МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____
И.Г.Игнатова
«23» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Защищенные информационные системы»

Направление подготовки – 10.04.01«Информационная безопасность»
Направленность (профиль) – «Аудит информационной безопасности»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций (подкомпетенций):

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1. ЗИС. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	**Знания** основные компоненты автоматизированных систем в защищенном исполнении (АСЗИ). Свойства и показатели АС. Жизненный цикл АС; состав системы защиты информации (СЗИ) АСЗИ. Функции СЗИ АСЗИ; стадии и этапы создания АСЗИ; основные требования к СЗИ АСЗИ; порядок формирования требований к структуре АСЗИ; требования и порядок разработки концепции АСЗИ; содержание: технического задания, эскизного проекта, технического проекта, рабочей документации. **Умения:** проводить предварительное обследование создаваемого объекта информатизации; формировать требований к АСЗИ в части системы защиты информации; разрабатывать проект технического задания на систему защиты информации (СЗИ) АС. **Опыт практической деятельности:** обоснования требований к системе обеспечения информационной безопасности и разработки проекта технического задания на ее создание.
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2. ЗИС. Способен разрабатывать технический проект автоматизированной системы в защищенном исполнении	**Знания** средства обеспечения надежности АСЗИ. Технологии создания отказоустойчивых систем; порядок сертификации средств защиты информации; порядок ввода АСЗИ в эксплуатацию на объекте информатизации; организацию обработки конфиденциальной информации АСЗИ; организацию технического обслуживания

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		АСЗИ. **Умения:** разрабатывать технический проект автоматизированной системы в защищенном исполнении; разрабатывать документацию на СЗИ АС; разрабатывать программы и методики испытаний системы защиты информации АС. **Опыт практической деятельности:** разработки технического проекта автоматизированной системы в защищенном исполнении.

В результате изучения дисциплины студент должен:

Знать:

- основные компоненты автоматизированных систем в защищенном исполнении (АСЗИ). Свойства и показатели АС. Жизненный цикл АС;
- состав системы защиты информации (СЗИ) АСЗИ. Функции СЗИ АСЗИ;
- стадии и этапы создания АСЗИ;
- основные требования к СЗИ АСЗИ;
- порядок формирования требований к структуре АСЗИ.
- требования и порядок разработки концепции АСЗИ;
- содержание: технического задания, эскизного проекта, технического проекта, рабочей документации;
- средства обеспечения надежности АСЗИ. Технологии создания отказоустойчивых систем;
- порядок сертификации средств защиты информации;
- порядок ввода АСЗИ в эксплуатацию на объекте информатизации;
- организацию обработки конфиденциальной информации АСЗИ;
- организацию технического обслуживания АСЗИ.

Уметь:

- проводить предварительное обследование создаваемого объекта информатизации;
- формировать требований к АСЗИ в части системы защиты информации;
- разрабатывать проект технического задания на систему защиты информации (СЗИ) АС;
- разрабатывать технический проект СЗИ АС;
- разрабатывать документацию на СЗИ АС.
- разрабатывать программы и методики испытаний системы защиты информации АС;
- проводить установку и настройку средств защиты информации от несанкционированного доступа;

– проводить контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа.

Иметь практический опыт:

– обоснования требований к системе обеспечения информационной безопасности и разработки проекта технического задания на ее создание;
– разработки технического проекта автоматизированной системы в защищенном исполнении.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙПРОГРАММЫ

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 2-м курсе в 3-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении дисциплин «Технологии защиты информации от утечки по техническим каналам» и «Технологии защиты информации от несанкционированного доступа», изучаемых в 1-м семестре.

Знания и умения, полученные в результате изучения дисциплины,используются в производственной практике и при подготовке ВКР.

Знания и умения, полученные в результате изучения дисциплины,используются в дисциплине«Защищенные информационные системы»,производственной практике и при подготовке ВКР.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы*	Практическая подготовка при выполнении курсового проекта	Вид промежуточной аттестации
				ВСЕГО	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации			
2	3	5	180	84	16	24	24	20	60	24	Экз. (36), КП

* Часы на самостоятельную работы, включая часы на практическую подготовку при выполнении курсовой работы

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы*	Практическая подготовка при выполнении курсового проекта	Формы текущего контроля
	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации			
1. «Создание автоматизированных систем в защищенном исполнении».	10	-	24	10	38	24	Компьютерный тест КТ-1.Зачет по ПЗ (ГУ) 1- 6 Защита КП
2. «Эксплуатация автоматизированных систем в защищенном исполнении».	6	24	-	10	22	-	Компьютерный тест КТ-2. Зачет по ЛР 1-5

* Часы на самостоятельную работы, включая часы на практическую подготовку при выполнении курсовой работы

4.1. Лекционные занятия

мер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
1.	1.	2	**Вводная. Автоматизированные системы – общие понятия.** Автоматизированные системы (АС) – общие понятия. Основные компоненты АС. Свойства и показатели АС. Жизненный цикл АС.
	2.	2	**Автоматизированные системы в защищенном исполнении (АСЗИ).** Состав системы защиты информации (СЗИ) АСЗИ. Функции СЗИ АСЗИ. Основные требования к СЗИ АСЗИ.
	3.	2	**Порядок создания АСЗИ** Стадии и этапы создания АСЗИ (в соотв. с ГОСТ Р 51583—2014 и ГОСТ 34.601-90). Формирование требований к структуре АСЗИ. Разработка концепции АСЗИ. Техническое задание. Эскизный проект. Технический

мер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			проект. Рабочая документация. Ввод в действие АСЗИ. Сопровождение АС.
	4.	2	**Средства обеспечения надежности АСЗИ** Средства обеспечения надежности АСЗИ. Технологии создания отказоустойчивых систем.
	5.	2	**Сертификация средств защиты информации** Сертификация технических средств защиты информации. Сертификация криптографических средств защиты информации. Сертификация антивирусных программ. Специальные исследования СВТ на ПЭМИН. Специальные технические проверки СВТ.
2.	6.	2	**Порядок ввода АСЗИ в эксплуатацию на объекте информатизации** Разработка схем расстановки основных технических средств и систем и вспомогательного оборудования на ОИ. Определение условий расположения ОИ относительно границ контролируемой зоны. Определение перечня сведений ограниченного доступа, подлежащих обработке на АСЗИ. Определение степени участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности. Определение режимов обработки информации в АС в целом и в отдельных компонентах. Классификация АС. Категорирование ОИ. Анализ угроз безопасности информации на ОИ. Разработка модели угроз безопасности информации. Настройка технических, программных и программно-аппаратных средств ЗИ. Разработка организационных мероприятий по ЗИ. Разработка организационно-распорядительных документов. Аттестация ОИ. Опытная эксплуатация АСЗИ. Приказ о вводе АСЗИ и СЗИ объекта информатизации в эксплуатацию.
	7.	2	**Организация обработки конфиденциальной информации АСЗИ** Порядок создания, учета, хранения и работы с электронными носителями конфиденциальной информации. Порядок уничтожения электронных носителей конфиденциальной информации. Порядок отправки электронных носителей конфиденциальной информации. Порядок печати конфиденциальных документов с электронных носителей, их регистрации и учета.

мер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	8.	2	**Организация технического обслуживания АСЗИ** Виды технического обслуживания АСЗИ. Средства диагностирования АСЗИ. Содержание и порядок ведения эксплуатационной документации. Организация восстановления системы защиты информации и защищаемой информации после воздействия угроз.

4.2. Практические занятия

Номер модуля дисциплины	Номер занятия	Объем занятий, часы	Краткое содержание
1.	1.	4	**Практическое занятие (групповое упражнение). Обследование создаваемого объекта информатизации и обоснование необходимости создания автоматизированной системы в защищенном исполнении (АСЗИ)** Анализ данных о назначении, функциях, условиях функционирования создаваемой АСЗИ. Определения перечня информации, подлежащей защите. Определение актуальных угроз безопасности информации. Разработка модели угроз безопасности информации. Технико-экономическая оценка целесообразности создания АСЗИ
	2.	4	**Практическое занятие (групповое упражнение). Формирование требований к АСЗИв части системы ЗИ** Подготовка исходных данных для формирования требований в части системы ЗИ к создаваемой АС (исходя из ее предназначения и условий использования), включая: - определение порядка обработки информации в АС в целом и в отдельных компонентах; - оценку степени участия персонала в обработке (обсуждении, передаче, хранении) защищаемой в АСЗИ информации; - определение требуемого класса (уровня) защищенности АС от

Номер модуля дисциплины	Номер занятия	Объем занятий, часы	Краткое содержание
			НСД; - выбор целесообразных (исходя из экономических, научно-технических, временных и других ограничений, а также технологии обработки информации) способов ЗИ и контроля состояния ЗИ в АС; - обоснование архитектуры и конфигурации системы ЗИ АС и ее отдельных составных частей, физических, функциональных и технологических связей как внутри АС, так и с другими взаимодействующими системами; - выбор ТС, которые могут быть использованы при разработке системы ЗИ АС; - оценку возможности создания АСЗИ, исходя из ресурсных ограничений; Формирование требований к системе ЗИ создаваемой АС в части требований по ЗИ.
	3.	4	**Практическое занятие (групповое упражнение). Разработка технического задания на систему защиты информации (СЗИ) АС** Состав, содержание и оформление ТЗ на СЗИ АС: общие сведения; назначение и цели создания (развития) системы; характеристика объекта автоматизации; требования к системе; состав и содержание работ по созданию системы; порядок контроля и приемки системы; требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие; требования к документированию; источники разработки. Общие требования к СЗИ АС (ГОСТ Р 51624): функциональные требования; требования к эффективности; технические требования; экономические требования; требования к документации. Номенклатура дополнительной документации по защите информации на АС.
	4.	4	**Практическое занятие (групповое упражнение). Разработка эскизного проекта системы ЗИ создаваемой АСЗИ.** Разработка предварительных проектных решений: - определение субъектов доступа (пользователей, процессов и иных субъектов доступа) и объектов доступа (устройств, объектов файловой системы, запускаемых и исполняемых модулей, объектов системы управления базами данных, объектов, создаваемых прикладным программным обеспечением, иных объектов доступа); - уточнение исходных данных, касающихся технических, инфор-

Номер модуля дисциплины	Номер занятия	Объем занятий, часы	Краткое содержание
			мационных, программных и организационных аспектов создания и функционирования системы ЗИ АСЗИ и АСЗИ в целом; - определение функций системы ЗИ создаваемой АСЗИ, состава комплексов задач и отдельных задач, решаемых подсистемой ЗИ; - проработку и рассмотрение вариантов построения системы ЗИ, определение общих требований к системе ЗИ (ее структура, состав (число) и места размещения составных частей системы ЗИ); - определение функций и параметров ТС и ПС системы ЗИ, особенностей их реализации в интересах блокирования (нейтрализации) угроз безопасности информации в АСЗИ; - определение состава организационных мер ЗИ, ТС и ПС системы ЗИ, выбор сертифицированных СЗИ с учетом их совместимости с основными ТС и ПС создаваемой (модернизируемой) АСЗИ; - обоснование номенклатуры СЗИ, специального технологического оборудования, средств контроля и измерений, подлежащих разработке в ходе создания АСЗИ.
	5.	4	**Практическое занятие (групповое упражнение). Разработка документации на СЗИ АС.** Разработка, оформление документации в объеме, необходимом для описания полной совокупностипринятых предварительных проектных решений и достаточном для дальнейшего выполнения работ по созданию системы ЗИ. Разработка рабочей документации на систему ЗИ, содержащей все необходимые и достаточные сведениядля обеспечения выполнения работ по вводу системы ЗИ АСЗИ в действие и ее эксплуатации, в томчисле для поддержания уровня эксплуатационных характеристик (качества) системы ЗИ в соответствиис принятыми проектными решениями, ее оформление, согласование и утверждение. Виды документов – по ГОСТ 34.201.
	6.	4	**Практическое занятие (групповое упражнение**). **Разработка программы и методик испытаний системы ЗИ АСЗИ.** Виды документов — по ГОСТ 34.201.

4.3.Лабораторные работы
(практическая подготовка при проведении лабораторных работ)

Номер модуля дисциплины	Номер лабораторной работы	Объем занятий, часы	Краткое содержание
2	1.	4	Установка и настройка программных средств защиты АС от НСД (ОС Windows (7, 8,10), «Фикс»). Установка и настройка подсистемы антивирусной защиты АС на основе антивирусных программы (Dr.Web, Касперский).
	2.	4	Лабораторная работа. Установка и настройка программно-аппаратных средств защиты АС от НСД («Панцирь-К», «Dallas Lock» и т.п.).
	3.	8	Лабораторная работа. Установка и настройка программного комплекса для обеспечения сетевой безопасности («Застава»).
	4.	4	Лабораторная работа. Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием средств контроля защищенности «Ревизор 1», «Ревизор 2», «TERRIER», «ФИКС».
	5.	4	Лабораторная работа. Контроль защищенности АС на соответствие требованиям по защите информации от несанкционированного доступа с использованием сканеров безопасности («Сканер-ВС», «Ревизор сети».

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1.	2	**Подготовка к практическому занятию (групповому упражнению) № 1:** Изучение материалов лекции №№ 1-5 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению практического занятия № 1.
	2	**Подготовка к практическому занятию (групповому упражнению) № 2:** Изучение материалов лекции №№ 1-5 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению практического занятия № 2.
	2	**Подготовка к практическому занятию (групповому упражнению) № 3:** Изучение материалов лекции №№ 1-5и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
		Изучениеметодических рекомендаций по проведению практического занятия № 3.
	2	**Подготовка к практическому занятию (групповому упражнению) № 4:** Изучение материалов лекции №№ 1-5 рекомендованной литературы. Изучениеметодических рекомендаций по проведению практического занятия № 4.
	2	**Подготовка к практическому занятию (групповому упражнению) № 5:** Изучение материалов лекции №№ 1-5 рекомендованной литературы. Изучениеметодических рекомендаций по проведению практического занятия № 5.
	2	**Подготовка к практическому занятию (групповому упражнению) № 6:** Изучение материалов лекции №№ 1-5 рекомендованной литературы. Изучениеметодических рекомендаций по проведению практического занятия № 6.
	2	**Подготовка к компьютерному тесту КТ-1** Изучение материалов лекции №№ 1-5 и рекомендованной литературы.
2.	4	**Подготовка к лабораторной работе № 1:** Изучение материалов лекции №№ 6-8 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению лабораторной работы № 1.
	4	**Подготовка к лабораторной работе № 2:** Изучение материалов лекции №№ 6-8 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению лабораторной работы № 2.
	4	**Подготовка к лабораторной работе № 3:** Изучение материалов лекции №№ 6-8 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению лабораторной работы № 3.
	4	**Подготовка к лабораторной работе № 4:** Изучение материалов лекции №№ 6-8 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению лабораторной работы № 4.
	4	**Подготовка к лабораторной работе № 5:** Изучение материалов лекции №№ 6-8 и рекомендованной литературы. Изучениеметодических рекомендаций по проведению лабораторной работы № 5.
	2	**Подготовка к компьютерному тесту КТ-2** Изучение материалов лекции №№ 6-8 и рекомендованной литературы.
1.	24	**Выполнениекурсового проекта**

4.5. Примерная тематика курсовых работ (проектов)

Тема курсового проекта «Разработка технического проекта на создание системы защиты информации автоматизированной системы».

Для выполнения задания студентам выделяются реально существующие объекты информатизации предприятий (учреждений).

Разработка технического проекта на создание системы защиты информации автоматизированной системы выбранных объектов информатизации проводятся студентами в ходе производственной практики.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Модуль 1.Методы и средства контроля эффективности защиты информации, обрабатываемой СВТ:

Тексты лекций № 1 – 2. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 1 – 3. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Методы и средства контроля эффективности защиты речевой информации

Тексты лекций № 3 – 4. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 4 – 6. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Гвоздева, Т. В. Проектирование информационных систем. Стандартизация: учеб. пособие / Т. В. Гвоздева, Б. А. Баллод. - 2-е изд., стер. - Санкт-Петербург: Лань, 2021. - 252 с. - URL: https://e.lanbook.com/book/169810 (дата обращения: 15.03.2021). - ISBN 978-5-8114-7963-4.

2. Коваленко В.В. Проектирование информационных систем: учеб. пособие. - М. : Форум, 2012. - 320 с. - (Высшее образование). - ISBN 978-5-91134-549-5.

3. Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва : Флинта : Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 16.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.

4. Программно-аппаратные средства защиты информации: учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1.

5. Программно-аппаратные средства защиты информации: учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образо-

вания и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 .

6. Зайцев А.П. Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.

7. Управление безопасностью критических информационных инфраструктур: учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8.

8. Хорев, А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А. А. Хорев. - М. : НПЦ "Аналитика", 2008. - 436 с. - 3000 экз. - ISBN 978-59901488-1-9.

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : – URL: https://docs.cntd.ru/document/901990051 - (дата обращения 15.03.2021).-Текст электронный .

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ: (ред. от 02.07.2021) «О персональных данных»; Текст: электронный // Техэксперт URL: https://docs.cntd.ru/document/573249803?marker=64U0IK (дата обращения 15.03.2021). - Текст: электронный.

3. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 30.11.2020) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации".

4. Постановление Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (ред. от 30.11.2020).

5. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

6. Методический документ. Методика оценки угроз безопасности информации. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2021 г. (утверждена ФСТЭК России 5 февраля 2021 г.)

7. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.

8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

9. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

11. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

12. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

13. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

14. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Общие положения; Национальный стандарт РФ : Введ. 09.02.1995: М.: Издательство стандартов (Переиздание) Стандартинформ, август 2006 -URL: https://docs.cntd.ru/document/1200004675 (дата обращения: 15.03.2021) -Текст: электронный.

15. Защита информации. Основные термины и определения; Protection of information. Basic terms and definitions: Национальный стандарт РФ: Введ. 01.02.2008: М.: Стандартинформ, 2008, -URL: https://docs.cntd.ru/document/1200058320 -Текст: электронный.

16. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatisation. Factors influencing the information. General: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, (Переиздание) 2018. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021) -Текст: электронный.

17. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Information protection. Sequence of protected operational system formation. General provisions; Национальный стандарт РФ: Введ. 01.09.2014.- М.: Стандартинформ, (Переиздание) октябрь 2018.-URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 15.03.2021) Текст: электронный.

18. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.-12 л. -Текст: непосредственный.

19. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: Technical information protection. Terms and

definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.-20 л.- Текст: непосредственный.

Периодические издания

1. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 16.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

3. «Information Security / Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Текст: электронный.

4. «Вопросы кибербезопасности». – URL: http://cyberrus.com/ (дата обращения: 15.03.2021). – Текст: электронный.

5. Inside ./ Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 10.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный

6. Jet Info./Издатель: компания «Инфосистемы Джет». – URL: http://www.jetinfo.ru (дата обращения: 15.03.2021). – Режим доступа: свободный.

7. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХБАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

4. Бюро научно-технической информации «Техника для спецслужб». – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Текст : электронный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС http://orioks.miet.ru.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (http://orioks.miet.ru).

Тестирование проводится в ОРИОКС (MOODLe).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome/Explorer).
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110	1. Операционная система Microsoft Win Pro 7 – 28 шт. 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL – 28 шт. 3. Лиц. наПО Multisim 9 Academic Edituon Single seal – 28 шт.

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	– 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	4. Корпоративная информационно - технологическая платформа ОРИОКС – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 – 28 шт. 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL – 28 шт. 3. Лиц. наПО Multisim 9 Academic Edituon Single seal– 28 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС – 28 шт.

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-1.ЗИС «Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание».

ФОС по подкомпетенции ОПК-2.ЗИС «Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности».

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/**.**

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

В целях практической подготовки в дисциплине предусмотрены практические занятия (групповые упражнения), лабораторные работы и выполнение курсовогопроекта.

Каждая лабораторная работа и практическое занятие направлены на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

Лабораторные работы и практические занятия выполняются каждым студентом индивидуально. По результатам выполнения каждой лабораторной работы и практического занятия студент оформляет и представляет отчет. При защите отчетов по лабораторным работам и практическим занятиям преподаватель разбирает типовые ошибки и указывает их причины.

Курсовой проект (КП) направлена на формирование общепрофессиональных компетенции. КП выполняются студентами индивидуально. По результатам выполнения КП каждый студент оформляет и представляет отчет. При защите отчетов по КП преподаватель разбирает типовые ошибки и указывает их причины.

11.2. Методические указания студентам по подготовке к лабораторным работам и групповым упражнениям

Выполнение студентами к лабораторных работ и групповых упражнений направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Ведущей дидактической цельюЛР (ГУ) является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Наряду с ведущей дидактической целью в ходе выполнения заданий у студентов формируются практические умения и навыки обращения с различными приборами, установками, лабораторным оборудованием, аппаратурой, которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).

Лабораторные работы и групповые упражнения, как виды учебных занятий проводиться в специально оборудованных учебных лабораториях. Продолжительность - не менее двух академических часов. Необходимыми структурными элементами ЛР (ГУ), помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

По каждойЛР (ГУ) разработаны и утверждены методические указания по их проведению.

Лабораторные работы и групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов наЛР (ГУ): индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения ЛР (ГУ)преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждой ЛР (ГУ), предусмотренными рабочей программой учебной дисциплины: в соответствии с количеством часов, требованиями к знаниям и умениям, темой практических занятий и лабораторных работ, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению ЛР (ГУ) включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ЛР (ГУ);
- наименование темы ЛР (ГУ);
- цель ЛР (ГУ) (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);
- требования по теоретической готовности студентов к выполнению ЛР (ГУ) (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;
- список рекомендуемой литературы;
- приложения.

При подготовке к ЛР (ГУ) студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ЛР (ГУ);
- ознакомиться с методическими рекомендации по выполнениюЛР (ГУ);
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к ЛР (ГУ);
- изучить схемы лабораторных установок (стендов), порядок работы на аппаратуре и технике, правила и меры безопасности;
- подготовить отчеты для заполнения.

На ЛР (ГУ) студент должен выполнить задание в соответствии с методическими указаниями.

Отчет о ЛР (ГУ) должен быть оформлен в соответствии методическими указаниями и ГОСТами.

При защите отчета о ЛР (ГУ) убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и провести исследования, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на ЛР (ГУ) обязаны соблюдать меры безопасности при работе на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

11.3. Методические указания студентам по подготовке курсовогопроекта

Тема курсового проекта «Разработка технического проекта на создание системы защиты информации автоматизированной системы».

Задачи выполнения курсовой работы:

привитие навыков описания защищаемой АС, обоснования состава системы защиты информации автоматизированной системы (СЗИ АС), технических требований к СЗИ АС, характеристик и объема выполняемых работ, требований к отчетным документам по итогам выполненной работы;

развитие умений разработки комплекта эксплуатационной документации на СЗИ АС: формуляр, инструкции эксплуатационные специальные (инструкция по мерам безопасности, инструкция по защите информации), ведомости эксплуатационных документов и т.д.;

формирование опыта деятельности при подготовке организационно-распорядительной документации на СЗИ АС: акт приемки СЗИ АС в эксплуатацию; протокол испытаний АСЗИ; план-график работ по вводу в эксплуатацию АСЗИ; приказ о вводе в эксплуатацию АСЗИ.

Объект исследования – система защиты информации автоматизированной системы обработки конфиденциальной информации (СЗИАС).

Для выполнения задания студентам выделяются реально существующие объекты информатизации предприятий (учреждений).

Разработка технического проекта на создание СЗИАС выбранных объектов информатизации студентами проводятся в ходе производственной практики.

При проведении проектирования СЗИАС студенты проводят:

1. Анализ полноты исходных данных, проверка их соответствия фактическим условиям размещения, монтажа и эксплуатации технических средств выбранного объекта.
2. Исследование технологического процесса обработки и хранения информации на выбранном объекте.
3. Исследование процесса создания АС как совокупности упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания АС, соответствующей заданным требованиям.
4. Анализ и выбор стадий и этапов создания АС как части процесса создания по соображениям рационального планирования и организации работ.
5. Проведение работы по развитию АС по стадиям и этапам, применяемым для создания АС.
6. Определение состава и правил выполнения работ на установленных стадиях и этапах.

После проведения работы по проектированию студенты оформляют:

- Техническое задание на создание СЗИАС.
- Технический проект на СЗИАС.

Курсовойпроект(КП) выполняется на основе глубокого изучения основной и дополнительной литературы по дисциплине (учебники, учебные пособия, монографии, журналы и другие периодические издания, сайты в INTERNET). При выполнении курсовой работы рекомендуется широко использовать внутренние документы организаций, а также привлекать различного рода официальную, справочную, инструктивную, методическую, нормативную и другую документацию.

Структура КП должна отвечать традиционным требованиям, предъявляемым к научным работам и включать следующие части (структурные элементы):

Титульный лист.

Задание на КП.

Реферат.

Содержание.

Перечень условных обозначений и сокращений.

Введение.

Основная часть (основные разделы работы, предусмотренные заданием).

Заключение.

Список использованных источников.

Приложения.

Объем пояснительно записки составляет 50 – 70 страниц машинописного текста с приложениями, выполненных на стандартных листах формата А4.

Титульный лист является первым листом в пояснительной записке.

Реферат – это сокращенное изложение содержания и существа КП с основными сведениями о выполненных разработках и полученных результатах.

Реферат имеет следующую структуру:

− перечень количественных сведений о КП;

− перечень ключевых слов;

− текст реферата.

Перечень количественных сведений о КП должен включать количество: ___ с., ___ рис., ___ табл., __ источник, ___ прил.)..

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста КП, которые в наибольшей мере характеризуют содержание и обеспечивают возможность информационного поиска. Ключевые слова приводятся в именительном падеже и печатаются строчными буквами в строку через запятые.

Текст реферата в общем случае должен отражать сведения:

− об объекте информатизации;

− автоматизированной системе;

− об использованных методах и средствах защиты информации;

− о результатах проектирования СЗИ.

Если КП не содержит сведений по какой-либо из перечисленных структурных частей реферата, то в тексте реферата она опускается, при этом последовательность изложения сохраняется.

Объем реферата определяется содержанием КП, количеством сведений и их научной и практической ценностью. Средний объем реферата составляет 1500 − 2000 знаков.

Перечень условных обозначений и сокращений. Принятые в работе малораспространенные условные обозначения, сокращения, символы, единицы и специфические термины необходимо представлять в виде отдельного списка. Если сокращения, условные обозначения, символы, единицы и термины повторяются в работе менее трех раз, отдельный список не составляют, а расшифровку дают непосредственно в тексте при первом упоминании.

Содержание пояснительной записки включает введение, наименования всех разделов, подразделов и пунктов (если последние имеют наименования), заключение, список использованных источников и наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки.

Введение должно содержать:

− общие сведения о целях, задачах и организации создаваемой СЗИ на выбранном объекте;

− постановку задачи исследования с указанием цели, используемых методов и средств;

− исходные данные по исследуемому объекту;

− планируемые результаты.

Объем введения 3 − 5 страниц.

Основная часть. Основная часть должна включать:

При подготовке технического задания:

Перечень требований к создаваемой СЗИ.

Пояснительную записку с описанием исследуемого объекта.

Вариант технического задания.

При разработке технического проекта:

Варианты организационных, технических и программных решений, соответствующих предъявляемым требованиям к системе.

Комплект эксплуатационной документации.

Вариант технического проекта.

Заключение должно содержать:

− краткие выводы по результатам выполнений работы;

− оценку полноты решений поставленных задач.

Типовой объем заключения составляет 1-2 страницы.

Список использованных источников должен содержать сведения обо всех источниках, использованных при написании КР. В список следует включать только те наименования, с которыми автор КР ознакомился лично. На все источники, приведенные в списке, должны быть ссылки в тексте. На источники, содержащие общие сведения по теме ВКР, ссылки делаются обычно во введении.

Источники в списке нумеруются в порядке появления ссылок в тексте.

При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ 7.1–2003.

Приложения. В приложения выносится планы и план-схемы объекта, схемы электропитания, заземления объекта, схемы инженерных коммуникаций, линий связи и т.д., перечень требований и варианты проектных решений по разрабатываемой системе, а также результаты сравнительного анализа предлагаемых технических и программных решений.

Все приложения нумеруются и располагаются в конце пояснительной записки в порядке ссылок на них. Каждое приложение начинается с новой страницы и имеет содержательный заголовок. При необходимости текст приложения может быть разбит на разделы, подразделы, пункты и подпункты, которые следует нумеровать в пределах каждого приложения в соответствии с требованиями для основной части записки.

Курсовой проект должен быть выполнен студентом самостоятельно, грамотно, по логически построенному плану. Прямое переписывание в работе текста из учебной и научной литературы не допускается.

11.3. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-бальная система.

Под накопительно-бальнойсистемой понимается система количественной, балльно - рейтинговой оценки качества освоения учебной дисциплины студентом $R_{нак}$ по суммарному результату текущего$R_{тек}$ и итогового контроля $R_{итог}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{пр}$.

Выполнение контрольных мероприятийтекущего контроля (сдача компьютерных тестов, защита отчетов по лабораторным работам, защита отчетов по выполнению практических заданий),посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача экзамена) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины –$R_{нор}$).

Примерная структура и график контрольных мероприятий приведены в таблице 11.1

Таблица 11.1

Структура и график контрольных мероприятий дисциплины

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
4	Практическое занятие № 1	4	2
5	Практическое занятие № 2	4	2
6	Практическое занятие № 3	4	2
7	Практическое занятие № 4	4	2
8	Практическое занятие № 5	4	2
9	Практическое занятие № 6	4	2
9	Компьютерный тест (КТ-1)	4	2
12	Лабораторная работа № 1	6	3
13	Лабораторная работа № 2	6	3
14	Лабораторная работа № 3	6	3
15	Лабораторная работа № 4	6	3
16	Лабораторная работа № 5	6	3
16	Компьютерный тест (КТ-2)	4	2
16	Посещаемость, активность	6	3
	Итого за текущий контроль	***68***	***34***
	Итоговый контроль	***32***	***16***
	Накопленный рейтинг	**100**	**50**

В экзаменационную ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Примерная структура и график контрольных мероприятий при выполнении курсовой работы приведены в таблице 11.2.

Таблица 11.2

Структура и график контрольных курсовой работы

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
8	Контроль № 1	10	5

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
12	Контроль № 2	10	5
16	Контроль № 3	10	5
17	Итоговый просмотр (оценка качества курсовой работы)	50	25
	Итого за текущий контроль	***80***	***40***
18	***Итоговый контроль****(защита курсовой работы)*	***20***	***10***
	Накопленный рейтинг	**100**	**50**

За курсовую работу в зачетную ведомость и зачетную книжку вносится ***итоговая 5-балльная оценка***, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в зачетную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в зачетную ведомость.

РАЗРАБОТЧИК

Профессор кафедры «Информационная безопасность»
доктор технических наук _____ В.А.Щербаков

Рабочая программа дисциплины «Защищенные информационные системы» по направлению подготовки 10.04.01 «Информационная безопасность», направленности (профилю) «Аудит информационной безопасности» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Лист согласования

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества
Начальник АНОК _____ / И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ
Директор библиотеки _____ / Т.П.Филиппова /