40. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

41. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

42. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	1. К какой разновидности моделей управления доступом относится модель Белла-Ла Падулы? а) модель дискреционного доступа; б) модель мандатного доступа; в) ролевая модель. 2. Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.? 3. К каким мерам защиты относится политика безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным. 4. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу? а) ACL; б) списки полномочий субъектов; в) атрибутные схемы. 5. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность. 6. К основным принципам построения системы защиты АИС относятся: а) открытость;

	б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота. 7. Какие из следующих высказываний о модели управления доступом RBAC справедливы? а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей; б) роли упорядочены в иерархию; в) с каждым объектом доступа ассоциировано несколько ролей ; г) для каждой пары «субъект-объект» назначен набор возможных разрешений. 8. Диспетчер доступа... а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа; б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале; 9. Какие предположения включает неформальная модель нарушителя? а) о возможностях нарушителя; б) о категориях лиц, к которым может принадлежать нарушитель; в) о привычках нарушителя; г) о предыдущих атаках, осуществленных нарушителем; д) об уровне знаний нарушителя. 10. Что представляет собой доктрина информационной безопасности РФ? а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности; б) федеральный закон, регулирующий правоотношения в области информационной безопасности; в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов; г) совокупность официальных взглядов на цели, задачи, принципы и основные на- правления обеспечения информационной безопасности Российской Федерации. 11. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности? а) политика безопасности верхнего уровня; б) политика безопасности среднего уровня; в) политика безопасности нижнего уровня; г) принцип минимизации привилегий; д) защита поддерживающей инфраструктуры. 12. Какие из перечисленных ниже угроз относятся к классу преднамеренных? а) заражение компьютера вирусами; б) физическое разрушение системы в результате пожара; в) отключение или вывод из строя подсистем обеспечения функционирования вы- числительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.); г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации; д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; е) вскрытие шифров криптозащиты информации.

43. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	1. Ролевая игра Разбейтесь на группы из 5 человек. Каждая группа выбирает сферу деятельности из представленного ниже списка: — производство высокотехнологичных товаров — рекламное агентство — разработка программного обеспечения — банк — университет Придумайте название для вашей организации, ее миссию, положение на рынке, основные задачи. Опишите особенности вашей организации в двух-трех абзацах. Распределите между собой роли, соответстующие организационной структуре вашей организации (директор предприятия, начальник ИТ-отдела, директор охраны, администратор сети и т.д.). Составьте политику безопасности вашей организации. Каждый участник группы отвечает за раздел политики безопасности, соответствующей своей роли. Оценка задания будет включать как индивидуальную оценку каждого участника, так и групповую (полнота и согласованность). *2. Программирование* Используя любой язык программирования, напишите программу, реализующую соответствующий алгоритм шифрования/дешифрования (варианты распределяются преподавателем): Модифицированный шифр Цезаря (ключом является любое число). Моноалфавитный шифр (шифр простой замены) Шифр Гронсфельда Шифр Плейфейера Шифр Хилла Простой перестановочный шифр Решетка Флейберга Скремблер Следующие варианты заданий являются усложненными и могут предлагаться группам по 2 человека. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Хилла в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Гронсфельда в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования. 11. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте решетку Флейберга в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования. 12. Напишите программу, реализующую протокол строгой двусторонней аутентификации на основе случайных чисел. Используйте Шифр Плейфейера в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования. 13. Запрограммируйте линейный конгруэнтный генератор псевдослучайных чисел. 14. Запрограммируйте смешанный квадратичный генератор псевдослучайных чисел Следующие варианты представляют задания повышенной сложности и могут вы-полняться группами по 3 человека. 15. Разработайте программу, реализующую модель безопасности Белла-ЛаПадула. Основные функции программы: регистрация пользователей (при регистрации пользователь получает уровень допуска), авторизация, создание

	текстовых заметок (при создании заметка получает уровень секретности), просмотр и редактирование заметок. 16. Разработайте программу, реализующую диспетчер безопасности на основе ACL. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту. 17. Разработайте программу, реализующую диспетчер безопасности на основе списков полномочий субъектов. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту. *3. Использование прикладных программ* —. Установите и настройте любой антивирус. Проверьте ваши жесткие диски в режиме сканнера таким образом, чтобы антивирус сформировал лог в виде файла. Отправьте этот файл преподавателю как результат выполнения задания. —. Установите программу PGP. Сгенерируйте пару ключей: открытый и закрытый. Отправьте ваш открытый ключ преподавателю. В ответ вы получите открытый ключ преподавателя и зашифрованное для вас сообщение, подписанное электронной цифровой подписью. Расшифруйте сообщение. Проверьте ЭЦП (она может оказаться неверной). Отправьте преподавателю ответное зашифрованное сообщение, подписанное вашей электронной цифровой подписью. В сообщении напишите результат проверки ЭЦП преподавателя и текст, содержащийся в расшифрованном вами сообщении.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Цель преподавания дисциплины «Защита информации в распределенных информационных системах» для студентов специальности «10.05.03 «Информационная безопасность автоматизированных систем» заключается в приобретении теоретических знаний и формировании практических навыков , связанных с проектированием архитектуры распределенных ИС, разработкой системы защиты информации в РИС, обеспечением безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС, организации защиты информации на уровне подсистемы управления, в каналах связи и в распределенных базах данных.

Под распределенными понимаются ИС, которые не располагаются на одной контролируемой территории, на одном объекте.

В общем случае, распределенная информационная система (РИС) представляет собой множество сосредоточенных ИС, связанных в единую систему с помощью коммуникационной подсистемы.

Сосредоточенными ИС могут быть отдельные ЭВМ, в т.ч. и ПЭВМ, вычислительные системы и комплексы, а также локальные вычислительные сети (ЛВС).

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках

дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

- Архитектура распределенных ИС
- Особенности защиты информации в РИС
- Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС
- Защита информации на уровне подсистемы управления
- Защита информации в каналах связи
- Особенности защиты информации в распределенных базах данных

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задания для лабораторных работ заключаются в решении задач, рассмотренных в ходе лекций, таких как:

1. Архитектура распределенных ИС
2. Особенности защиты информации в РИС
3. Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных ИС
4. Защита информации на уровне подсистемы управления
5. Защита информации в каналах связи
6. Особенности защиты информации в распределенных базах данных

Лабораторные занятия проводятся после чтения лекций, дающих теоретические основы для их выполнения. Допускается выполнение лабораторных занятий до прочтения лекций с целью облегчения изучения теоретического материала при наличии описаний работ, включающих необходимые теоретические сведения или ссылки на конкретные учебные издания, содержащие эти сведения.

Преподаватель имеет право определять содержание лабораторных работ, выбирать методы и средства проведения лабораторных исследований, наиболее полно отвечающие их особенностям и обеспечивающие высокое качество учебного процесса.

Преподаватель формирует рубежные и итоговые результаты (рейтинги) студента по результатам выполнения лабораторных работ.

На лабораторном занятии студент имеет право задавать преподавателю и (или) лаборанту вопросы по содержанию и методике выполнения работы и требовать ответа по существу обращения.

Студент имеет право на выполнение лабораторной работы по оригинальной методике с согласия преподавателя и под его надзором – при безусловном соблюдении требований безопасности.

К выполнению лабораторной работы допускаются студенты, подтвердившие готовность в объеме требований, содержащихся в методических указаниях к лабораторной работе и (или) в устных предварительных указаниях преподавателя.

В ходе лабораторных занятий студенты ведут необходимые записи, составляют (по требованию преподавателя) итоговый письменный отчет. На первом занятии цикла лабораторных работ преподаватель должен дать конкретные указания по составлению и оформлению отчетов с целью обеспечения единообразия. В зависимости от особенностей цикла лабораторных занятий отчет составляется каждым студентом индивидуально, либо общий отчет – подгруппой из 2-3 студентов. По окончании лабораторной работы студенты обязаны представить отчет преподавателю для проверки с последующей защитой. По согласованию с преподавателем допускается представление к защите отчета о лабораторной работе во время следующего лабораторного занятия или в индивидуальные сроки, оговоренные с преподавателем. Допускается по согласованию с преподавателем представлять отчет о лабораторной работе в электронном виде.

Лабораторное занятие состоит из следующих элементов: вводная часть, основная и заключительная.

Вводная часть обеспечивает подготовку студентов к выполнению заданий работы. В ее состав входят:

– формулировка темы, цели и задач занятия, обоснование его значимости в профессиональной подготовке студентов;

– изложение теоретических основ работы;

– характеристика состава и особенностей заданий работы и объяснение методов (способов, приемов) их выполнения;

– характеристика требований к результату работы;

– инструктаж по технике безопасности при эксплуатации технических средств;

– проверка готовности студентов выполнять задания работы;

– указания по самоконтролю результатов выполнения заданий студентами.

Основная часть включает процесс выполнения лабораторной работы, оформление отчета и его защиту. Она может сопровождаться дополнительными разъяснениями по ходу работы, устранением трудностей при ее выполнении, текущим контролем и оценкой результатов отдельных студентов, ответами на вопросы студентов. Возможно пробное выполнение задания(ий) под руководством преподавателя.

Заключительная часть содержит:

– подведение общих итогов занятия;

– оценку результатов работы отдельных студентов;

– ответы на вопросы студентов;

– выдачу рекомендаций по устранению пробелов в системе знаний и умений студентов, по улучшению результатов работы;

– сбор отчетов студентов для проверки, изложение сведений, касающихся подготовки к выполнению следующей работы.

Вводная и заключительная части лабораторного занятия проводятся фронтально. Основная часть может выполняться индивидуально или коллективно (в зависимости от формы организации занятия).

Структура и форма отчета о лабораторной работе

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;
3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

Требования к оформлению отчета о лабораторной работе

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники…) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой