Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.06
Проектирование защищенных автоматизированных систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 104
самостоятельная работа 74,8
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 8
зачеты 7
курсовые проекты 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	15 5/6		7 4/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	24	24	40	40
Лабораторные	32	32	32	32	64	64
Индивидуальные консультации			0,5	0,5	0,5	0,5
Контактная работа на аттестации (в период экз. сессий)			0,3	0,3	0,3	0,3
Контактная работа на аттестации	0,2	0,2	0,5	0,5	0,7	0,7
Консультации перед экзаменом			1	1	1	1
В том числе в форме практ.подготовки			8	8	8	8
Итого ауд.	48	48	56	56	104	104
Контактная работа	48,2	48,2	58,3	58,3	106,5	106,5
Сам. работа	23,8	23,8	51	51	74,8	74,8
Часы на контроль			34,7	34,7	34,7	34,7
Итого	72	72	144	144	216	216

Программу составил(и):
ктн, Доцент, Цебренко Константин Николаевич

Рецензент(ы):
д.т.н. , Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Проектирование защищенных автоматизированных систем

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Основной целью освоения дисциплины "Проектирование защищенных
1.2	автоматизированных систем" является формирование у студентов знаний о
1.3	защищенных автоматизированных системах, их проектированию, разработке и
1.4	эксплуатации. Кроме того, целью дисциплины является развитие в процессе обучения
1.5	системного мышления, необходимого для решения задач по обеспечению
1.6	необходимого уровня информационной безопасности автоматизированных систем.

Задачи: -изучение принципов эксплуатации защищенных автоматизированных систем;

- овладение средствами и методами проектирования и разработки защищенных автоматизированных систем;

- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы информационной безопасности
2.1.2	Организационное и правовое обеспечение информационной безопасности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная практика: Преддипломная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах	
ПК-3.1: Фиксирует возникновение инцидентов информационной безопасности	
Знать	
Уровень 1	Минимальный необходимый уровень знаний фиксирования возникновения инцидентов информационной безопасности
Уровень 2	Уровень знаний фиксирования возникновения инцидентов информационной безопасности в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний фиксирования возникновения инцидентов информационной безопасности в объёме, соответствующем программе подготовки, без ошибок
ПК-3.2: Использует методы и средства резервного копирования информации	
Уметь	
Уровень 1	Продемонстрированы основные умения использования методов и средств резервного копирования информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения использования методов и средств резервного копирования информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения использования методов и средств резервного копирования информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-3.3: Устраняет уязвимости в автоматизированной системе	
Владеть	
Уровень 1	Имеется минимальный набор навыков устранения уязвимости в автоматизированной системе с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки устранения уязвимости в автоматизированной системе с некоторыми недочётами
Уровень 3	Продемонстрированы навыки устранения уязвимости в автоматизированной системе без ошибок и недочётов
ПК-3.4: Соотносит изменения в конфигурации автоматизированной системы с её защищенностью	
Знать	
Уровень 1	Минимальный необходимый уровень знаний соотнесения изменений в конфигурации автоматизированной системы с её защищенностью
Уровень 2	Уровень знаний соотнесения изменений в конфигурации автоматизированной системы с её защищенностью, допущено несколько негрубых ошибок

Уровень 3	Уровень знаний соотнесения изменений в конфигурации автоматизированной системы с её защищенностью без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Использует методы и средства резервного копирования информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Использует методы и средства резервного копирования информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Использует методы и средства резервного копирования информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Устраняет уязвимости в автоматизированной системе с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Устраняет уязвимости в автоматизированной системе с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Устраняет уязвимости в автоматизированной системе без ошибок и недочётов

ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении	
ПК-4.1: Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний разработки проектных документов на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний разработки проектных документов на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний разработки проектных документов на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
ПК-4.2: Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	
Уметь	
Уровень 1	Продемонстрированы основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-4.3: Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков проверки программы и алгоритмов на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки проверки программы и алгоритмов на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки проверки программы и алгоритмов на предмет соответствия требованиям защиты информации без ошибок и недочётов
ПК-4.4: Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками,

	выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения подготовки технической и проектной документации по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации без ошибок и недочётов
ПК-4.5: Предлагает конфигурации и состав автоматизированной системы	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков проверки программы и алгоритмы на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки проверки программы и алгоритмы на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки проверки программы и алгоритмы на предмет соответствия требованиям защиты информации без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Понятия и сущность защищённых автоматизированных систем.					
1.1	Тема 1. Основные понятия и классификация защищенных автоматизированных систем /Лек/	7	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
1.2	Тема 1: Основные понятия и классификация защищенных автоматизированных систем. /Лаб/	7	16	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	

1.3	Тема 2. Основы защиты информации в защищенных автоматизированных системах /Лек/	7	4	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
1.4	Тема 3. Угрозы безопасности информации в защищенных автоматизированных системах /Лек/	7	4	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
1.5	Тема 2: Программнотехнический уровень защиты автоматизированных систем. /Лаб/	7	16	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
1.6	Тема 4: Программнотехнический уровень защиты автоматизированных систем. /Лек/	7	2	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
1.7	Понятия и сущность защищённых автоматизированных систем /Ср/	7	23,8		Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Общие принципы проектирования и разработки защищённых автоматизированных систем					
2.1	Тема 5: Основы организации разработки защищенных АС. /Лек/	8	4	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
2.2	Тема 6: Общие принципы проектирования защищенных АС. /Лек/	8	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
2.3	Тема 7: Основы эксплуатации защищенных АС. /Лек/	8	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
2.4	Тема 7: Основы эксплуатации защищенных АС. /Лаб/	8	12	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	2
2.5	Тема 8: Криптографические протоколы обеспечения безопасности. /Лек/	8	4	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	

2.6	Тема 8: Криптографические протоколы обеспечения безопасности. /Лаб/	8	10	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	3
2.7	Тема 9: Основы администрирования АС. /Лек/	8	4	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
2.8	Тема 9: Основы администрирования АС. /Лаб/	8	10	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	3
2.9	Общие принципы проектирования и разработки защищённых автоматизированных систем /Ср/	8	51		Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. Промежуточная аттестация					
3.1	Индивидуальные консультации по курсовму проекту /ИК/	8	0,5	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
3.2	Защита курсового проекта /КА/	8	0,5	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
3.3	Зачет /КА/	7	0,2	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
3.4	Экзамен /КАЭ/	8	0,3	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	
3.5	Консультация перед экзаменом /Консл/	8	1	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4 ПК-4.1 ПК-4.2 ПК-4.3 ПК-4.4 ПК-4.5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

Задания в открытой форме
1. Автоматизированная система — это…
2. Информационные системы можно классифицировать по признакам…
3. Подсистема-это…
4. Унифицированные системы документации-это…
5. В концепции обеспечения информационной безопасности предприятия определяются…
6. Конфиденциальную информацию обычно классифицируют…
7. Обеспечение безопасности должно основываться на…
8. Для обеспечения мероприятия для защиты информации необходимо произвести…

9.К принципам построения технической системы безопасности относятся…
10. Архитектура системы должна быть…
11. В качестве объектов уязвимости рассматриваются…
12. Наличие и полнота политики безопасности-это…
13. Механизм одобрения для защищенных систем основан на…
14. Владелец информации и владелец ресурсов могут быть…
15. Формирование защиты в АС основывается на…
16. Организационное обеспечение-это…
17. В структуру информационного обеспечения входит…
18. На этапе хранения данных автоматизированная система охватывает…
19. База данных-это…
20. На этапе публикации (представления) информации ИО включает…

КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ
1. Реализуйте схему объекта информатизации
2. Реализуйте параметры локальной сети и список сотрудников
3. Реализуйте классификацию угроз по источнику
4. Реализуйте классификацию угроз по последствиям
5. Реализуйте перечень нормативно-правовых актов в области информационной безопасности
6.Реализуйте поиск и удаление временных файлов вручную
7. Реализуйте шифрование и дешифрование данных с помощью программ
8. Реализуйте схему построения модели СЗИ 9. Реализуйте архитектуру Веб-приложений 10. Реализуйте защиту от вирусов в Интернете
11. Реализуйте Защиту программы от несанкционированного использования с помощью USB-ключей
12. Реализуйте защиту папок и файлов
13. Реализуйте восстановление удаленных файлов и необратимое удаление информации
14. Реализуйте перечень антивирусных программ, указывая преимущества и недостатки
15. Реализуйте признаки заражения вредоносным ПО 16. Реализуйте характеристику оценочных стандартов
17. Реализуйте защитные средства программно-технического уровня для построения эшелонированной обороны информационной системы
18. Реализуйте процесс стеганографии и объясните принцип работы
19.Реализуйте свойства подписи на бумаге и электронной подписи
20. Реализуйте примеры нарушений целостности данных

КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ
Лабораторная работа№1 «Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»
1. Дать определение понятию « безопасность информации».
2. Какие действия понимаются под безответственностью пользователя?
3. Критерии оценки информационных систем.
4. Какие параметры защиты не учитываются концепцией защиты информации?
5. На чем основан механизм одобрения для защищенных систем?
Лабораторная работа№2 «Определение показателей защищенности информации при несанкционированном доступе»
1. В каких случаях используется способ декомпозиции задачи оценки эффективности защищенности системы?
2. Схема многозвенной защиты объекта информатизации
3. Требования к показателям защищенности шестого класса.
4. Что можно отнести к основным угрозам?
Лабораторная работа№3 «Критерии оценки и выбора CASE-средств. 1. Функциональные характеристики критериев 2. Что такое построение диаграмм?
3. Что такое имитационное моделирование?
4. Что такое прототипирование?
5. Назовите общие функции.
Лабораторная работа№4 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»
1. Для чего служит Доктрина информационной безопасности? 2. Что выступает в качестве средств защиты информации, подлежащих сертификации в Системе сертификации средств защиты информации по требованиям безопасности информации?
3. Основные схемы сертификации средств защиты информации.
4. Какие функции осуществляет ФСТЭК России в пределах своей компетенции?
Лабораторная работа№5 «Создание модели вероятного нарушителя» 1. Составляющие модели нарушителя.
2. Цели и задачи вероятного нарушителя.
3. Четыре категории нарушителя.
4. Что такое неформализованная модель?
5. Что такое формализованная модель?
Лабораторная работа№6 «Оценка защищённости информационной системы на основании методики ФСТЭК»
1. В каких случаях обязательно выполнение рекомендаций регулятора? 2. Что регламентируют нормы ФСТЭК?
3. Что относится к документам государственной организации?
4. Методы проверки в ходе аттестации.

5.2. Темы письменных работ

Тема курсового проекта: «Разработка эскизного проекта системы защиты автоматизированной информационной системы организации».
Задание на курсовой проект включает в себя разработку эскизного проекта подсистемы защиты информации от несанкционированного доступа для определенной в задании защищенной автоматизированной информационной системы (ЗАС) предприятия.
Задание предусматривает разработку и реализацию студентом одного из элементов политики безопасности учреждения (предприятия) в виде таблицы разграничения доступа (ТРД), а также экспериментальную проверку и оптимизацию выбранных решений (контрмер) по организации защиты ЗАС путем управления информационными рисками на основе моделей угроз и информационных потоков в среде программного комплекса Digital Security Office или другим способом.
При выполнении курсового проекта студент должен выполнить:
Определение перечня защищаемых ресурсов и их критичности.
Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.
Определение особенностей расположения, функционирования и построения средств ЗАС.
Определение угроз безопасности информации и класса защищенности ЗАС.
Формирование требований к построению СЗИ.
Определение уязвимостей автоматизированной системы и выбор средств защиты информации.
Проведение экспериментальных проверок и оптимизацию выбранных решений (контрмер) по организации защиты ЗАС
Оформить пояснительную записку и графическую часть проекта.
Кроме того, по решению кафедры в состав проекта могут быть включены дополнительные разделы, связанные с научно-исследовательской работой.
Примерный список тем выглядит следующим образом:
1. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации муниципального подчинения на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу голосовых сообщений.
2. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу голосовых сообщений.
3. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей
4. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу видеоизображений.
5. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.
6. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, поддерживающей передачу голосовых сообщений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования
7. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края, поддерживающей передачу голосовых сообщений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования
8. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района с сервисом электронной почты на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования
9. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, поддерживающей передачу видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования
10. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края, поддерживающей передачу голосовых сообщений, на базе локальной вычислительной сети
11. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ
12. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с сервисом электронной посты на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ
13. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края с использованием механизмов операционных систем на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ
14. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей, поддерживающей передачу видеоизображений и голосовых сообщений.
15. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с использованием механизмов операционных систем на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.
16. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с сервисом электронной посты на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.
17. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения

администрации края с ограничением пользователей в допуске к различным разделам информационной базы для распределенной вычислительной сети, состоящей из локальных вычислительных сетей.
18. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, с сервисом передачи видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования
19. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с ограничением пользователей в допуске к различным разделам информационной базы для комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования
20. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с использованием механизмов операционных систем на базе локальной вычислительной сети
21. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с применением программно-аппаратных средств защиты от несанкционированного доступа на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.
22. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей, где ЭВМ системы расположены в нескольких контролируемых зонах.
23. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации муниципального подчинения
24. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района
25. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края
26. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе комплекса локальных вычислительных сетей вычислительной сети, соединенных каналами общего пользования
27. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе локальной вычислительной сети
28. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из отдельных ЭВМ

5.3. Фонд оценочных средств

Задания в закрытой форме
1. Что отражает модель жизненного цикла информационной системы?
1) все события, происходящие с системой в процессе ее создания и использования
2) процесс создания системы
3) процессы, связанные с использованием системы 4) все события в системе во время ее эксплуатации
2. Для чего производится предварительное обследование объекта автоматизации?
1) для формирования концепции создания системы 2) для создания прототипа системы
3) для выяснения готовности предприятия к автоматизации 4) для формирования команды, которая будет работать над созданием системы
3. Из перечисленного аутентификация используется на уровнях:
1) Прикладном 2) сетевом
3) транспортном 4) сеансовом 5) канальном 6) физическом
4. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:
1) Аутентификация 2) контроль доступа 3) причастность 4) целостность
5) идентификация
6) контроль трафика
5. Укажите основную цель детального обследования объекта автоматизации.
1) формирование технического задания на систему 2) подбор исполнителя для создания системы 3) определение целей автоматизации
4) выбор технических и программных инструментов
6. Отметьте методы сбора информации при проведении обследования объекта автоматизации.
1) анкетирование
2) интервьюирование 3) метод аналогий
4) создание "фотографии рабочего дня" 5) метод проб и ошибок 6) метод Монте-Карло
7. Из перечисленного в автоматизированных системах используется аутентификация по:
1) Паролю 2) Предмету
3) физиологическим признакам 4) терминалу
5) периферийным устройствам
8. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:
1) расследование причин нарушения защиты 2) исправление ошибок в программном обеспечении 3) управление доступом пользователей к данным 4) устранение дефектов
9. Какие данные обрабатываются в фактографических информационных системах?
1) структурированные данные в виде текстов и чисел 2) любые изображения
3) только числовые
4) исторические факты
10. Какая методология моделирования систем использует понятие "Прецедент"?
1) методология объектно-ориентированного моделирования 2) структурное моделирование 3) визуальное моделирование
4) функциональное моделирование

11. Из перечисленного в ОС UNIX регистрационная запись средств аудита включает поля:
1) дата и время события
2) идентификатор пользователя 3) команда, введенная пользователем 4) пароль пользователя 5) результат действия
6) тип события
12. Из перечисленного в ОС UNIX существуют администраторы:
1) Аудита 2) Печати
3) Службы контроля 4) Тирожирования 5) Системных утилит
6) Службы аутентификации
13. В основе архитектурного проектирования лежат понятия:
1) Проектирование – как средство достижения поставленного результата 2) Архитектура – как результат 3) Архитектура – как видение
4) Проектирование – как инструмент планирования разработки
14. Проектирование — это
1) вид активности, направленный на создание уникального продукта (услуги), последовательность этапов реализации которого, будет определяться «внешними» факторами, и определять его конечные преимущества и недостатки
2) видение конечного результата реализации информационной системы 3) процесс формирования структуры проекта
4) анализ текущего состояния структуры компании и предложение идей об улучшении бизнес-процессов
15. Из перечисленного в соответствии с видами объектов привилегии доступа подразделяются на:
1) базы данных 2) процедуры 3) сервер баз данных 4) события
5) терминалы 6) модули
16. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:
1) Владельца
2) конкретных заданных пользователей 3) Всех основных пользователей
4) конкретных заданных групп пользователей 5) Членов группы владельца
17. Архитектурное проектирование - это
1) процесс реализации пожеланий Стэйкхолдеров 2) работы по подготовке структуры взаимодействия систем в организации
3) вид активности, который своей целью ставит создание архитектуры в процессе выполнения проекта
4) вид работ по определению границ проекта
18. Архитектурное проектирование программного обеспечения, одной из задач ставит
1) бесперебойное функционирование информационных систем компании 2) поддержку и развитие существующих процессов и информационных систем компании
3) формирование особого видения, всех участников проекта, на конечный продукт
4) создание артефакта (архитектуры), который должен обеспечить достижение результатов деятельности организаций, использующих программные продукты для реализации своих процессов
19. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:
1) визуальное сканирование
2) исследование динамических характеристик движения руки

3) фрагментарное сканирование
4) исследование траектории движения руки
20. Из перечисленного для аутентификации по физиологическим признакам терминальных пользователей наиболее приемлемыми считаются:
1) Голос
2) Личная подпись 3) Отпечатки пальцев 4) Форма кисти 5) Форма губ
6) Форма ушной раковины
21. Программные продукты – это
1) исполняемые процедуры
2) реализация требований Спонсоров проекта 3) взаимосвязанные информационные сущности, выполняющие запросы Пользователей
4) основной элемент большинства современных высокотехнологичных доменов деятельности
22. Причиной развития темы архитектуры программного обеспечения является
1) рост издержек предприятий 2) развитие технологий
3) нарастающая конкуренция
4) требования к качеству информационных продуктов
23. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие
1) Выполнение 2) Запись 3) Чтение
4) Копирование 5) Удаление
24. Из перечисленного для СУБД важны такие аспекты информационной безопасности, как:
1) Своевременность 2) Доступность
3) Конфиденциальность
4) Целостность
5) многоплатформенность
25. Шаблоны проектирования (design patterns) представляет собой
1) руководство по реализации
2) универсальный свод информации 3) проектная документация на разработку 4) ограничения по реализации
26. Архитектурные решения - это

1) соглашения, учитывающие и удовлетворяющие различные точки зрения, «силы», принципы, как технического, так и не технического характера
2) соглашения, между Архитектором и Командой по реализации 3) тип используемых методик проектирования 4) видение конечного результата реализации
27. Из перечисленного защита процедур и программ осуществляется на уровнях:
1) Аппаратуры 2) Канальном 3) Сеансом 4) Данных
5) прикладном
6) Программного обеспечения
28. Из перечисленного контроль доступа используется на уровнях:
1) Прикладном 2) Сеансовом 3) Канальном 4) Сетевом
5) Транспортном
29. Выбор стиля использования шаблонов производится на основании
1) имеющихся ресурсов 2) конкурентной среды 3) политики организации 4) требований
30. Сложность обеспечения информационной безопасности является следствием:
1) злого умысла разработчиков информационных систем 2) объективных проблем современной технологии программирования 3) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы
31. Из перечисленного метка безопасности состоит из таких компонентов, как:
1) Категория
2) Ключ шифра 3) Области
4) Уровень секретности 5) Множество ролей
32. Из перечисленного методами защиты потока сообщений являются:
1) нумерация сообщений; 2) отметка времени;
3) использование случайных чисел; 4) нумерация блоков сообщений; 5) копирование потока сообщений
33. Сложность обеспечения информационной безопасности является следствием:
1) невнимания широкой общественности к данной проблематике 2) все большей зависимости общества от информационных систем 3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним
34. Что из перечисленного относится к числу основных аспектов информационной безопасности:
1) подотчетность - полнота регистрационной информации о действиях субъектов
2) приватность - сокрытие информации о личности пользователя
3) конфиденциальность - защита от несанкционированного ознакомления
35. Из перечисленного на сетевом уровне рекомендуется применение услуг:
1) идентификации; 2) конфиденциальности; 3) контроля трафика; 4) контроля доступа; 5) целостности;
6) аутентификации
36. Из перечисленного на транспортном уровне рекомендуется применение услуг:
1) идентификации; 2) конфиденциальности; 3) контроля трафика; 4) контроля доступа; 5) целостности;
6) аутентификации
37. Компьютерная преступность в мире:
1) остается на одном уровне 2) снижается
3) растет
38. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
1) доступность 2) целостность
3) защита от копирования 4) конфиденциальность
39. Из перечисленного объектами для монитора обращений являются:
1) терминалы; 2) программы; 3) файлы; 4) задания; 5) порты;
6) устройства
40. Из перечисленного пользователи СУБД разбиваются на категории:
1) системный администратор; 2) сетевой администратор;
3) администратор сервера баз данных;
4) администратор базы данных; 5) конечные пользователи; 6) групповые пользователи
41. Укажите, с какой целью строятся диаграммы для экспозиции (FEO).
1) для иллюстрации отдельных фрагментов модели 2) для иллюстрации альтернативной точки зрения 3) для иллюстрации специальных целей
4) для иллюстрации взаимосвязи между работами
42. Укажите, что показывает диаграмма дерева узлов.
1) иерархическую зависимость работ 2) взаимосвязи между работами 3) глубины детализации
43. Из перечисленного привилегии в СУБД могут передаваться:
1) субъектам; 2) группам; 3) ролям;
4) объектам; 5) процессам
44. Из перечисленного привилегиями безопасности являются:
1) субъектам; 2) группам; 3) ролям;
4) объектам; 5) процессам
45. Укажите, что входит в определение контекста модели.
1) определение субъекта моделирования 2) определение цели моделирования 3) определение точки зрения
4) определение количества уровней декомпозиции
46. Какие типы элементарных моделей используются для построения организационно-функциональной структуры?
1) древовидные модели (классификаторы) 2) процессные модели
3) матричные модели

47. Из перечисленного система брандмауэра может быть:
1) репитором; 2) маршрутизатором; 3) ПК;
4) хостом;
5) ресивером
48. Из перечисленного структура ОС с точки зрения анализа ее безопасности включает уровни:
1) внешний; 2) сетевой;
3) клиентский; 4) серверный; 5) системный; 6) приложений
49. Какая модель отвечает на вопросы: зачем компания занимается именно этим бизнесом, почему предполагает быть конкурентоспособной, какие цели и стратегии для этого необходимо реализовать?
1) стратегическая модель целеполагания 2) организационно-функциональная модель 3) функционально-технологическая модель 4) процессно-ролевая модель 5) модель структуры данных
50. Сформулируйте цель методологии проектирования ИС
1) регламентация процесса проектирования ИС и обеспечение управления этим процессом с тем, чтобы гарантировать выполнение требований как к самой ИС, так и к характеристикам процесса разработки
2) формирование требований, направленных на обеспечение возможности комплексного использования корпоративных данных в управлении и планировании деятельности предприятия
3) автоматизация ведения бухгалтерского аналитического учета и технологических процессов
51. Из перечисленного субъектами для монитора обращений являются:
1) терминалы; 2) программы;

3) файлы; 4) задания; 5) порты;
6) устройства
52. Из перечисленного функция подтверждения подлинности сообщения использует следующие факты:
1) санкционированный канал связи; 2) санкционированный отправитель; 3) лицензионное программное обеспечение; 4) неизменность сообщения при передаче; 5) доставка по адресу
53. Выделите утверждение, верное в отношении защиты сетей.
1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена
2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев
3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена
4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев
54. Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?
1) эффективность безопасности 2) гарантированность безопасности 3) непрерывность безопасности 4) надежность безопасности
55. Из перечисленного электронная почта состоит из:
1) электронного ключа;
2) расширенного содержания письма; 3) краткого содержания письма; 4) тела письма;
5) прикрепленных файлов
56. Из перечисленного, ГОСТ 28147-89 используется в режимах:
1) выработка имитовставки
2) гаммирование
3) гаммирование с обратной связью 4) простая замена
57. Каким термином обозначается анализ регистрационной информации системы защиты?
1) мониторинг 2) аудит
3) аккредитация 4) сертификация
58. Какие компоненты присутствуют в модели системы защиты с полным перекрытием?
1) область угроз 2) область рисков
3) защищаемая область 4) система защиты
5) область безопасности
59. Антивирусными программами являются:
1) Kaspersky Securite 2) Eset NOD 32 3) WinRar 4) DropBox
5) Avast
6) Mozilla Firefox
60. Главной составной частью системного программного обеспечения является:
1) графический интерфейс 2) операционная система 3) операционная оболочка 4) система обслуживания
61. Как называется возможность осуществления угрозы T в отношении объекта O?
1) слабость 2) неполнота 3) уязвимость 4) риск
62. Что означает система защиты с полным перекрытием?
1) для половины (и более) уязвимостей есть устраняющие барьеры 2) для любой уязвимости есть устраняющий ее барьер 3) у любой уязвимости есть риск ее реализации 4) количество уязвимостей меньше, чем количество препятствующих им барьеров
63. Что не входит в правовое обеспечение информационной безопасности?
1) Конституция РФ
2) Международная конвенция 3) Гражданский кодекс
4) Биометрическая зашита данных
64. Информационная безопасность – это:
1) защита целостности, доступности и конфиденциальности информации 2) комплекс мероприятий, направленных на

обеспечение информационной безопасности
3) потенциальная возможность определенным образом нарушить информационную безопасность
65. Чем характеризуется степень сопротивляемости механизма защиты?
1) вероятностью его преодоления
2) количеством угроз, которым этот механизм препятствует 3) величиной потерь в случае успешного прохождения 4) стоимостью механизма защиты
66. При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...
1) 0 2) 1
67. Какие программы относятся к прикладному ПО:
1) Paint, MS Word, 1С-Бухгалтерия 2) MS PowerPoint, Google, Skype 3) Блокнот, Windows Media, Wordpad
68. К формам защиты информации не относится:

1) аналитическая 2) правовая
3) организационно-техническая
69. Защищенность системы защиты определяется как величина…
1) обратная суммарному количеству рисков 2) обратная остаточному риску 3) обратная уязвимости
4) равная сумме всех уязвимостей
70. В чем заключается идеология открытых систем информационной безопасности?
1) в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы
2) в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре
3) в открытости информации о стоимости реализации конкретной системы защиты
4) в открытости программных кодов средств защиты от производителей разных стран
71. Наиболее защищенная файловая система – это:
1) FAT 32 2) NASA 3) NTFS 4) FAT 16
72. Что не входит в виды угроз:
1) угроза доступности 2) угроза дублирования 3) угроза конфиденциальности 4) угроза целостности
73. Для чего в первую очередь нужна идеология открытых систем информационной безопасности?
1) для удешевления средств защиты информации 2) для минимизации рисков от реализации угроз
3) для совместимости компонент различных информационных систем
74. В чем заключается принцип минимизации привилегий?
1) выделение полных прав доступа только администраторам системы 2) выделение только тех прав, которые необходимы для реализации своих должностных обязанностей
3) выделение прав доступа в зависимости от величины возможного ущерба
75. Программа, которая предназначена для выполнения определенных пользовательских задач и рассчитана на непосредственное взаимодействие с пользователем:
1) лицензия
2) прикладное ПО 3) программный продукт 4) системное ПО
76. Комплекс мероприятий, которые направлены на защиту информации:
1) угроза
2) правовая защита 3) защита информации 4) спам
77. В чем заключается принцип эшелонирования обороны?
1) в том, чтобы использовать максимально возможное количество защитных средств
2) в простоте и управляемости информационной системы 3) в усилении самого надежного защитного рубежа 4) в том, чтобы не полагаться на один защитный рубеж
78. Что из нижеперечисленного относится к оперативным методам повышения безопасности?
1) систематическое тестирование
2) предотвращение ошибок в CASE-технологиях 3) обязательная сертификация 4) программная избыточность
79. Выберите виды информационных угроз:
1) контроль доступа, доступность, анонимность 2) сайты-подделки, взлом, целостность
3) доступность, конфиденциальность, целостность
80. Программное обеспечение классифицируется на:
1) базовое, стандартное, прикладное
2) практическое, прикладное, системное
3) системное, прикладное, системы программирования
81. Что из нижеперечисленного относится к мерам предотвращения угроз безопасности?
1) систематическое тестирование
2) предотвращение ошибок в CASE-технологиях 3) обязательная сертификация 4) программная избыточность
82. Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:
1) ошибки персонала при эксплуатации 2) ошибки программирования
3) сбой и отказы аппаратуры ЭВМ 4) ошибки алгоритмизации задач
83. Перечислите основные угрозы при незащищённом использовании сети Интернет:
1) спам
2) хостинг 3) бан 4) вирус
5) вредоносное ПО 6) платные подписки
84. Назначение операционной системы:
1) организовать взаимодействие пользователя с компьютером и выполнение всех других программ

2) редактирование, сохранение текстовых документов 3) монтировать видео, фото и звуковую информацию 4) выводить информацию на экран или печатающее устройство
85. На каких принципах должна строиться архитектура ИС?
1) проектирование на принципе закрытых систем

2) проектирование на принципе открытых систем 3) усиление самого сильного звена 4) усиление самого слабого звена 5) эшелонирование обороны
86. Какие органы исполнительной власти являются ключевыми в области технической защиты информации?
1) ФСТЭК России 2) ФСБ России 3) СВР России 4) МВД России 5) Роскомнадзор
87. В состав системного ПО входит Сервисное ПО. К нему относится:
1) набор программ, выполняющих прикладные задачи пользователя 2) набор утилит, которые позволяют пользователю управлять ресурсами компьютера
3) программы, предназначенные для создания других программ
88. К биометрической системе защиты относятся:
1) защита паролем
2) идентификация по радужной оболочке глаз 3) физическая защита данных
4) идентификация по отпечаткам пальцев 5) антивирусная защита
89. Какой орган государственной власти осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных?
1) ФСТЭК России 2) ФСБ России 3) СВР России 4) МВД России 5) Роскомнадзор
90. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?
1) ФСТЭК России 2) ФСБ России 3) МВД России
4) Роскомнадзор
91. Очень сложные пароли гарантируют 100% защиту?
1) Нет
2) Да, если после работы полностью очищать куки и не хранить пароль на компьютере
3) Да, если пароль не сохранен на компьютере
92. Какие вирусы активизируются после включения ОС?
1) Снифферы 2) Загрузочные 3) Трояны 4) Черви
93. Какой орган исполнительной власти осуществляет сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
1) ФСТЭК России 2) ФСБ России 3) МВД России 4) Роскомнадзор
94. Какой орган исполнительной власти в настоящее время выполняет функции Гостехкомиссиии России в области технической защиты информации?
1) ФСТЭК России 2) ФСБ России 3) МВД России 4) Роскомнадзор
95. Представляют ли угрозу вирусы для крупных компаний?
1) Нет
2) Да, представляют
3) Скорее нет. В крупных компаниях развита система безопасности 4) Если компания обладает сотрудниками занимающимися безопасностью сети, вирусы не могут нанести такому предприятию вреда
96. С чем связана атака введением произвольных запросов в базу данных?
1) Уязвимость SQL Injection 2) Сбой Denial of Service 3) Ошибка Denial of Service 4) Неполадка PHP Include
97. Какой орган исполнительной власти реализует контрольные функции в области обеспечения защиты (некриптографическими методами) информации?
1) ФСТЭК России 2) ФСБ России 3) МВД России 4) Роскомнадзор
98. Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?
1) ФСТЭК России 2) ФСБ России 3) МВД России 4) Роскомнадзор
99. Фильтрация контента, для чего она служит?
1) Защищает от скрытой загрузки вредоносного программного обеспечения
2) Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени
3) Отключает назойливую рекламу 4) Отсеивает поисковый спам
100. Какой уровень безопасности трафика обеспечивает WPA2?
1) Высокий 2) Низкий
3) Достаточный для домашней сети 4) Средний

Задания на установление правильной последовательности
1. Установить последовательность этапов стадии создания системы защиты информации
1. Внедрение системы защиты информации (этап установки, настройки, испытаний)
2. Формирование требований к системе защиты информации (предпроектный этап)
3. Подтверждение соответствия системы защиты информации (этап оценки)
4. Разработка системы защиты информации (этап проектирования)
2. Установить последовательность этапов внедрения системы безопасности
1. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и

процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
2. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
3. Установка и настройка средств защиты информации
4. Испытания и опытная эксплуатации системы защиты информации
3. Установить порядок проведения аттестации информационных систем по требованиям безопасности информации
Проведение аттестационных испытаний объекта
1. Предварительное ознакомление с аттестуемым объектом (при необходимости)
2. Оформление, регистрация и выдача аттестата соответствия
3. Подача и рассмотрение заявки на аттестацию
4. Разработка программы и методики аттестационных испытаний
4. Определить этапы уровня защищенности персональных данных 1. классификация информационной системы
2. сбор и анализ исходных данных по информационной системе
3. установление уровня защищенности персональных данных и его документальное оформление
4. формирование модели угроз и определение категории нарушителя
5.Установить последовательность этапов принципа действия сетевых червей
1. Поиск "жертв»
2. Подготовка копий
3. Проникновение в систему
4. Распространение копий
5. Активация
6. Установить последовательность этапов методического процесса построения корпоративной системы защиты от вирусов
1. Разработка политики антивирусной безопасности
2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности 3. Реализация плана антивирусной безопасности
4. Разработка плана обеспечения антивирусной безопасности
7. Установить порядок обеспечения защиты информации
1. Проверяется эффективность принятых мер
2. Составляется перечень коммерческих тайн и сведений, не подлежащих разглашению
3. Разрабатываются способы хранения информации (использование электронных носителей, бумажных документов, технических средств обработки)
8. Установить последовательность клиент-серверной архитектуры
1. клиентские компьютеры выступают потребителями
2. серверы являются поставщиками услуг (сервисов)
3. информационная система
9. Установить последовательность многозвенной архитектуры
1. Уровень данных 2. Представление 3. Уровень логики
4. Данные
5. Уровень представления
10. Установить последовательность этапов архитектуры распределенных систем с репликацией
1. Репликация
2. Сервер без данных
3. Клиентская ЭВМ
4. Репликация
11. Установить последовательность итерационного процесса разработки и реализации политики ИБ
1. Принципы контроля состояния систем защиты информации
2. Вопросы резервного копирования данных и информации
3. Принципы администрирования системы ИБ и управление доступом к вычислительным и телекоммуникационным средствам, программам и информационным ресурсам,
4. Принципы использования информационных ресурсов персоналом компании и внешними пользователями
5. антивирусную защиту и защиту против действий хакеров
12. Установить последовательность распределения ответственности за обеспечение безопасности
1. Назначение для каждого ресурса (или процесса) ответственного сотрудника из числа руководителей
2. Определение и документальное закрепление для каждого ресурса списка прав доступа (матрицы доступа)
3. Определение ресурсов, имеющих отношение к информационной безопасности по каждой системе
13. Установить последовательность ролевого управления доступом
1. Сеанс работы пользователя
2. Объект
3. Пользователь
4. Роль
5. Операция
14. Установить последовательность Метода OCTAVE
1. Осуществляется оценка организационных аспектов
2. Проводится разработка стратегии обеспечения безопасности
3. Высокоуровневый анализ ИТ-инфраструктуры организации
4. Определяются требования безопасности
5. Сроится профиль угроз для каждого критического ресурса
15. Установить последовательность возникновения плана обработки рисков метода OCTAVE
1. Атака на данные системы электронного документооборота

2. Выход из строя системы эл. документооборота или изменение/уничтожение данных на ресурсе 3. Атака на данные сервера разработки
4. Выход из строя сервера разработки или уничтожение изменение данных на данном ресурсе
16. Установить последовательность полной обработки рисков
1. Выход из строя сервера разработки или изменение/ уничтожение данных
2. Выход из строя СЭД или изменение/уничтожение данных
3. Угроза
4. Атака на данные СЭД
5. Атака на данные сервера разработки
17. Установить последовательность этапов проектирования информационных систем
1. Требуемой пропускной способности системы
2. Определения цели проекта
3. Требуемой функциональности системы и уровня ее адаптивности к Изменяющимся условиям функционирования
4. Безотказной работы системы
5. Простоты эксплуатации и поддержки системы
18. Установить последовательность этапов ЖЦ построения и последовательного преобразования ряда согласованных моделей
1. Требований к приложениям
2. Организации 3. Проекта ИС
4. Требований к ИС
19. Установить последовательность этапов создания АС 1. Реализация
2. Формирование требований к системе
3. Ввод в действие
4. Тестирование
5. Проектирование
20. Установить последовательность совокупности архитектурой программных систем
1. Выбор структурных элементов, составляющих систему и их интерфейсов
2. Объединение элементов в подсистемы 3. Организации программной системы
4. Поведение элементов во взаимодействии с другими элементами

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2022, URL: https://znanium.com/catalog/document?id=397282
Л1.2	Семеновых В.И., Перминов А.А.	Проектирование автоматизированных систем: Учебное пособие	Вологда: Инфра-Инженерия, 2022, URL: https://znanium.com/catalog/document?id=417415
Л1.3	Бабаш А. В., Баранова Е. К.	Криптографические методы и средства защиты информации: Учебник	Москва: КноРус, 2024, URL: https://book.ru/book/950118
Л1.4	Макаренко С.И., Ковальский А.А., Краснов С.А.	Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях: Учебное пособие	Санкт-Петербург: Наукоемкие технологии, 2020, URL: https://book.ru/book/942928
Л1.5	Бабаш А.В., Баранова Е.К.	Моделирование системы защиты информации: Практикум: Учебное пособие	Москва: Издательский Центр РИО□, 2023, URL: https://znanium.com/catalog/document?id=435530

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Коваленко Ю. И., Тараскин М. М., Торба О. И.	Нормативное обеспечение информационных систем в защищенном исполнении: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934104

	Авторы, составители	Заглавие	Издательство, год
Л2.2	Ковалев И.В., Золотарев В.В.	Поддержка принятия решений при проектировании систем защиты информации: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2020, URL: http://znanium.com/catalog/document?id=343296
Л2.3	Куняев Н.Н., Демушкин А.С.	Конфиденциальное делопроизводство и защищенный электронный документооборот: Учебник	Москва: Издательская группа "Логос", 2020, URL: http://znanium.com/catalog/document?id=367431
Л2.4	Королев М. В.	Обеспечение защищенности речевой информации при использовании систем виброакустического зашумления: Монография	Москва: Русайнс, 2022, URL: https://book.ru/book/944860
Л2.5	Енютина Т.А., Кулагина Л.В.	Расчет и проектирование систем обеспечения безопасности: Учебное пособие	Красноярск: Сибирский федеральный университет, 2022, URL: https://znanium.com/catalog/document?id=433082
Л2.6	Царегородцев А. В., Романовский С.В., Волков С.Д.	Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2024, URL: https://znanium.com/catalog/document?id=436066

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Национальный открытый университет "ИНТУИТ". - Режим доступа: https://www.intuit.ru/studies/courses%20
Э2	Электронно-библиотечная система . - Режим доступа: http://znanium.com/%20
Э3	ЭИОС. - Режим доступа: http://eios.imsit.ru/
Э4	ЭБС Айбукс. - Режим доступа: http://www.ibooks.ru/
Э5	РПД. - Режим доступа: http://rpd.eios.imsit.ru:8080/RPD/Index/1636711/%20http://www.book.ru

6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL

6.3.2. Перечень профессиональных баз данных и информационных справочных систем

6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
119	Лаборатория управления проектной деятельностью	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение

		Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express AnyLogic Archimate Klite Mega Codec Pack MS Office Standart 2007 Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	
114а	Лаборатория сетей и систем передачи информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Astra Linux Special Edition	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
Читальный зал	Информационно-библиотечный	7-Zip Яндекс Браузер	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и

	центр (помещение для самостоятельной работы обучающихся)	Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Проектирование защищенных автоматизированных систем», разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.
Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Проектирование защищенных автоматизированных систем».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная

последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями